(*May 18, 2017*)

Number theory notes 2011-12

Paul Garrett garrett@math.umn.edu http://www.math.umn.edu/˜garrett/

[This document is http://www.math.umn.edu/˜garrett/m/number_theory/Notes_2011-12.pdf]

These notes are derived from overheads used in my 2011-12 course, reformatted, with repetitions mostly eliminated, details and examples added. After the basics, the Iwasawa-Tate viewpoint on ζ-functions and L-functions is discussed fairly completely. To give a comparably complete, intelligible treatment of classfield theory would require far more background discussion of homological algebra than would fit into a number theory course or notes. Rather than aim for complete proofs, we have given many examples, and have reinterpreted many preliminary results in homological style to suggest how things are put together.

Basics

1. Example: Riemann's explicit formula 3
2. Exploiting analytic properties of generating functions 11
3. Quadratic reciprocity and factorization of ζ-functions 13
4. Hensel's lemma: equations modulo p^n, p-adic numbers 23
5. Characterizations versus constructions 31
6. Algebraic integers, Dedekind domains 35
7. Coverings of the affine line over $\mathbb{C}$ 43
8. Extensions of local fields 53
9. Primes lying over/under 60
10. Localization 62
11. More about primes-lying-over 68
12. Unique factorization of ideals in Dedekind domains 72
13. Ramification, residue field extension degrees, e, f, g 75
14. Finiteness of ramification 77
15. Dedekind zeta functions 78
16. Topologies, limits, completions 87
17. More on differents $\mathfrak{d}_{K/k}$ and complementary modules 97
18. Example: cyclotomic extensions of $\mathbb{Q}$ 101
19. Kummer, Eisenstein, Gauss sums, Lagrange resolvents 102
20. Fujisaki: units theorem, finiteness of class numbers 113

Iwasawa-Tate theory of ζ-functions and L-functions

21. Toward Iwasawa-Tate on L-functions 122
22. Volume of $SL_n(\mathbb{Z})\backslash SL_n(\mathbb{R})$ 129
23. Knowability of $\zeta(n)$ and other special values 133
24. Change-of-measure and Haar measure on $\mathbb{A}$ and k_v 135
25. Toward Iwasawa-Tate: Fourier series on $\mathbb{A}/k$ 139
26. Spectral theorem for compact self-adjoint operators 147
27. Iwasawa-Tate for Riemann's $\zeta(s)$ 150
28. Iwasawa-Tate for Dirichlet L-functions 153
29. Iwasawa-Tate for Dedekind zetas of number fields 155
30. Iwasawa-Tate general case: Hecke L-functions 159
31. Recapitulation 161
32. Local functional equations 162
33. The elementary global integral 163
34. Vanishing of ramified elementary global integrals 164
35. Good finite-prime local zeta integrals 165
36. Archimedean local zeta integrals 166
37. Convergence of local zeta integrals 168
38. Convergence of global half-zeta integrals 170

Toward classfield theory, reciprocity laws, homology

39. Classfield theory: semi-classical preview, examples 172
40. Classfield theory: semi-modern preview, examples 178
41. Homological ideas: Hilbert's theorem 90 181
42. Classfield theory: connecting local and global 182
43. Proof of quadratic norm-residue symbol reciprocity 185
44. Herbrand quotients, topological antecedents 191
45. Homological paraphrase of Hilbert's Theorem 90 194
46. Sample exact sequences 195
47. Herbrand quotients: less-bare definition 197
48. The snake lemma and the Gamma function 200
49. Local cyclic norm index theorem 202
50. More cohomology, statements of theorems 204

Bibliography 208

1. *Example: Riemann's explicit formula*

Already in the number theory of $\mathbb{Z}$, the relationship between *primes* and analytic properties of the Riemann-Euler $\zeta(s)$ is striking.

More interesting than a Prime Number Theorem of [Hadamard 1896] and [de la Vallée-Poussin 1896] is the *precise* relationship between primes and zeros of zeta discovered by [Riemann 1859].

Such ideas apply to any zeta or L-function for which we know an analytic continuation and other reasonable properties.

It took 40 years for [Hadamard 1893], [vonMangoldt 1895], and others to complete Riemann's sketch of the *Explicit Formula* relating primes to zeros of the Euler-Riemann zeta function. Even then, as long as we lack a zero-free strip inside the critical strip, the Explicit Formula does *not* yield a Prime Number Theorem, despite giving a precise relationship between primes and zeros of zeta.

[1.1] Riemann's explicit formula

Riemann's dramatic relation between primes and zeros of the zeta function depends on many ideas undeveloped in Riemann's time. Thus, the following sketch, roughly following Riemann, is not a proof. Rather, the sketch exposes supporting ideas needing development to produce a proof.

Euler had already observed that $\zeta(s)$ has an *Euler product* expansion in a half-plane

$$\zeta(s) \;=\; \sum_{n\geq 1} \frac{1}{n^s} \;=\; \prod_{p \text{ prime}} \frac{1}{1-\frac{1}{p^s}} \qquad\qquad (\mathrm{Re}\, s > 1)$$

Riemann showed that $\zeta(s)$ has a *meromorphic continuation* throughout $\mathbb{C}$ (see below).

If we believe, as Riemann did, and as Hadamard and others later *proved*, that it *also* has a *Riemann-Hadamard product* expansion

$$(s-1)\,\zeta(s) \;=\; e^{a+bs} \prod_\rho \Big(1-\frac{s}{\rho}\Big)\, e^{s/\rho} \cdot \prod_{n=1}^\infty \Big(1+\frac{s}{2n}\Big)\, e^{-s/2n}$$

product over ρ non-trivial zero of ζ, for all $s \in \mathbb{C}$, *then*, following Riemann, we can extract tangible information from the equality of the two products

$$(s-1) \prod_p \frac{1}{1-\frac{1}{p^s}} \quad=\quad e^{a+bs} \prod_\rho \Big(1-\frac{s}{\rho}\Big)\, e^{s/\rho} \cdot \prod_{n=1}^\infty \Big(1+\frac{s}{2n}\Big)\, e^{-s/2n} \qquad\qquad (\mathrm{Re}\, s > 1)$$

as follows. Take logarithmic derivatives of both sides, using $-\log(1-x) = x + x^2/2 + x^3/3 + \ldots$ on the left-hand side:

$$\frac{1}{s-1} - \sum_{m\geq 1,\; p} \frac{\log p}{p^{ms}} \;=\; b \;+\; \sum_\rho \Big(\frac{1}{s-\rho} + \frac{1}{\rho}\Big) \;+\; \sum_n \Big(\frac{1}{s+2n} - \frac{1}{2n}\Big)$$

A slight rearrangement gives

$$\sum_{m\geq 1,\; p} \frac{\log p}{p^{ms}} \;=\; \frac{1}{s-1} - b \;-\; \sum_\rho \Big(\frac{1}{s-\rho} + \frac{1}{\rho}\Big) \;-\; \sum_n \Big(\frac{1}{s+2n} - \frac{1}{2n}\Big)$$

The left-hand side needs $\mathrm{Re}\, s > 1$ for convergence, while the right-hand side converges for all $s \in \mathbb{C}$ apart from the visible poles at 1, the non-trivial zeros ρ, and the trivial zeros $2, 4, 6, \ldots$. Apply the *Perron identity*

$$\frac{1}{2\pi i} \int_{\sigma - i\infty}^{\sigma+i\infty} \frac{Y^s}{s}\, ds \;=\; \begin{cases} 1 & (\text{for } Y > 1) \\ \\ 0 & (\text{for } 0 < Y < 1) \end{cases} \qquad\qquad (\text{for } \sigma > 0)$$

The limits are fragile: more precisely,

$$\lim_{T\to\infty} \frac{1}{2\pi i}\int_{\sigma-iT}^{\sigma+iT} \frac{Y^s}{s}\,ds \;=\; \begin{cases} 1 & (\text{for } Y>1) \\ 0 & (\text{for } 0<Y<1)\end{cases} \qquad (\text{for } \sigma>0)$$

If we can apply this to entire expressions, by

$$f \longrightarrow \lim_{T\to\infty}\frac{1}{2\pi i}\int_{\sigma-iT}^{\sigma+iT} f(s)\cdot\frac{X^s}{s}\,ds \qquad (\text{with } \sigma>1)$$

term-wise to the left-hand side, *and* use residues *term*-wise to evaluate the right-hand side,

$$\sum_{p^m<X}\log p \;=\; (X-1)\;-\;b\;-\;\sum_\rho\Big(\frac{X^\rho}{\rho}+\frac{1}{-\rho}+\frac{1}{\rho}\Big)\;-\;\sum_n\Big(\frac{X^{-2n}}{-2n}+\frac{1}{2n}-\frac{1}{2n}\Big)$$

which simplifies to von Mangoldt's reformulation of *Riemann's Explicit Formula:*

$$\sum_{p^m<X}\log p \;=\; X\;-\;(b+1)\;-\;\sum_\rho\frac{X^\rho}{\rho}\;+\;\sum_{n\geq 1}\frac{X^{-2n}}{2n}$$

Slightly more precisely, because of the way the Perron integral transform is applied, and the fragility of the convergence,

$$\sum_{p^m<X}\log p \;=\; X\;-\;(b+1)\;-\;\lim_{T\to\infty}\sum_{|\mathrm{im}(\rho)|<T}\frac{X^\rho}{\rho}\;+\;\sum_{n\geq 1}\frac{X^{-2n}}{2n}$$

The Riemann-Hadamard product needs both *generalities* about Weierstraß-Hadamard product expressions for entire functions of prescribed growth, and *specifics* about the growth of the *analytic continuation* of $\zeta(s)$.

[1.2] Remark: The two sides of the equality of logarithmic derivatives are qualitatively different. The logarithmic derivative of the Euler product converges in right half-planes, and converges all the better farther to the right. The logarithmic derivative of the Riemann-Hadamard product does not converge strongly, but is not restricted to a half-plane, and its poles are exhibited explicitly by the expression.

[1.3] Remark: See [Guinand 1947] and [Weil 1952], [Weil 1972] for modern re-interpretations of Riemann's 1859 formula.

[1.4] Analytic continuation and functional equation of $\zeta(s)$

The ideas gained publicity and importance from Riemann's paper, but were apparently known to some degree before Riemann's time.

The key is that the completed zeta function has an *integral representation* in terms of an *automorphic form*, namely, the simplest theta function. Both the analytic continuation and the functional equation of zeta follow from this integral representation using a parallel functional equation of the theta function, the latter demonstrated by *Poisson summation.*

Elementary-but-doomed argument: It is worthwhile to see that simple calculus can extend the domain of $\zeta(s)$ a little. The idea is to pay attention to *quantitative* aspects of the integral test. That is,

$$\zeta(s)-\frac{1}{s-1}\;=\;\zeta(s)-\int_1^\infty\frac{dx}{x^s}\;=\;\sum_n\Big(\frac{1}{n^s}-\int_n^{n+1}\frac{dx}{x^s}\Big)\;=\;\sum_n\Big(\frac{1}{n^s}-\frac{1}{s-1}\Big[\frac{1}{n^{s-1}}-\frac{1}{(n+1)^{s-1}}\Big]\Big)$$

Even for complex s, we have a Taylor-Maclaurin expansion with error term

$$(n+1)^{1-s}\;=\;\big(n\cdot(1+\frac{1}{n})\big)^{1-s}\;=\;n^{1-s}\cdot\big(1+\frac{1-s}{n}+O(\tfrac{1}{n^2})\big)\;=\;\frac{1}{n^{s-1}}-\frac{s-1}{n^s}+O(\frac{s-1}{n^{s+1}})$$

The constant in the big-O term is *uniform* in n for fixed s. Thus,

$$\frac{1}{n^s} - \frac{1}{s-1}\Big[\frac{1}{n^{s-1}} - \frac{1}{(n+1)^{s-1}}\Big] \;=\; O\big(\tfrac{1}{n^{s+1}}\big)$$

That is, for fixed $\mathrm{Re}(s) > 0$, we have *absolute convergence* of

$$\sum_n \Big(\frac{1}{n^s} - \frac{1}{s-1}\Big[\frac{1}{n^{s-1}} - \frac{1}{(n+1)^{s-1}}\Big]\Big)$$

in the larger region $\mathrm{Re}(s) > 0$. A similar but increasingly complicated device produces a meromorphic continuation to half-planes $\mathrm{Re}(s) > \ell$. However, this approach is under-powered.

A more serious argument: Euler's integral for the **gamma function** is

$$\Gamma(s) \;=\; \int_0^\infty e^{-t}\, t^s\, \frac{dt}{t}$$

Among other roles, the gamma function $\Gamma(s)$ interpolates the *factorial function*: integration by parts yields $\Gamma(n) = (n-1)!$ for positive integer n.

[1.5] Theorem: The *completed* zeta function

$$\xi(s) \;=\; \pi^{-\frac{s}{2}}\, \Gamma(\frac{s}{2})\, \zeta(s)$$

has an analytic continuation to $s \in \mathbb{C}$, except for simple poles at $s = 0, 1$, and has the *functional equation*

$$\xi(1-s) \;=\; \xi(s)$$

... and (anticipating the Riemann-Hadamard product issues) $s(s-1)\xi(s)$ is entire and **bounded in vertical strips**.

The following proof-sketch is itself an archetype. The simplest *theta function* is

$$\theta(z) \;=\; \sum_{n\in\mathbb{Z}} e^{\pi i n^2 z}$$

with z in the complex upper half-plane $\mathfrak{H}$. By Riemann's time, Jacobi's functional equation of $\theta(z)$ was well-known, as the simplest example of a larger technical phenomenon:

$$\theta(z) \;=\; \frac{1}{\sqrt{-iz}} \cdot \theta(-1/z)$$

(Proven below.) The modified version

$$\frac{\theta(iy)-1}{2} \;=\; \sum_{n=1}^\infty e^{-\pi n^2 y}$$

appears just below. The connection to $\zeta(s)$ is the *integral presentation*:

[1.6] Claim: For $\mathrm{Re}(s) > 1$

$$\pi^{-s/2}\,\Gamma(\frac{s}{2}) \cdot \zeta(s) \;=\; \int_0^\infty \frac{\theta(iy)-1}{2} \cdot y^{s/2} \cdot \frac{dy}{y}$$

Meaning? An integral against t^s with dt/t, a *Mellin transform*, is just a *Fourier transform* in different coordinates.

Starting from the integral, for $\mathrm{Re}(s) > 1$, compute directly

$$\int_0^\infty \frac{\theta(iy)-1}{2}\, y^{s/2}\, \frac{dy}{y} \;=\; \int_0^\infty \sum_{n\geq 1} e^{-\pi n^2 y}\, y^{s/2}\, \frac{dy}{y} \;=\; \sum_{n\geq 1}\int_0^\infty e^{-\pi n^2 y}\, y^{s/2}\, \frac{dy}{y}$$

$$= \pi^{-s/2}\sum_{n\geq 1}\frac{1}{n^{2s}}\int_0^\infty e^{-y}\, y^{s/2}\, \frac{dy}{y}$$

by replacing y by $y/(\pi n^2)$, and this is

$$\pi^{-s/2}\Gamma(\frac{s}{2})\cdot\sum_{n\geq 1}\frac{1}{n^s} \;=\; \xi(s) \qquad\qquad (\text{for } \mathrm{Re}(s) > 1)$$

$\dfrac{\theta(iy)-1}{2} = \displaystyle\sum_{n=1}^{\infty} e^{-\pi n^2 y}$ is of rapid decay as $y \to +\infty$:

$$\frac{\theta(iy)-1}{2} \;=\; \sum_{n\geq 1} e^{-\pi n^2 y} \;\leq\; e^{-\pi y/2}\sum_{n\geq 1} e^{-\pi n^2/2} \;=\; \text{const}\cdot e^{-\pi y/2} \qquad\qquad (\text{for } y \geq 1)$$

Thus, the integral from 1 (not 0) to $+\infty$ is nicely convergent for *all* values of s, and

$$\int_1^\infty \frac{\theta(iy)-1}{2}\, y^{s/2}\, \frac{dy}{y} \;=\; \text{entire in } s$$

The trick (known before Riemann) is to use Jacobi's functional equation for $\theta(z)$ to convert the part of the integral from 0 to 1 into a similar integral from 1 to $+\infty$. It is not obvious that $\theta(iy)$ has any property that would ensure this. However, in the early 19th century theta functions were intensely studied. Again, the functional equation of θ, proven below, is

$$\theta(z) \;=\; \frac{1}{\sqrt{-iz}}\cdot\theta(-1/z)$$

Book-keeping:

$$\frac{\theta(-1/iy)-1}{2} = y^{1/2}\frac{\theta(iy)-1}{2} + \frac{y^{1/2}}{2} - \frac{1}{2}$$

Then

$$\int_0^1 \frac{\theta(iy)-1}{2}\, y^{s/2}\, \frac{dy}{y} \;=\; \int_1^\infty \frac{\theta(-1/iy)-1}{2}\, y^{-s/2}\, \frac{dy}{y} \;=\; \int_1^\infty \left(y^{1/2}\frac{\theta(iy)-1}{2} + \frac{y^{1/2}}{2} - \frac{1}{2}\right) y^{-s/2}\, \frac{dy}{y}$$

$$= \int_1^\infty \frac{\theta(iy)-1}{2}\, y^{-s/2}\, \frac{dy}{y} + \int_1^\infty \left(\frac{y^{(1-s)/2}}{2} - \frac{y^{-s/2}}{2}\right)\frac{dy}{y} \;=\; \int_1^\infty \frac{\theta(iy)-1}{2}\, y^{-s/2}\, \frac{dy}{y} + \frac{1}{s-1} - \frac{1}{s}$$

$$= (\text{entire}) + \frac{1}{s-1} - \frac{1}{s}$$

The elementary expressions $1/(s-1)$ and $1/s$ certainly have meromorphic continuations to $\mathbb{C}$, with explicit poles. Thus, together with the first integral from 1 to ∞, we have

$$\pi^{-s/2}\,\Gamma(\frac{s}{2})\,\zeta(s) \;=\; \int_1^\infty \frac{\theta(iy)-1}{2}\,(y^{s/2} + y^{(1-s)/2})\,\frac{dy}{y} + \frac{1}{s-1} - \frac{1}{s} \;=\; (\text{entire}) + \frac{1}{s-1} - \frac{1}{s}$$

The right-hand side is visibly symmetrical under $s \to 1-s$, which gives the functional equation. ///

[1.7] Remark: Attempting to avoid the gamma factor $\pi^{-s/2}\Gamma(\frac{s}{2})$ leads to an unsymmetrical and unenlightening form. The fact that $\Gamma(s/2)$ has no zeros assures that it masks no poles of $\zeta(s)$. Non-vanishing of $\Gamma(s)$ follows from the identity

$$\Gamma(s)\cdot\Gamma(1-s) \;=\; \frac{\pi}{\sin \pi s}$$

[1.8] Claim: *(Jacobi's functional equation for $\theta(z)$)*

$$\theta(-1/iy) = \sqrt{y}\cdot\theta(iy)$$

Proof: This symmetry itself follows from a more fundamental fact, the *Poisson summation formula*

$$\sum_{n\in\mathbb{Z}} f(n) \;=\; \sum_{n\in\mathbb{Z}} \widehat{f}(n) \qquad\qquad (\widehat{f} \text{ is Fourier transform})$$

where

$$\text{Fourier transform of } f \;=\; \widehat{f}(\xi) \;=\; \int_{\mathbb{R}} f(x)\, e^{-2\pi i x\xi}\, dx$$

The Poisson summation formula is applied to

$$f(x) \;=\; \varphi(\sqrt{y}\cdot x) \quad\text{ with }\quad \varphi(x) \;=\; e^{-\pi x^2}$$

The Gaussian $\varphi(x) = e^{-\pi x^2}$ has the useful property that it is its own Fourier transform. We can prove that the Gaussian is its own Fourier transform by completing the square and a contour integration shift:

$$\widehat{\varphi}(\xi) \;=\; \int_{\mathbb{R}} e^{-\pi x^2}\, e^{-2\pi i x\xi}\, dx \;=\; \int_{\mathbb{R}} e^{-\pi(x+i\xi)^2-\pi\xi^2}\, dx \;=\; e^{-\pi\xi^2}\int_{\mathbb{R}} e^{-\pi(x+i\xi)^2}\, dx$$

By moving the contour of integration, the latter integral is

$$\int_{\mathbb{R}} e^{-\pi(x+i\xi)^2}\, dx \;=\; \int_{\mathbb{R}+i\xi} e^{-\pi x^2}\, dx \;=\; \int_{\mathbb{R}} e^{-\pi x^2}\, dx$$

Thus, the integral is a independent of ξ. In fact, the constant is 1. By a straightforward change of variables, Fourier transform behaves well with respect to *dilations*:

$$\widehat{f}(\xi) \;=\; \int_{\mathbb{R}} \varphi(\sqrt{y}\,x)\, e^{-2\pi i x\xi}\, dx \;=\; \frac{1}{\sqrt{y}}\int_{\mathbb{R}} \varphi(x)\, e^{-2\pi i x\xi/\sqrt{y}}\, dx \;=\; \frac{1}{\sqrt{y}}\widehat{\varphi}(\xi/\sqrt{y}) \;=\; \frac{1}{\sqrt{y}}e^{-\pi\xi^2/y}$$

replacing x by $x/\sqrt{y}$. Applying Poisson summation to $f(x) = e^{-\pi x^2 y}$,

$$\sum_{n\in\mathbb{Z}} e^{-\pi n^2 y} \;=\; \frac{1}{\sqrt{y}}\sum_{n\in\mathbb{Z}} e^{-\pi n^2/y}$$

This gives

$$\theta(iy) \;=\; \frac{1}{\sqrt{y}}\theta(-1/iy)$$

Remark For $z \in \mathfrak{H}$, also $-1/z \in \mathfrak{H}$, and the series for $\theta(z)$ and $\theta(-1/z)$ are nicely convergent. The identity proven for θ is $\theta(-1/z) = \sqrt{-iz}\,\theta(z)$ on the imaginary axis. The *Identity Principle* from complex analysis implies that the same equality holds for all $z \in \mathfrak{H}$.

Heuristic for *Poisson summation*

$$\sum_{n\in\mathbb{Z}} f(n) \;=\; \sum_{n\in\mathbb{Z}} \widehat{f}(n)$$

The *periodicized* version of a function f on $\mathbb{R}$ is

$$F(x) \;=\; \sum_{n\in\mathbb{Z}} f(x+n)$$

A periodic function should be (!) represented by its *Fourier series*:

$$F(x) \;=\; \sum_{\ell\in\mathbb{Z}} e^{2\pi i\ell x} \int_0^1 F(x)\, e^{-2\pi i\ell x}\, dx$$

Fourier *coefficients* of F expand to be the Fourier *transform* of f:

$$\int_0^1 F(x)\, e^{-2\pi i\ell x}\, dx \;=\; \int_0^1 \sum_{n\in\mathbb{Z}} f(x+n)\, e^{-2\pi i\ell x}\, dx \;=\; \sum_{n\in\mathbb{Z}} \int_n^{n+1} f(x)\, e^{-2\pi i\ell x}\, dx$$

$$=\; \int_{\mathbb{R}} f(x)\, e^{-2\pi i\ell x}\, dx \;=\; \widehat{f}(\ell)$$

Evaluating at 0, we should have

$$\sum_{n\in\mathbb{Z}} f(n) \;=\; F(0) \;=\; \sum_{\ell\in\mathbb{Z}} \widehat{f}(\ell)$$

What would it take to legitimize this? Certainly f must be of sufficient decay so that the integral for its Fourier transform is convergent. and so that summing its translates by $\mathbb{Z}$ is convergent.

We'd want f to be continuous, probably differentiable, so that we can talk about pointwise values of F

... and to make plausible the hope that the Fourier series of F converges to F pointwise.

For f and several derivatives rapidly decreasing, the Fourier transform $\widehat{f}$ will be of sufficient decay so that its sum over $\mathbb{Z}$ does converge.

A simple sufficient hypothesis for convergence is that f be in the *Schwartz space* of infinitely-differentiable functions all of whose derivatives are of *rapid decay*, that is,

$$\text{Schwartz space} = \{\text{smooth}\, f : \sup_x (1+x^2)^\ell |f^{(i)}(x)| < \infty \text{ for all } i,\ell\}$$

Representability of a periodic function by its Fourier series is a serious question, with several possible senses. We want *pointwise convergence.* A special, self-contained argument gives a good-enough result for immediate purposes.

Consider ($\mathbb{Z}$-)periodic functions on $\mathbb{R}$, that is, complex-valued functions f on $\mathbb{R}$ such that $f(x+n) = f(x)$ for all $x \in \mathbb{R}$, $n \in \mathbb{Z}$. For periodic f sufficiently nice so that integrals

$$\widehat{f}(n) \;=\; \int_0^1 f(x)\, e^{-2\pi i n x}\, dx \qquad\qquad (n^{th} \text{ Fourier coefficient of } f)$$

make sense, the *Fourier expansion* of f is

$$f \;\sim\; \sum_{n\in\mathbb{Z}} \widehat{f}(n)\, e^{2\pi i n x}$$

We want

$$f(x_o) \;=\; \sum_{n\in\mathbb{Z}} \widehat{f}(n)\, e^{2\pi i n x_o}$$

Consider periodic *piecewise-C^o* functions which are left-continuous and right-continuous at any discontinuities.

[1.9] Theorem: For periodic piecewise-C^o function f, left-continuous and right-continuous at discontinuities, for points x_o at which f is C^0 and *left-differentiable* and *right-differentiable*, the Fourier series of f evaluated at x_o *converges* to $f(x)$:

$$f(x_o) \;=\; \sum_{n\in\mathbb{Z}} \widehat{f}(n)\, e^{2\pi i n x_o}$$

That is, for such functions, at such points, the Fourier series *represents* the function *pointwise.*

A notable missing conclusion is *uniform* pointwise convergence. For more serious applications, pointwise convergence not known to be uniform is often useless.

Proof: Can reduce to $x_o = 0$ and $f(0) = 0$. Representability of $f(0)$ by the Fourier series is the assertion that

$$0 \;=\; f(0) \;=\; \lim_{M,N\to+\infty} \sum_{-M\le n<N} \widehat{f}(n)\, e^{2\pi i n\cdot 0} \;=\; \lim_{M,N\to+\infty} \sum_{-M\le n<N} \widehat{f}(n)$$

Substituting the defining integral for the Fourier coefficients:

$$\sum_{-M\le n<N} \widehat{f}(n) \;=\; \sum_{-M\le n<N} \int_0^1 f(u)\, e^{-2\pi i n u}\, du \;=\; \int_0^1 \sum_{-M\le n<N} f(u)\, e^{-2\pi i n u}\, du$$

$$=\; \int_0^1 f(u)\cdot \frac{e^{2\pi i M u} - e^{-2\pi i N u}}{1 - e^{-2\pi i u}}\, du$$

We will show that

$$\lim_{\ell\to\pm\infty} \int_0^1 \frac{f(u)\cdot e^{-2\pi i \ell u}}{1 - e^{-2\pi i u}}\, du \;=\; 0$$

Since $f(0) = 0$, the function

$$g(x) \;=\; \frac{f(x)}{1 - e^{-2\pi i x}}$$

is piecewise-C^o, and left-continuous and right-continuous at discontinuities. The only issue is at integers, and by the periodicity it suffices to prove continuity at 0.

$$\frac{f(x)}{1 - e^{-2\pi i x}} \;=\; \frac{f(x)}{x} \cdot \frac{x}{1 - e^{-2\pi i x}}$$

The two-sided limit

$$\lim_{x\to 0} \frac{x}{1 - e^{-2\pi i x}} \;=\; \frac{d}{dx}\Big|_{x=0} \frac{x}{1 - e^{-2\pi i x}}$$

exists, by differentiability. Similarly, we have left and right limits

$$\lim_{x\to 0^-} \frac{f(x)}{x} \qquad \text{and} \qquad \lim_{x\to 0^+} \frac{f(x)}{x}$$

by the one-sided differentiability of f. So both one-sided limits exist, giving the one-sided continuity of g at 0. ///

We find ourselves wanting a *Riemann-Lebesgue lemma*, that that the Fourier coefficients of a periodic, piecewise-C^o function g, with left and right limits at discontinuities, go to 0.

The essential property approximability by step functions: given $\varepsilon > 0$ there is a *step function* $s(x)$ such that

$$\int_0^1 |s(x) - g(x)|\, dx \;<\; \varepsilon$$

With such s,

$$|\widehat{s}(n) - \widehat{g}(n)| \;\le\; \int_0^1 |s(u) - g(u)|\, du \;<\; \varepsilon \qquad \text{(for all } \varepsilon > 0)$$

It suffices that Fourier coefficients of *step functions* go to 0, an easy computation:

$$\int_a^b e^{-2\pi i\ell x}\, dx \;=\; [\frac{e^{-2\pi i\ell x}}{-2\pi i\ell}]_a^b \;=\; \frac{e^{-2\pi i\ell b} - e^{-2\pi i\ell a}}{-2\pi i\ell} \;\longrightarrow\; 0$$

as $\ell \to \pm\infty$. Thus, the Fourier coefficients of g go to 0, so the Fourier series of f converges to $f(0)$ when f is C^1 at 0.

[1.10] $\Gamma(s) \cdot \Gamma(1-s) = \pi/\sin \pi s$ This useful identity is proven by a residue integration trick that has other applications, as well. Take $0 < \mathrm{Re}(s) < 1$ for convergence of both integrals, and compute

$$\Gamma(s) \cdot \Gamma(1-s) \;=\; \int_0^\infty \int_0^\infty u^s\, e^{-u} \cdot v^{1-s}\, e^{-v}\, \frac{du}{u}\, \frac{dv}{v} \;=\; \int_0^\infty \int_0^\infty u\, e^{-u(1+v)}\, v^{1-s}\, \frac{du}{u}\, \frac{dv}{v}$$

by replacing v by uv. Replacing u by $u/(1+v)$ (another instance of the basic *gamma identity*) and noting that $\Gamma(1) = 1$ gives

$$\int_0^\infty \frac{v^{-s}}{1+v}\, dv$$

Replace the path from 0 to ∞ by the *Hankel contour* H_ε described as follows. Far to the right on the real line, start with the branch of v^{-s} given by $(e^{2\pi i}v)^{-s} = e^{-2\pi is}v^{-s}$, integrate from $+\infty$ to $\varepsilon > 0$ along the real axis, clockwise around a circle of radius ε at 0, then back out to $+\infty$, now with the standard branch of v^{-s}. For $\mathrm{Re}(-s) > -1$ the integral around the little circle goes to 0 as $\varepsilon \to 0$. Thus,

$$\int_0^\infty \frac{v^{-s}}{1+v}\, dv \;=\; \lim_{\varepsilon \to 0} \frac{1}{1 - e^{-2\pi is}} \int_{H_\varepsilon} \frac{v^{-s}}{1+v}\, dv$$

The integral of this integrand over a large circle goes to 0 as the radius goes to $+\infty$, for $\mathrm{Re}(-s) < 0$. Thus, this integral is equal to the limit as $R \to +\infty$ and $\varepsilon \to 0$ of the integral

from R to ε
from ε clockwise back to ε
from ε to R
from R counterclockwise to R

This integral is $2\pi i$ times the sum of the residues inside it, namely, that at $v = -1 = e^{\pi i}$. Thus,

$$\Gamma(s) \cdot \Gamma(1-s) \;=\; \int_0^\infty \frac{v^{-s}}{1+v}\, dv \;=\; \frac{2\pi i}{1 - e^{-2\pi is}} \cdot (e^{\pi i})^{-s} \;=\; \frac{2\pi i}{e^{\pi is} - e^{-\pi is}} \;=\; \frac{\pi}{\sin \pi s}$$

2. *Exploiting analytic properties of generating functions*

The Perron identity used to reach the final step in the Riemann Explicit Formula above exemplifies extraction of elementary identities from analytic properties of generating functions.

In fact, integral transforms convert *one* spectral identity into *another*, by a Fourier transform. The point is that choices of transforms are made to heighten an *asymmetry*, with one side seemingly elementary and uncomplicated, and the other whatever it must be.

We consider Perron-type identities more carefully.

[2.1] Heuristic

The best-known identity starts from the *idea* that for $\sigma > 0$

$$\int_{\sigma-i\infty}^{\sigma-i\infty} \frac{X^s}{s}\, ds \;=\; \begin{cases} 1 & (\text{for } X > 1) \\ \\ 0 & (\text{for } 0 < X < 1) \end{cases} \qquad\qquad (\text{convergence?})$$

The *idea* of the proof of this identity is that, for $X > 1$, the contour of integration slides indefinitely to the left, eventually vanishing, picking up the residue at $s = 0$, while for $0 < X < 1$, the countour slides indefinitely to the right, eventually vanishing, picking up *no* residues.

The *idea* of the application is that this identity can extract *counting* information from a meromorphic continuation of a Dirichlet series: for example, from

$$\sum_n \frac{a_n}{n^s} \;=\; f(s) \qquad\qquad (\text{left-hand side convergent for } \mathrm{Re}\, s > 1)$$

we would have

$$\sum_{n<X} a_n \;=\; \text{sum of residues of } X^s\, f(s)/s$$

That is, the *counting* function $\sum_{n<X} a_n$ is *extracted* from the analytic object $\sum_\lambda a_n/n^s$ by the contour integration. With f a logarithmic derivative, such as $f(s) = \zeta'(s)/\zeta(s)$, the poles of f are mostly the zeros of ζ.

However, the tails of these integrals are fragile.

[2.2] Simple precise assertion

The elegant simplicity of the idea about moving lines of integration must be elaborated for correctness: for fixed $\sigma > 0$, for $T > 0$, we claim that

$$\int_{\sigma-iT}^{\sigma-iT} \frac{X^s}{s}\, ds \;=\; \begin{cases} 1 + O_\sigma\big(\frac{X^\sigma}{T\cdot \log X}\big) & (\text{for } X > 1) \\ \\ \quad O_\sigma\big(\frac{X^\sigma}{T\cdot |\log X|}\big) & (\text{for } 0 < X < 1) \end{cases}$$

The proof is a precise form of the idea of sliding vertical contours. That is, for $X > 1$, consider the contour integral around the rectangle with *right* edge $\sigma \pm iT$, namely, with vertices $\sigma - iT$, $\sigma + it$, $-B + iT$, $-B - iT$, with $B \to +\infty$. For $0 < X < 1$ consider the contour integral around the rectangle with *left* edge $\sigma \pm iT$, namely, with vertices $\sigma - iT$, $\sigma + it$, $B + iT$, $B - iT$, with $B \to +\infty$.

For both $X > 1$ and $0 < X < 1$, the $\pm(B \pm iT)$ edge of the rectangle is dominated by

$$\int_{-T}^{T} \frac{e^{-B|\log X|}}{|B \pm it|}\, dt \;\ll\; T \cdot \frac{e^{-B|\log X|}}{B} \;\to\; 0 \qquad\qquad (\text{as } B \to +\infty)$$

in both cases, the top and bottom edges of the rectangle are dominated by

$$X^\sigma \cdot \int_0^\infty \frac{e^{-u|\log X|}}{|(\sigma \pm u) + iT|}\,du \;\ll\; X^\sigma \cdot \int_0^\infty \frac{e^{-u|\log X|}}{T}\,du \;\ll\; \frac{X^\sigma}{T\cdot|\log X|}$$

This proves the claim. Replacing X by e^X in the estimate gives the equivalent

$$\frac{1}{2\pi i}\int_{\sigma-iT}^{\sigma-iT} \frac{e^{sX}}{s}\,ds \;=\; \begin{cases} 1 + O_\sigma(\frac{e^{\sigma X}}{T\cdot X}) & (\text{for } X>0) \\ O_\sigma(\frac{e^{\sigma X}}{T\cdot|X|}) & (\text{for } X<0)\end{cases}$$

[2.3] Hazards

When the quantity X above is summed, especially if the summation is over a set whose precise specifications are difficult, the denominators of the big-O error terms may blow up. In situations such as

$$\frac{1}{2\pi i}\int_{\sigma-iT}^{\sigma+iT} \Big(\sum_j a_j\, e^{-sX_j}\Big)\frac{e^{sX}}{s}\,ds \;=\; \sum_{j\,:\,X_j<X} a_j \;+\; \sum_j a_j\cdot O_\sigma\Big(\frac{e^{\sigma(X-X_j)}}{T\cdot|X-X_j|}\Big)$$

the distribution of the values X_j has an obvious effect on the convergence of the error term.

[2.4] The other side of the equation

A desired and plausible conclusion such as

$$\lim_T \frac{1}{2\pi i}\int_{\sigma-iT}^{\sigma-iT} f(s)\,\frac{e^{sX}}{s}\,ds \;=\; \big(\text{sum of } \mathrm{Res}_{s=\rho}\, f(s)\cdot \tfrac{e^{\rho X}}{\rho}\big)$$

summed over poles ρ of f in the left half-plane $\mathrm{Re}\, s < \sigma$, requires that the contour integrals over the other three sides of the rectangle with side $\sigma \pm iT$ go to 0, and that the tails of the vertical integral go to 0. The integral over the large rectangle will be evaluated with X large positive, so the decay condition applies to f to the *left*. The left side of the rectangle will go to 0 for large enough positive X when $f(s)$ has at worst exponential growth to the left, that is, when $f(s) \ll e^{-C\cdot|\mathrm{Re}\, s|}$ for *some* large-enough C and $\mathrm{Re}\, s \to -\infty$. The top and bottom are more fragile, since e^{sX}/s does not have strong decay vertically.

Not unexpectedly, the *poles* of f near $\sigma + iT$ may *bunch up* as T grows, so that a countour integral must be **threaded** between them, and the corresponding integral will be somewhat larger simply because of proximity to these poles. This contribution to vertical growth of f is significant in examples, and motivates alternatives, as below.

[2.5] Variant identities

When e^{sX}/s is altered to help convergence of the integral against the *counting* aspect is inevitably altered. The proofs of variants follow the same straightforward line as above for the simplest case. Rather than replacing e^{sX}/s with e^{sX}/s^2, a better effect is achieved with $e^{sX}/s(s+1)$. In fact, for $\theta > 0$ and $1 \le \ell \in \mathbb{Z}$

$$\frac{1}{2\pi i}\int_{\sigma-iT}^{\sigma-iT} \frac{e^{sX}}{s(s+\theta)(s+2\theta)\ldots(s+\ell\theta)}\,ds \;=\; \begin{cases} \frac{1}{\ell!\theta^\ell}(1-e^{-\theta X})^\ell + O_\sigma(\frac{e^{\sigma X}}{T^2\cdot X}) & (\text{for } X>0) \\ O_\sigma(\frac{e^{\sigma X}}{T^2\cdot|X|}) & (\text{for } X<0)\end{cases}$$

Indeed, the residues at the poles $0, -\theta, -2\theta, \ldots, -\ell\theta$ sum to

$$\frac{e^{0\cdot X}}{(0+\theta)(0+2\theta)\cdots(0+(\ell-1)\theta)(0+\ell\theta)} + \frac{e^{-\theta\cdot X}}{(-\theta+0)(-2\theta+\theta)\cdots(-\theta+(\ell-1)\theta)(-\theta+\ell\theta)}$$

$$+\ \frac{e^{-2\theta\cdot X}}{(-2\theta+0)(-2\theta+\theta)\cdots(-2\theta+\ell\theta)} + \ldots + \frac{e^{-\ell\theta\cdot X}}{(-\ell\theta+0)(-\ell\theta+\theta)\cdots(-\ell\theta+(\ell-1)\theta)}$$

$$= \frac{1}{\ell!\,\theta^\ell} - \frac{e^{-\theta X}}{1!\,(\ell-1)!\,\theta^\ell} + \frac{e^{-2\theta X}}{2!\,(\ell-2)!\,\theta^\ell} + \ldots \pm \frac{e^{-\ell\theta X}}{\ell!\,0!\,\theta^\ell} \;=\; \frac{(1-e^{-\theta X})^\ell}{\ell!\,\theta^\ell}$$

3. *Quadratic reciprocity and factorization of ζ-functions*

A different example (though connected to zeta functions and L-functions at a deeper level!) is Gauss' *Quadratic Reciprocity.*

[3.1] Fermat's two-squares theorem a prime number p is expressible as $p = a^2 + b^2$ if and only if $p = 1 \bmod 4$ (or $p = 2$):

Yes, one direction is easy: the squares mod 4 are $0, 1$. The ring of Gaussian integers $\mathbb{Z}[i]$ is *Euclidean*, so is a PID. The Galois norm N from $\mathbb{Q}(i)$ to $\mathbb{Q}$ is $N(a + bi) = a^2 + b^2$.

A prime is expressible as $p = (a + bi)(a - bi)$, if and only if it is *not* prime in $\mathbb{Z}[i]$, if and only if $\mathbb{Z}[i]/p\mathbb{Z}[i]$ is *not* an integral domain. Compute

$$\mathbb{Z}[i]/p \approx \big(\mathbb{Z}[x]/\langle x^2 + 1\rangle\big)/p \approx \big(\mathbb{Z}[x]/p\big)/\langle x^2 + 1\rangle \approx \mathbb{F}_p[x]/\langle x^2 + 1\rangle$$

The latter *is not* an integral domain if and only if there is a fourth root of unity $\sqrt{-1}$ in $\mathbb{F}_p$. Since $\mathbb{F}_p^\times$ is *cyclic*, presence of $\sqrt{-1}$ is equivalent to $p = 1 \bmod 4$ (or $p = 2$).

[3.2] When is 2 a square mod p? (for $p > 2$) $\mathbb{Z}[\sqrt{2}]$ is Euclidean, and the same argument as for Fermat's two-squares theorem shows that

$$p \;=\; a^2 - 2b^2 \qquad \Longleftrightarrow \qquad 2 \text{ is a square mod } p$$

A main feature of finite fields is the cyclic-ness of multiplicative groups, from which arises *Euler's criterion*

$$b \in \mathbb{F}_p^\times \text{ is a square} \qquad \Longleftrightarrow \qquad b^{\frac{p-1}{2}} = 1 \bmod p$$

Also, there is a handy connection between roots of unity and 2:

$$(1 + i)^2 \;=\; 2i \qquad \Longrightarrow \qquad 2 \;=\; -i(1 + i)^2$$

Computing in the ring $\mathbb{Z}[i]/p$ (!), using $\binom{p}{j} = 0$ for $0 < j < p$,

$$2^{\frac{p-1}{2}} \;=\; \big(-i(1+i)^2\big)^{\frac{p-1}{2}} \;=\; (-i)^{\frac{p-1}{2}} \frac{(1+i)^p}{1+i} \;=\; (-i)^{\frac{p-1}{2}} \frac{1+i^p}{1+i}$$

Quasi-astonishingly, this depends only on p mod 8, and

$$2 \text{ is a square mod } p \qquad \Longleftrightarrow \qquad p = \pm 1 \bmod 8$$

[3.3] When is q a square mod p, for odd primes $p \neq q$? Genuinely-amazingly, the answer depends only on p mod $4q$. The *quadratic symbol* is

$$\left(\frac{b}{p}\right)_2 = \begin{cases} 0 & \text{for } b = 0 \bmod p \\ 1 & \text{for } b \text{ nonzero square mod } p \\ -1 & \text{for } b \text{ nonzero non-square mod } p \end{cases}$$

Gauss' Law of Quadratic Reciprocity is

$$\left(\frac{q}{p}\right)_2 \cdot \left(\frac{p}{q}\right)_2 \;=\; (-1)^{\frac{(p-1)(q-1)}{4}}$$

This is arguably the historically-first non-trivial theorem in number theory.

Again, the cyclicness of $\mathbb{F}_p^\times$ shows that *exactly half* the non-zero things mod p are squares, and Euler's criterion

$$b \in \mathbb{F}_p^\times \text{ is a square} \quad \iff \quad b^{\frac{p-1}{2}} = 1 \bmod p$$

also shows that $b \to \left(\frac{b}{p}\right)_2$ is a *group homomorphism* $\mathbb{F}_p^\times \to \{\pm 1\}$. For brevity, write $\chi(b) = \left(\frac{b}{q}\right)_2$.

The surprise is that *every* prime q is expressible, *systematically* in terms of roots of unity. Fix a group homomorphism $\psi(b) = e^{2\pi i b/q}$ on the *additive* group of $\mathbb{F}_q$. The quadratic *Gauss sum* mod q is

$$g(\chi) \;=\; \sum_{b \bmod q} \chi(b) \cdot \psi(b)$$

Obviously, this is a weighted average of q^{th} roots of unity, with weights ± 1 (or 0). Such Gauss sums with more general *characters* χ on $\mathbb{F}_p^\times$ are useful, too, but we just want the quadratic character for now.

The Galois group of $\mathbb{Q}(e^{2\pi i/q})$ over $\mathbb{Q}$ is isomorphic to $\mathbb{Z}/q^\times$, and $\ell \in \mathbb{Z}/q^\times$ acts on q^{th} roots of unity by $\sigma_\ell : e^{2\pi i/q} \to e^{2\pi i \ell/q}$. Certainly the quadratic Gauss sum

$$g(\chi) \;=\; \sum_{b \bmod q} \chi(b) \cdot \psi(b)$$

lies in $\mathbb{Q}(e^{2\pi i/q})$. By a change of variables (replacing b by $\ell^{-1}b$),

$$\sigma_\ell\, g(\chi) \;=\; \sum_{b \bmod q} \chi(b) \cdot \psi(\ell b) \;=\; \sum_{b \bmod q} \chi(\ell^{-1}b) \cdot \psi(b) \;=\; \chi(\ell) \cdot \sum_{b \bmod q} \chi(b) \cdot \psi(b) \;=\; \chi(\ell) \cdot g(\chi)$$

With hindsight, since χ is multiplicative, this *equivariance* is really *designed into* the Gauss sum.

Then $\sigma_\ell\left(g(\chi)^2\right) = \chi(\ell)^2 \cdot g(\chi)^2 = g(\chi)^2$, so by Galois theory $g(\chi)^2 \in \mathbb{Q}$!?!?

[3.4] Claim: $g(\chi)^2 = q \cdot (-1)^{q-1}$ Compute directly, keeping track of the trick that $\chi(0) = 0$:

$$g(\chi)^2 \;=\; \sum_{a \neq 0, b \neq 0} \chi(a)\, \chi(b)\, \psi(a+b) \;=\; \sum_{a \neq 0, b \neq 0} \chi(ab)\, \chi(b)\, \psi(ab+b)$$

$$= \sum_{a \neq 0, b \neq 0} \chi(a)\, \psi((a+1)b) \;=\; \sum_{a \neq 0, -1,\; b \neq 0} \chi(a)\, \psi((a+1)b) + \chi(-1) \sum_{b \neq 0} 1$$

To simplify all this, use the *Cancellation Lemma:* for $\alpha : H \to \mathbb{C}^\times$ a group homorphism from a finite group H to $\mathbb{C}^\times$,

$$\sum_{h \in H} \alpha(h) \;=\; \begin{cases} |H| & \text{for } \alpha \text{ identically } 1 \\ 0 & \text{for } \alpha \textit{ not } \text{identically } 1 \end{cases}$$

Proven by change-of-variables: for α not trivial, let $\alpha(h_o) \neq 1$, and

$$\sum_{h \in H} \alpha(h) \;=\; \sum_{h \in H} \alpha(h h_o) \;=\; \alpha(h_o) \sum_{h \in H} \alpha(h)$$

So $(1 - \alpha(h_o)) \sum_{h \in H} \alpha(h) = 0$. ///

Thus, since $b \to \psi(c \cdot b)$ is a group hom $\mathbb{F}_q$ to $\mathbb{C}^\times$, non-trivial for $c \in \mathbb{F}_q^\times$, for $a + 1 \neq 0$, we can evaluate inner sums over b:

$$\sum_{b \neq 0} \psi((a+1)b) \;=\; \sum_{\text{all } b} \psi((a+1)b) - \psi((a+1)0) \;=\; 0 - 1 \;=\; -1$$

Thus,

$$\sum_{a\neq 0,-1,\, b\neq 0} \chi(a)\,\psi((a+1)b) \;+\; \chi(-1)\sum_{b\neq 0} 1 \;=\; \sum_{a\neq 0,-1} \chi(a)\cdot(-1) \;+\; \chi(-1)\cdot(q-1)$$

$$= -\sum_{a\neq 0}\chi(a) + \chi(-1) + \chi(-1)\cdot(q-1) \;=\; 0 + \chi(-1)q \;=\; \chi(-1)q$$

That is, $g(\chi)^2 = \chi(-1)q$. ///

Using $g(\chi)^2 = \chi(-1)q$ and plugging into Euler's criterion: computing mod p in $\mathbb{Z}[e^{2\pi i/q}]$, noting that apparently q and $g(\chi)$ are invertible there (!),

$$\begin{pmatrix} q \\ p \end{pmatrix}_2 \;=\; q^{\frac{p-1}{2}} \;=\; \big((-1)^{\frac{q-1}{2}}\cdot g(\chi)^2\big)^{\frac{p-1}{2}} \;=\; (-1)^{\frac{(p-1)(q-1)}{4}}\cdot\frac{g(\chi)^p}{g(\chi)}$$

Again using $\binom{p}{j} = 0 \bmod p$ for $0<j<p$,

$$g(\chi)^p \;=\; \sum_{b \bmod q} \chi(b)^p\cdot\psi(p\cdot b) \;=\; \sum_{b \bmod q}\chi(b)\cdot\psi(p\cdot b) \;=\; \sum_{b \bmod q}\chi(bp^{-1})\cdot\psi(b) \;=\; \begin{pmatrix} p \\ q \end{pmatrix}_2 \cdot g(\chi) \bmod p$$

Thus, in $\mathbb{Z}[e^{2\pi i/q}]$ mod p,

$$\begin{pmatrix} q \\ p \end{pmatrix}_2 \;=\; (-1)^{\frac{(p-1)(q-1)}{4}}\cdot\frac{g(\chi)^p}{g(\chi)} \;=\; (-1)^{\frac{(p-1)(q-1)}{4}}\cdot\frac{\binom{p}{q}_2\cdot g(\chi)}{g(\chi)} \;=\; (-1)^{\frac{(p-1)(q-1)}{4}}\cdot\begin{pmatrix} p \\ q \end{pmatrix}_2$$

Since these values are ± 1, their equality in $\mathbb{Z}[e^{2\pi i/q}]$ mod p for $p>2$ gives their equality as numbers in $\{\pm 1\}$, proving the main part of Quadratic Reciprocity. ///

[3.5] Factorization of Dedekind zeta functions

As noted earlier, Dirichlet's 1837 theorem on primes in arithmetic progressions $a+\ell N$ needs a *non-vanishing* result for L-functions, namely, $L(1,\chi)\neq 0$ for Dirichlet characters χ mod N.

Dirichlet proved this in simple cases by showing that these L-functions are factors in *Dedekind zeta functions* $\zeta_{\mathfrak{o}}(s)$ of rings of integers $\mathfrak{o}=\mathbb{Z}[\omega]$ with ω an N^{th} root of unity, and using simple properties of the zeta functions $\zeta_{\mathfrak{o}}(s)$.

To describe Dedekind zetas, for an ideal $\mathfrak{a}$ of suitable $\mathfrak{o}$, let the *ideal norm* be $N\mathfrak{a} = \mathrm{card}(\mathfrak{o}/\mathfrak{a})$. Then

$$\zeta_{\mathfrak{o}}(s) \;=\; \sum_{\mathfrak{a}\neq 0}\frac{1}{(N\mathfrak{a})^s}$$

In suitable $\mathfrak{o}$, every non-zero ideal factors uniquely into *prime ideals* (not necessarily prime *numbers*) (one says these are *Dedekind domains*), so the zeta function has an Euler product

$$\zeta_{\mathfrak{o}}(s) \;=\; \sum_{\mathfrak{a}\neq 0}\frac{1}{(N\mathfrak{a})^s} \;=\; \prod_{\mathfrak{p}\text{ prime}}\frac{1}{1-N\mathfrak{p}^{-s}} \qquad (\text{for } \mathrm{Re}(s)>1)$$

For $\mathfrak{o}=\mathbb{Z}[\omega]$, the factorization is equivalent to understanding the behavior of rational primes in the extension ring $\mathbb{Z}[\omega]$ of $\mathbb{Z}$: do they *stay prime*, or do they *factor* as products of primes in $\mathbb{Z}[\omega]$?

Letting ω be a primitive q^{th} root of unity for q prime, and Φ_q the q^{th} cyclotomic polynomial,

$$\mathbb{Z}[\omega]/p \;\approx\; \big(\mathbb{Z}[x]/\Phi_q\big)/p \;\approx\; \big(\mathbb{Z}[x]/p\big)/\Phi_q \;\approx\; \mathbb{F}_p[x]/\Phi_q \;\approx\; \mathbb{F}_p[x]/\varphi_1\oplus\ldots\oplus\mathbb{F}_p[x]/\varphi_m$$

where φ_i are irreducible factors of Φ_q in $\mathbb{F}_p[x]$.

On the other hand, assuming the Dedekind-domain property, and that $p = \mathfrak{P}_1 \ldots \mathfrak{P}_n$ with distinct $\mathfrak{P}_i$, then by Sun-Ze's theorem

$$\mathbb{Z}[\omega]/p \;\approx\; \mathbb{Z}[\omega]/\mathfrak{P}_1 \oplus \ldots \oplus \mathbb{Z}[\omega]/\mathfrak{P}_n$$

Thus,

$$\mathbb{F}_p[x]/\varphi_1 \oplus \ldots \oplus \mathbb{F}_p[x]/\varphi_m \;\approx\; \mathbb{Z}[\omega]/\mathfrak{P}_1 \oplus \ldots \oplus \mathbb{Z}[\omega]/\mathfrak{P}_n$$

A factorization of a zeta function of an extension as a product of Dirichlet L-functions of the base ring is a type of **reciprocity law**. The first reciprocity law was *quadratic reciprocity*, conjectured by Legendre and Gauss, and proven by Gauss in 1799. In the mid-19th century, Eisenstein proved *cubic* and *quartic* reciprocity. About 1928, Takagi and Artin proved a general reciprocity law, called *classfield theory*, for *abelian* field extensions. In the late 1960's, Langlands formulated conjectures including reciprocity laws for *non-abelian* extensions.

Since the rings $\mathbb{Z}[\omega]$ are rarely principal ideal domains, examples where the rings involved *are* principal ideal domains are best at first.

The easiest proofs of PID-ness are by Euclidean-ness.

[3.6] Gaussian integers $\mathfrak{o} = \mathbb{Z}[i]$

Let $\sigma : \mathbb{Q}(i) \to \mathbb{Q}(i)$ be the non-trivial automorphism

$$\sigma \;:\; a + bi \;\longrightarrow\; a - bi \qquad\qquad (\text{with } a, b \in \mathbb{Q})$$

The automorphism σ stabilizes $\mathfrak{o}$. Let $N : \mathbb{Q}(i) \to \mathbb{Q}$ be the *norm*

$$N(a+bi) \;=\; (a+bi)\cdot(a+bi)^\sigma \;=\; (a+bi)(a-bi) \;=\; a^2 + b^2$$

The norm maps $\mathbb{Q}(i) \to \mathbb{Q}$, and $\mathfrak{o} \to \mathbb{Z}$. Since σ is a field automorphism, the norm is *multiplicative*:

$$N(\alpha\beta) \;=\; (\alpha\beta)\cdot(\alpha\beta)^\sigma \;=\; \alpha\alpha^\sigma \cdot \beta\beta^\sigma \;=\; N\alpha \cdot N\beta$$

Units $\mathfrak{o}^\times$ For $\alpha\beta = 1$ in $\mathfrak{o}$, taking norms gives $N\alpha \cdot N\beta = 1$. Since the norm maps $\mathfrak{o} \to \mathbb{Z}$, $N\alpha = \pm 1$. Since the norm is of the form $a^2 + b^2$, it must be 1. That is, the norm of a unit in the Gaussian integers is 1. It is easy to determine all the units: solve $a^2 + b^2 = 1$ for integers a, b, finding the four units

$$\mathfrak{o}^\times \;=\; \{1,\, -1,\, i,\, -i\}$$

Euclidean-ness We claim that the Gaussian integers $\mathfrak{o}$ form a *Euclidean* ring: given α, β in $\mathfrak{o}$ with $\beta \neq 0$, we can divide α by β with an integer remainder *smaller* than β. That is, given α, β with $\beta \neq 0$, there is $q \in \mathfrak{o}$ such that

$$N(\alpha - q\cdot\beta) \;<\; N\beta \qquad\qquad (\text{given } \alpha, \beta \neq 0, \text{ for some } q \in \mathfrak{o})$$

The inequality is equivalent to the inequality obtained by dividing through by $N\beta$, using the multiplicativity:

$$N(\frac{\alpha}{\beta} - q) \;<\; N(1) \;=\; 1$$

That is, given $\gamma = \alpha/\beta \in \mathbb{Q}(i)$, there should be $q \in \mathfrak{o}$ such that $N(\gamma - q) < 1$. Indeed, let $\gamma = a + bi$ with $a, b \in \mathbb{Q}$, and let $a', b' \in \mathbb{Z}$ be the closest integers to a, b, respectively. (If a or b falls exactly half-way between integers, choose either.) Then $|a - a'| \le \frac{1}{2}$ and $|b - b'| \le \frac{1}{2}$, and

$$N(\gamma - q) \;=\; (a-a')^2 + (b-b')^2 \;\le\; (\tfrac{1}{2})^2 + (\tfrac{1}{2})^2 \;=\; \tfrac{1}{4} + \tfrac{1}{4} \;<\; 1$$

This proves the Euclidean-ness, and PID-ness, and UFD-ness.

Behavior of primes in the extension $\mathbb{Z}[i]$ of $\mathbb{Z}$ Prime numbers p in $\mathbb{Z}$, which we'll call *rational primes* to distinguish them, do not usually *stay prime* in larger rings. For example, the prime 5 factors:

$$5 \;=\; (2+i)\cdot(2-i)$$

The norms of $2\pm i$ are both 5, so these are not units.

Expanding on the two-squares theorem:

[3.7] Theorem: A rational prime p stays prime in $\mathbb{Z}[i]$ if and only if $p = 3 \bmod 4$. A rational prime $p = 1 \bmod 4$ factors as $p = p_1 p_2$ with distinct primes p_i. The rational prime 2 *ramifies*, in the sense that $2 = (1+i)(1-i)$ and $1+i$ and $1-i$ differ by a unit.

Terminology: Primes that *stay* prime are *inert*, and primes that *factor* (with no factor repeating) are *split*. A prime that factors and has *repeated factors* is *ramified*.

Proof: The case of 2 is clear. An ideal I in a commutative ring R is *prime* if and only if R/I is an *integral domain*. Again,

$$\mathbb{Z}[i]/\langle p\rangle \;\approx\; \mathbb{Z}[x]/\langle x^2+1, p\rangle \;\approx\; \Big(\mathbb{Z}[x]/\langle p\rangle\Big)/\langle x^2+1\rangle \;\approx\; \mathbb{F}_p[x]/\langle x^2+1\rangle$$

This is a quadratic field extension of $\mathbb{F}_p$ if and only if x^2+1 is irreducible in $\mathbb{F}_p$. For odd p, this happens if and only if there is *no* primitive fourth root of unity in $\mathbb{F}_p$. Since $\mathbb{F}_p^\times$ is cyclic of order $p-1$, there is a primitive fourth root of unity in $\mathbb{F}_p$ if and only if $4|p-1$. That is, if $p = 3 \bmod 4$, x^2+1 is irreducible in $\mathbb{F}_p$, and p stays prime in $\mathbb{Z}[i]$.

When $p = 1 \bmod 4$, $\mathbb{F}_p$ contains primitive fourth roots of unity, so there are $\alpha, \beta \in \mathbb{F}_p$ such that $x^2+1 = (x-\alpha)(x-\beta)$. The derivative of x^2+1 is $2x$, and 2 is invertible mod p, so $\gcd(x^2+1, 2x) = 1$ in $\mathbb{F}_p[x]$. Thus, $\alpha \neq \beta$. Thus, by Sun-Ze's theorem

$$\mathbb{Z}[i]/\langle p\rangle \;\approx\; \frac{\mathbb{F}_p[x]}{\langle x^2+1\rangle} \;\approx\; \frac{\mathbb{F}_p[x]}{\langle x-\alpha\rangle} \times \frac{\mathbb{F}_p[x]}{\langle x-\beta\rangle} \;\approx\; \mathbb{F}_p \times \mathbb{F}_p$$

So far, for split p, and for ρ a $\sqrt{-1}$ in $\mathbb{F}_p$,

$$\mathbb{Z}[i]/p \approx \mathbb{F}_p[x]/\langle x^2+1\rangle \approx \mathbb{F}_p[x]/\langle x-\rho\rangle \oplus \mathbb{F}_p[x]/\langle x+\rho\rangle$$

By the cyclic-ness of $\mathbb{F}_p^\times$, p has a $\sqrt{-1}$ exactly when $p = 1 \bmod 4$. That is, $p = 1 \bmod 4$ is *split*, specifically, $p\cdot\mathbb{Z}[i]$ is of the form $p_1p_2\cdot\mathbb{Z}[i]$ for *distinct* (non-associate) prime elements p_i of $\mathbb{Z}[i]$.

[3.8] Lemma: For an ideal I in a PID R, suppose there is an isomorphism

$$\varphi \;:\; R \longrightarrow R/I \;\approx\; D_1 \times D_2$$

to a product of integral domains D_i (with $0 \neq 1$ in each). Then $I = \ker\varphi$ is generated by a product p_1p_2 of two distinct (non-associate) prime elements p_i.

Proof: In a *principal* ideal domain, every non-zero prime ideal is *maximal*. Let φ_i be the further composition of φ with the projection to D_i. Then $\ker\varphi_i$ of $\varphi_i : R \to D_i$ is a prime ideal containing I, and

$$\ker\varphi \;=\; \ker\varphi_1 \cap \ker\varphi_2$$

$\ker\varphi_1 \neq \ker\varphi_2$, or else $I = \ker\varphi_1 = \ker\varphi_2$ would already be prime, and R/I would be an integral domain, not a product. Let $\ker\varphi_i = p_i \cdot R$ for non-associate prime elements p_1, p_2 of R. Then

$$I \;=\; p_1R \cap p_2R \;=\; \{r \in R \;:\; r = a_1p_1 = a_2p_2 \text{ for some } a_1, a_2 \in R\}$$

p_1 and p_2 are distinct, so $p_2|a_1$ and $p_1|a_2$, and $I = p_1p_2 \cdot R$. ///

Description of behaviors in an extension, in terms of behavior in the ground ring, is a *reciprocity law.*

Quadratic symbol as Dirichlet character: conductor The *quadratic symbol* that tells whether or not -1 is a square mod p is

$$\left(\frac{-1}{p}\right)_2 = \left\{\begin{array}{ll} 0 & (p=2) \\ \\ +1 & (\text{when } -1 \text{ is a square mod } p) \\ \\ -1 & (\text{when } -1 \text{ is not a square mod } p) \end{array}\right\} \quad (\text{prime } p)$$

This quadratic symbol is determined by p mod 4. That is, the *conductor* of this symbol is 4. That is, this quadratic symbol is a *Dirichlet character* mod 4:

$$\left(\frac{-1}{p}\right)_2 = \begin{cases} 0 & (p=2) \\ \\ +1 & (\text{when } p = 1 \bmod 4) \\ \\ -1 & (\text{when } p = 3 \bmod 4) \end{cases}$$

Factoring $\zeta_{\mathbb{Z}[i]}(s)$ The zeta function of $\mathfrak{o} = \mathbb{Z}[i]$ is a sum over non-zero elements of $\mathfrak{o}$ modulo units: (note that the *ideal* norm is expressible in terms of the *Galois* norm here)

$$\zeta_{\mathfrak{o}}(s) = \sum_{0 \neq \alpha \in \mathfrak{o} \bmod \mathfrak{o}^\times} \frac{1}{|N\alpha|^s} \qquad (\text{Galois norm})$$

Since $|\mathfrak{o}^\times| = 4$, this is also

$$\zeta_{\mathfrak{o}}(s) = \frac{1}{4}\sum_{0 \neq \alpha \in \mathfrak{o}} \frac{1}{(N\alpha)^s} = \frac{1}{4}\sum_{m,n\in\mathbb{Z} \text{ not both } 0} \frac{1}{(m^2+n^2)^s}$$

Easy estimates prove convergence for $\mathrm{Re}(s) > 1$. As in the Euler factorization of $\zeta_{\mathbb{Z}}(s)$, unique factorization in $\mathfrak{o} = \mathbb{Z}[i]$ gives

$$\zeta_{\mathfrak{o}}(s) = \prod_{\text{primes } \pi \bmod \mathfrak{o}^\times} \frac{1}{1 - \frac{1}{|N\pi|^s}} \qquad (\text{for } \mathrm{Re}(s) > 1)$$

With $\chi(p) = \left(\frac{-1}{p}\right)_2$, we claim a factorization

$$\zeta_{\mathfrak{o}}(s) = \zeta_{\mathbb{Z}}(s) \cdot L(s,\chi)$$

To this end, group the Euler factors according to the rational primes the Gaussian prime divides:

$$\zeta_{\mathfrak{o}}(s) = \prod_{\text{rational } p} \prod_{\pi|p} \frac{1}{1 - \frac{1}{|N\pi|^s}}$$

The prime $p = 2$ is *ramified*: $\pi = 1+i$ is the unique prime dividing 2, and $2 = (1+i)^2/i$. Since $\chi(2) = 0$,

$$\prod_{\pi|2} \frac{1}{1 - \frac{1}{|N\pi|^s}} = \frac{1}{1 - \frac{1}{|N(1+i)|^s}} = \frac{1}{1 - \frac{1}{2^s}} = \frac{1}{1 - \frac{1}{2^s}} \cdot 1$$

$$= \quad 2^{th} \text{ factor of } \zeta_{\mathbb{Z}}(s) \times 2^{th} \text{ factor of } L(s,\chi)$$

Primes $p = 3 \bmod 4$ stay prime in $\mathfrak{o}$, and $\chi(p) = -1$, so

$$\prod_{\pi|p} \frac{1}{1 - \frac{1}{|N\pi|^s}} \;=\; \frac{1}{1 - \frac{1}{|Np|^s}} \;=\; \frac{1}{1 - \frac{1}{p^{2s}}} \;=\; \frac{1}{1 - \frac{1}{p^s}} \times \frac{1}{1 + \frac{1}{p^s}}$$

$$= \frac{1}{1 - \frac{1}{p^s}} \cdot \frac{1}{1 - \frac{\chi(p)}{p^s}} \;=\; p^{th} \text{ factor of } \zeta_(s) \;\times\; p^{th} \text{ factor of } L(s,\chi)$$

Primes $p = 1 \bmod 4$ factor as $p = p_1 p_2$, and $\chi(p) = +1$. Note that $p^2 = Np = Np_1 \cdot Np_2$, so since the p_i are not units, $Np_i = p$. Then

$$\prod_{\pi|p} \frac{1}{1 - \frac{1}{|N\pi|^s}} \;=\; \frac{1}{1 - \frac{1}{|Np_1|^s}} \times \frac{1}{1 - \frac{1}{|Np_2|^s}} \;=\; \frac{1}{1 - \frac{1}{p^s}} \times \frac{1}{1 - \frac{1}{p^s}}$$

$$= \frac{1}{1 - \frac{1}{p^s}} \cdot \frac{1}{1 - \frac{\chi(p)}{p^s}} = p^{th} \text{ factor of } \zeta_{\mathbb{Z}}(s) \;\times\; p^{th} \text{ factor of } L(s,\chi)$$

Putting this together, $\zeta_{\mathfrak{o}}(s) \;=\; \zeta_{\mathbb{Z}}(s) \cdot L(s,\chi)$.

[3.9] Example: extension $\mathbb{Z}[\sqrt{2}]$ of $\mathbb{Z}$ A little work shows that the ring $\mathfrak{o} = \mathbb{Z}[\sqrt{2}]$ is *Euclidean*, so a *PID*.

The group of units $\mathfrak{o}^\times$ is highly non-trivial: it has non-torsion element $1 + \sqrt{2}$. In fact, $\mathfrak{o}^\times$ is generated by $1 + \sqrt{2}$ and -1.

[3.10] Theorem: A rational prime p stays prime in $\mathfrak{o} = \mathbb{Z}[\sqrt{2}]$ if and only if $p = 3, 5 \bmod 8$. A rational prime $p = \pm 1 \bmod 8$ factors as $p = p_1 p_2$ with distinct primes p_i. The rational prime 2 *ramifies*, in the sense that $2 = (\sqrt{2})^2$.

Proof: The $p = 2$ case is clear. With $p > 2$,

$$\mathfrak{o}/p \;=\; \mathbb{Z}[\sqrt{2}]/p \;\approx\; \mathbb{Z}[x]/\langle x^2 - 2, p\rangle \;\approx\; \mathbb{F}_p[x]/\langle x^2 - 2\rangle$$

When 2 is a non-square mod p, $x^2 - 2$ is irreducible in $\mathbb{F}_p[x]$, and $\mathfrak{o}/p$ is a field, so p is prime. When 2 is a square mod $p > 2$, there are two *distinct* square roots ρ_1, ρ_2, and by Sun-Ze's theorem

$$\mathbb{F}_p[x]/\langle x^2 - 2\rangle \;\approx\; \mathbb{F}_p[x]/\langle x - \rho_1\rangle \oplus \mathbb{F}_p[x]/\langle x - \rho_2\rangle$$

The earlier Lemma shows that p factors in $\mathfrak{o}$ as a product of two distinct (non-associate) primes, so p *splits.* ///

In fact, taking any representatives ρ in $\mathbb{Z}$ for a square root of 2 mod p, the isomorphism shows that the *pairs* $p, \rho - \sqrt{2}$ and $p, \rho + \sqrt{2}$ generate the two prime ideals into which $p \cdot \mathfrak{o}$ factors.

Group the Euler factors of the Dedekind zeta function for $\mathfrak{o} = \mathbb{Z}[\sqrt{2}]$ by rational primes:

$$\zeta_{\mathfrak{o}}(s) \;=\; \prod_p \Big(\prod_{\pi|p} \frac{1}{1 - |N\pi|^{-s}} \Big) \;=\; (\text{ramified}) \cdot (\text{split}) \cdot (\text{inert})$$

The only ramified prime is 2. Split primes are $p = \pm 1 \bmod 8$, and $p = \pi_1 \cdot \pi_2$ implies

$$p^2 \;=\; Np \;=\; N\pi_1 \cdot N\pi_2$$

so the norms of any two prime factors are p. Inert primes are $p = 3, 5 \bmod 8$, they remain prime in $\mathfrak{o}$, and $Np = p^2$. Thus,

$$\zeta_{\mathfrak{o}}(s) \quad = \quad \prod_{\pi|2} \frac{1}{1-|N\pi|^{-s}} \times \prod_{p=\pi_1\pi_2} \frac{1}{1-|N\pi_1|^{-s}} \cdot \frac{1}{1-|N\pi_2|^{-s}} \times \prod_{p=3,5 \bmod 8} \frac{1}{1-|Np|^{-s}}$$

With $\chi(p) = \left(\frac{2}{p}\right)_2$, this is

$$\zeta_{\mathfrak{o}}(s) \; = \; \frac{1}{1-2^{-s}} \times \prod_{p=\pm 1 \bmod 8} \frac{1}{1-p^{-s}} \cdot \frac{1}{1-p^{-s}} \times \prod_{p=3,5 \bmod 8} \frac{1}{1-p^{-s}} \cdot \frac{1}{1+p^{-s}}$$

$$= \; \prod_p \frac{1}{1-p^{-s}} \cdot \frac{1}{1-\chi(p)p^{-s}} \; = \; \zeta(s) \cdot L(s,\chi)$$

Continuing: *factorization* of Dedekind zeta-functions into Dirichlet L-functions, equivalently, *behavior of primes in extensions.* So far,

$$\zeta_{\mathbb{Z}[i]}(s) \; = \; \zeta(s) \cdot L(s,\chi) \qquad \chi(p) = \left(\frac{-1}{p}\right)_2$$

$$\zeta_{\mathbb{Z}[\sqrt{2}]}(s) \; = \; \zeta(s) \cdot L(s,\chi) \qquad \chi(p) = \left(\frac{2}{p}\right)_2$$

$$\zeta_{\mathbb{Z}[\sqrt{-2}]}(s) \; = \; \zeta(s) \cdot L(s,\chi) \qquad \chi(p) = \left(\frac{-2}{p}\right)_2$$

Next, $\mathbb{Z}[\omega]$ with ω an eighth root of unity. First, look at the eighth cyclotomic polynomial x^4+1.

[3.11] Remark: The change of variables $x \to x+1$ gives $x^4+4x^3+6x^2+4x+2$, so *Eisenstein's criterion and Gauss' Lemma* prove irreducibility of x^4+1 in $\mathbb{Q}[x]$.

A peculiar feature of the polynomial x^4+1:

[3.12] Claim: x^4+1 is *reducible* modulo every prime p. $p=2$ is easy. For $p>2$, for $x^4+1=0$ to have a root in $\mathbb{F}_p$ requires existence of an element of order 8 in $\mathbb{F}_p^\times$, so $8|p-1$, and $p=1 \bmod 8$. For $x^4+1=0$ to have a root in $\mathbb{F}_{p^2}$ requires existence of an element of order 8 in $\mathbb{F}_{p^2}\times$, so $8|p^2-1$.

Interestingly-enough, $\mathbb{Z}/8^\times$ is not cyclic, but is isomorphic to $\mathbb{Z}/2 \oplus \mathbb{Z}/2$. Thus, $p^2 = 1 \bmod 8$ for all odd p. That is, at worst, $x^4+1=0$ has a root in $\mathbb{F}_{p^2}$ for all odd p. ///

Comment For f a monic polynomial in $\mathbb{Z}[x]$ irreducibility of its image in $\mathbb{F}_p[x]$ certainly implies its irreducibility in $\mathbb{Z}[x]$. We might hope that there'd be a sort of converse, namely, that irreducible monics in $\mathbb{Z}[x]$ would be irreducible mod *some* prime p... but x^4+1 is a counter-example.

[3.13] Example: eighth roots of unity. Let $\omega = \frac{1+i}{\sqrt{2}}$ be a primitive eighth root of unity, and $\mathfrak{o} = \mathbb{Z}[\omega]$. The non-trivial characters mod 8 are $\left(\frac{-1}{p}\right)_2$, $\left(\frac{2}{p}\right)_2$, and $\left(\frac{-2}{p}\right)_2$.

[3.14] Claim:

$$\zeta_{\mathfrak{o}}(s) \; = \; \zeta(s) \cdot L(s, \left(\tfrac{-1}{p}\right)) \cdot L(s, \left(\tfrac{2}{p}\right)) \cdot L(s, \left(\tfrac{-2}{p}\right))$$

Without determining whether $\mathfrak{o}$ is a PID, or what its units are, if/when it becomes necessary, let's be willing to grant that it is a *Dedekind domain*, in that *every non-zero ideal factors uniquely into prime ideals.*

By Euler's criterion, computing mod p,

$$\left(\frac{-2}{p}\right)_2 \; = \; (-2)^{\frac{p-1}{2}} \; = \; (-1)^{\frac{p-1}{2}} \cdot 2^{\frac{p-1}{2}} \; = \; \left(\frac{-1}{p}\right)_2 \cdot \left(\frac{2}{p}\right)_2$$

The characters of $\mathbb{Z}/8^\times$

$p\backslash\chi$	triv	$\left(\frac{-1}{*}\right)$	$\left(\frac{2}{*}\right)$	$\left(\frac{-2}{*}\right)$
1 mod 8	1	1	1	1
3 mod 8	1	-1	-1	1
5 mod 8	1	1	-1	-1
7 mod 8	1	-1	1	-1

For $3, 5, 7$ there are exactly two -1's in each row.

As earlier, for rational prime $p > 2$,

$$\mathfrak{o}/p \;\approx\; \mathbb{Z}[x]/\langle x^4+1, p\rangle \;\approx\; \mathbb{F}_p[x]/\langle x^4+1\rangle \;\approx\; \begin{cases} \mathbb{F}_p \oplus \mathbb{F}_p \oplus \mathbb{F}_p \oplus \mathbb{F}_p & (\text{for } p = 1 \bmod 8) \\ \\ \mathbb{F}_{p^2} \oplus \mathbb{F}_{p^2} & (\text{for } p = 3, 5, 7 \bmod 8) \end{cases}$$

Observe: Prime splitting determined by congruence conditions!!!

Since $x^4 + 1 = (x+1)^4 \bmod 2$, for $p = 2$ something more complicated happens:

$$\mathbb{F}_2[x]/(x+1)^4 \;\neq\; \text{product of fields}$$

Indeed, we already saw that, in the PIDs $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{2}]$, inside the intermediate fields, 2 is *ramified.* A little later we'll have means to see that the above computation implies 2 is *totally ramified* in the extension $\mathfrak{o} = \mathbb{Z}[\omega]$ of $\mathbb{Z}$, namely, $2\mathfrak{o} = \mathfrak{p}^4$.

Write $\chi_D(p) = \left(\dfrac{D}{p}\right)_2$ for $D = -1, 2, -2$. For $p = 1 \bmod 8$, applying the ideal norm to $p\mathfrak{o} = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$ gives $N\mathfrak{p}_i = p$, so

$$\prod_{\mathfrak{p}|p} \frac{1}{1 - N\mathfrak{p}^{-s}} \;=\; \Big(\frac{1}{1-p^{-s}}\Big)^4 \;=\; \frac{1}{1 - \dfrac{1}{p^s}} \cdot \frac{1}{1 - \dfrac{\chi_{-1}(p)}{p^s}} \cdot \frac{1}{1 - \dfrac{\chi_2(p)}{p^s}} \cdot \frac{1}{1 - \dfrac{\chi_{-2}(p)}{p^s}}$$

$$=\; \text{Euler } p\text{-factors from } \zeta(s),\ L(s,\chi_{-1}),\ L(s,\chi_2),\ L(s,\chi_{-2})$$

For $p = 3, 5, 7 \bmod 8$, $p\mathfrak{o} = \mathfrak{p}_1\mathfrak{p}_2$ gives $N\mathfrak{p}_i = p^2$, so

$$\prod_{\mathfrak{p}|p} \frac{1}{1 - N\mathfrak{p}^{-s}} \;=\; \Big(\frac{1}{1-p^{-2s}}\Big)^2 \;=\; \frac{1}{1 - \dfrac{1}{p^s}} \cdot \frac{1}{1 + \dfrac{1}{p^s}} \cdot \frac{1}{1 - \dfrac{1}{p^s}} \cdot \frac{1}{1 + \dfrac{1}{p^s}} \qquad (\text{in } \textit{some} \text{ order!?!})$$

$$=\; \frac{1}{1 - \dfrac{1}{p^s}} \cdot \frac{1}{1 - \dfrac{\chi_{-1}(p)}{p^s}} \cdot \frac{1}{1 - \dfrac{\chi_2(p)}{p^s}} \cdot \frac{1}{1 - \dfrac{\chi_{-2}(p)}{p^s}} \qquad (\text{order?})$$

$$=\; \text{Euler } p\text{-factors from } \zeta(s),\ L(s,\chi_{-1}),\ L(s,\chi_2),\ L(s,\chi_{-2})$$

We *could* have treated $p = 3, 5, 7$ separately, tracking *which* two-out-of-three characters took values -1, but this would not have accomplished much. Except for the Euler 2-factors, we've proven

$$\zeta_{\mathfrak{o}}(s) \;=\; \zeta(s) \cdot L(s, \left(\tfrac{-1}{p}\right)) \cdot L(s, \left(\tfrac{2}{p}\right)) \cdot L(s, \left(\tfrac{-2}{p}\right))$$

[3.15] Example: fifth roots of unity. Let ω be a primitive fifth root of unity, and $\mathfrak{o} = \mathbb{Z}[\omega]$. The group $\mathbb{Z}/5^\times$ has four characters: the trivial one, an order-two character χ_2, and two order-four characters χ_1, χ_3. (**Note:** This indexing is incompatible with earlier...)

[3.16] Claim:

$$\zeta_{\mathfrak{o}}(s) \;=\; \zeta(s) \cdot L(s,\chi_1) \cdot L(s,\chi_2) \cdot L(s,\chi_3)$$

Without determining whether $\mathfrak{o}$ is a PID, or what its units are, if necessary, grant that it is a *Dedekind domain*, ...

As earlier, for rational prime p, with $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$ the fifth cyclotomic polynomial,

$$\mathfrak{o}/p \;\approx\; \mathbb{Z}[x]/\langle \Phi_5, p\rangle \;\approx\; \mathbb{F}_p[x]/\langle \Phi_5\rangle \;\approx\; \begin{cases} \mathbb{F}_p \oplus \mathbb{F}_p \oplus \mathbb{F}_p \oplus \mathbb{F}_p & (\text{for } 5|p-1) \\ \mathbb{F}_{p^2} \oplus \mathbb{F}_{p^2} & (\text{for } 5|p^2-1 \text{ but } 5 \not| p-1) \\ \mathbb{F}_{p^4} & (\text{for } 5|p^4-1 \text{ but } 5 \not| p^2-1) \end{cases}$$

$$\approx \begin{cases} \mathbb{F}_p \oplus \mathbb{F}_p \oplus \mathbb{F}_p \oplus \mathbb{F}_p & (\text{for } p = 1 \bmod 5) \\ \mathbb{F}_{p^2} \oplus \mathbb{F}_{p^2} & (\text{for } p = -1 \bmod 5) \\ \mathbb{F}_{p^4} & (\text{for } p = 2,3 \bmod 5) \end{cases}$$

Observe: Prime splitting determined by congruence conditions!!! For p splitting completely $p\mathfrak{o} = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$, norms are $N\mathfrak{p}_i = p$, and

$$\prod_{\mathfrak{p}|p} \frac{1}{1 - N\mathfrak{p}^{-s}} \;=\; \Big(\frac{1}{1-p^{-s}}\Big)^4 \;=\; \frac{1}{1-\dfrac{1}{p^s}} \cdot \frac{1}{1-\dfrac{\chi_1(p)}{p^s}} \cdot \frac{1}{1-\dfrac{\chi_2(p)}{p^s}} \cdot \frac{1}{1-\dfrac{\chi_3(p)}{p^s}}$$

$$= \text{ Euler } p\text{-factors from } \zeta(s),\ L(s,\chi_1),\ L(s,\chi_2),\ L(s,\chi_3)$$

For p splitting *half-way* $p\mathfrak{o} = \mathfrak{p}_1\mathfrak{p}_2$, norms are $N\mathfrak{p}_i = p^2$, and

$$\prod_{\mathfrak{p}|p} \frac{1}{1 - N\mathfrak{p}^{-s}} \;=\; \Big(\frac{1}{1-p^{-2s}}\Big)^2 \;=\; \frac{1}{1-\dfrac{1}{p^s}} \cdot \frac{1}{1-\dfrac{1}{p^s}} \cdot \frac{1}{1+\dfrac{1}{p^s}} \cdot \frac{1}{1+\dfrac{1}{p^s}}$$

$$= \frac{1}{1-\dfrac{1}{p^s}} \cdot \frac{1}{1-\dfrac{\chi_2(p)}{p^s}} \cdot \frac{1}{1-\dfrac{\chi_1(p)}{p^s}} \cdot \frac{1}{1-\dfrac{\chi_3(p)}{p^s}}$$

$$= \text{ Euler } p\text{-factors from } \zeta(s),\ L(s,\chi_2),\ L(s,\chi_1),\ L(s,\chi_3)$$

... in that order, except that we can't distinguish the order-four characters χ_1,χ_3. For p *inert* $p\mathfrak{o} = \mathfrak{p}$, the norm is $N\mathfrak{p} = p^4$, and

$$\prod_{\mathfrak{p}|p} \frac{1}{1 - N\mathfrak{p}^{-s}} \;=\; \frac{1}{1-p^{-4s}} \;=\; \frac{1}{1-\dfrac{1}{p^s}} \cdot \frac{1}{1+\dfrac{1}{p^s}} \cdot \frac{1}{1-\dfrac{i}{p^s}} \cdot \frac{1}{1+\dfrac{i}{p^s}}$$

$$= \frac{1}{1-\dfrac{1}{p^s}} \cdot \frac{1}{1-\dfrac{\chi_2(p)}{p^s}} \cdot \frac{1}{1-\dfrac{\chi_1(p)}{p^s}} \cdot \frac{1}{1-\dfrac{\chi_3(p)}{p^s}}$$

$$= \text{ Euler } p\text{-factors from } \zeta(s),\ L(s,\chi_2),\ L(s,\chi_1),\ L(s,\chi_3)$$

... not distinguishing the order-four characters χ_1,χ_3. This proves the claimed factorization, except for $p = 5$. The interested reader might show that $5\mathfrak{o} = (\omega - 1)^4$, and then it's easy to see the complete factorization of the Dedekind zeta.

For $\mathfrak{o} = \mathbb{Z}[\omega]$, the factorization is equivalent to understanding the behavior of rational primes in the extension ring $\mathbb{Z}[\omega]$ of $\mathbb{Z}$: do they *stay prime*, or do they *factor* as products of primes in $\mathbb{Z}[\omega]$?

Letting ω be a primitive q^{th} root of unity for q prime, and Φ_q the q^{th} cyclotomic polynomial,

$$\mathbb{Z}[\omega]/p \;\approx\; \big(\mathbb{Z}[x]/\Phi_q\big)/p \;\approx\; \big(\mathbb{Z}[x]/p\big)/\Phi_q$$

$$\approx\; \mathbb{F}_p[x]/\Phi_q \;\approx\; \mathbb{F}_p[x]/\varphi_1 \oplus \ldots \oplus \mathbb{F}_p[x]/\varphi_m$$

where φ_i are irreducible factors of Φ_q in $\mathbb{F}_p[x]$.

On the other hand, assuming the Dedekind-domain property, and that $p = \mathfrak{P}_1 \ldots \mathfrak{P}_n$ with distinct $\mathfrak{P}_i$, then by Sun-Ze's theorem

$$\mathbb{Z}[\omega]/p \;\approx\; \mathbb{Z}[\omega]/\mathfrak{P}_1 \oplus \ldots \oplus \mathbb{Z}[\omega]/\mathfrak{P}_n$$

Thus,

$$\mathbb{F}_p[x]/\varphi_1 \oplus \ldots \oplus \mathbb{F}_p[x]/\varphi_m \;\approx\; \mathbb{Z}[\omega]/\mathfrak{P}_1 \oplus \ldots \oplus \mathbb{Z}[\omega]/\mathfrak{P}_n$$

4. *Hensel's lemma: equations modulo p^n, p-adic numbers*

Recall: solving *linear* equations mod N, we need just a simple case: for $\gcd(a, N) = 1$, for the equation

$$ax + b \;=\; 0 \bmod N$$

a solution $x \in \mathbb{Z}$ *exists*, and is *unique* up to multiples of N. Proof: recall (!) that there are integers c, d such that

$$\gcd(a, N) \;=\; c \cdot a + d \cdot N$$

Since the *gcd* is 1, this is $1 = ca + dN$. Thus, we have an inverse $c = a^{-1} \bmod N$ for $a \bmod N$. This gives *existence* and *uniqueness* all at once:

$$ax + b \;=\; 0 \bmod N \quad\Longleftrightarrow\quad x = -a^{-1}b \bmod N$$

[4.1] Remark: The case N *prime* is conceptually simpler, since $\mathbb{Z}/p$ is provably a *field.* However, indeed, some part of the above discussion is exactly what proves $\mathbb{Z}/p$ is a field.

[4.2] Example: Solving $x^2 + 1 = 0 \bmod 5^n$ for large n. Since $4|5-1$ and $\mathbb{F}_5^\times$ is cyclic, there *exists* an integer solution $x_1 \bmod 5$. In fact, $x_1 = 2$ or $3 \bmod 5$.

Next, given x_1, try to adjust it by multiples of 5 to obtain a solution $x_2 \bmod 5^2$: let $x_2 = x_1 + 5y$ and solve for y:

$$0 \;=\; x_2^2 + 1 \;=\; (x_1 + 5y)^2 + 1 \;=\; x_1^2 + 10x_1y + 5^2y^2 + 1 \bmod 5^2$$

The y^2 term has coefficient $0 \bmod 5^2$, so this becomes a *linear* equation in y:

$$0 \;=\; x_1^2 + 10x_1y + 1 \bmod 5^2$$

By design, $x_1^2 + 1$ is divisible by 5, so we can divide through by 5:

$$\frac{x_1^2 + 1}{5} + 2x_1y \;=\; 0 \bmod 5$$

Since $2x_1$ is invertible mod 5, there is a *unique* solution y mod 5. Thus, there is *unique* x_2 mod 5^2 such that both $x_2 = x_1$ mod 5 and $x_2^2 + 1 = 0 \bmod 5^2$.

Induction to get a solution x_{n+1} mod 5^{n+1} from a solution x_n mod 5^n. Try to adjust x_n by a multiple of 5^n: $x_{n+1} = x_n + 5^n y$. Solve for y:

$$0 \;=\; x_{n+1}^2 + 1 \;=\; x_n^2 + 2 \cdot 5^n x_n y + 5^{2n} y^2 + 1 \bmod 5^{n+1}$$

Again, the coefficient of y^2 is $0 \bmod 5^{n+1}$, since $2n \geq n+1$ for $n \geq 1$, giving a *linear* equation in y. By induction, $x_n^2 + 1 = 0 \bmod 5^2$, so divide through by 5^n:

$$\frac{x_n^2+1}{5^n} + 2x_n y \;=\; 0 \bmod 5$$

For that matter, by induction, $x_n = x_1$ mod 5, so

$$y \;=\; -(2x_1)^{-1} \cdot \frac{x_n^2+1}{5^n} \quad \bmod 5$$

A somewhat-more-general case:

[4.3] Theorem: *(Hensel)* For f monic in $\mathbb{Z}[x]$, for prime p, if there is $x_1 \in \mathbb{Z}$ such that $f(x_1) = 0 \bmod p$ but $f'(x_1) \neq 0 \bmod p$, then there is a unique x_n mod p^n such that $f(x_n) = 0 \bmod p^n$ and $x_n = x_1 \bmod p$. Specifically, with $f'(x_1)$ inverted mod p,

$$x_{n+1} \;=\; x_n - \frac{f(x_n)}{f'(x_1)} \quad \bmod p^{n+1}$$

Proof: As in the example, given x_n, solve for $y \bmod p$ so that $x_{n+1} = x_n + p^n y$ is a solution mod p^{n+1}. Taylor series for polynomials are legitimate:

$$0 \;=\; f(x_{n+1}) \;=\; f(x_n + p^n y)$$

$$=\; f(x_n) + \frac{f'(x_n)}{1!} p^n y + \frac{f''(x_n)}{2!}(p^n y)^2 + \ldots \quad \bmod p^{n+1}$$

The sum is finite, but division by factorials...? In fact, for $f \in \mathbb{Z}[x]$, $f^{(k)}(x)$ has coefficients divisible by $k!$(!) It suffices to prove this for monomials:

$$\frac{d^k}{dx^k} x^n \;=\; n(n-1)(n-2)\ldots(n-k+1) \cdot x^{n-k}$$

Hopefully, we recognize

$$\frac{n(n-1)(n-2)\ldots(n-k+1)}{k!} \;=\; \frac{n!}{(n-k)!\,k!}$$

$$=\; \text{binomial coefficient } \in \mathbb{Z}$$

As $2n \geq n+1$ for $n \geq 1$, the equation becomes *linear* in y:

$$0 \;=\; f(x_{n+1}) \;=\; f(x_n + p^n y) \;=\; f(x_n) + \frac{f'(x_n)}{1!} p^n y \quad \bmod p^{n+1}$$

Inductively, $x_n = x_1 \bmod p$, so $f'(x_n) = f(x_1) \bmod p$. Thus, it is invertible mod p, and mod p^{n+1}. Then

$$p^n y \;=\; -\frac{f(x_n)}{f'(x_n)} \quad \bmod p^{n+1}$$

Using $f(x_n) = 0 \bmod p^n$,

$$y \;=\; -\frac{f(x_n)}{p^n \cdot f'(x_1)} \bmod p$$

Thus,

$$x_{n+1} \;=\; x_n + p^n y \;=\; x_n - \frac{f(x_n)}{f'(x_n)} \;=\; x_n - \frac{f(x_n)}{f'(x_1)} \bmod p^{n+1}$$

Done.

The sequence of solutions x_{n+1} looks like

$$\begin{array}{rcl} x_1 & = & x_1 \\ x_2 & = & x_1 + py_1 \\ x_3 & = & x_1 + py_1 + p^2y_2 \\ x_4 & = & x_1 + py_1 + p^2y_2 + p^3y_3 \\ & \ldots & \end{array}$$

The adjustments y_i can be in the range $\{0, 1, 2, \ldots, p-1\}$ if we want.

From x_n we can recover all the earlier ones: $x_{n-1}, x_{n-2}, \ldots, x_2, x_1$, at least modulo the respective p^k's.

It would be conceptually economical if the sequence $x_1, x_2, x_3, \ldots$ had a *limit*, x_∞, which somehow solved the equation modulo p^∞, from which we could recover solutions modulo p^n for all finite n.

There are at least two different-looking ways to make the limiting process legitimate.

The more popular, more accessible approach is by making up a metric, the p-adic metric $d(-,-)$, coming from the p-adic *norm* $|*|_p$, in which p^n get *smaller* as n gets *larger*. Then the **p-adic integers $\mathbb{Z}_p$** are the *completion* of $\mathbb{Z}$ with respect to the p-adic metric, and the p-adic rational numbers $\mathbb{Q}_p$ are the completion of $\mathbb{Q}$. We'll do this first.

The other approach, perhaps less popular, because it is less elementary, is nevertheless more revealing of the true workings of p-adic numbers and other things arising in a similar fashion: $\mathbb{Z}_p$ is the *(projective) limit* of the $\mathbb{Z}/p^n$. We'll look at this second.

The p-adic norm $|*|_p$ is defined on $\mathbb{Q}$ by

$$\Big|p^n \cdot \frac{a}{b}\Big|_p \;=\; p^{-n} \qquad\qquad (\text{with } a, b \text{ prime to } p,\ n \in \mathbb{Z})$$

The p-adic *metric* is made from the norm in the same way that the usual (”real”) metric on $\mathbb{Q}$ is made from the usual absolute value: $d(x,y) = |x-y|_p$. It is obviously symmetric and reflexive, but the *triangle inequality*

$$d(x,z) \;\le\; d(x,y) + d(y,z)$$

takes a bit of thought. Yes, $|k|_p \le 1$ for all $k \in \mathbb{Z}$. Examples:

$$\begin{array}{rclcrclcrcl} |5|_2 & = & 1 && |5|_5 & = & \frac{1}{5} && |5|_3 & = & 1 \\[2ex] |10|_2 & = & \frac{1}{2} && |10|_5 & = & \frac{1}{5} && |10|_3 & = & 1 \\[2ex] |\frac{2}{3}|_2 & = & \frac{1}{2} && |\frac{2}{3}|_5 & = & 1 && |\frac{2}{3}|_3 & = & 3 \\[2ex] |\frac{35}{18}|_2 & = & 2 && |\frac{35}{18}|_5 & = & \frac{1}{5} && |\frac{35}{18}|_3 & = & 9 \end{array}$$

A metric space is *complete* if every Cauchy sequence has a limit. The *completion* $\widetilde{X}, \tilde{d}$ of a metric space X, d can be *characterized* as a complete metric space with an inclusion $j : X \to \widetilde{X}$ preserving the metric, that is, $\tilde{d}(jx, jy) = d(x,y)$, and such that X is *dense*, that is, every point of $\widetilde{X}$ is a limit of a Cauchy sequence in X.

Completions $\widetilde{X}$ are proven to *exist* by giving a *construction*: $\widetilde{X}$ is Cauchy sequences in X modulo the equivalence relation $\{x_n\} \sim \{y_n\}$ when $\lim_n d(x_n, y_n) = 0$. The metric on this model is $\tilde{d}(\{x_n\}, \{y_n\}) = \lim_n d(x_n, y_n)$. There are things to be checked to certify that this construction succeeds in making a completion.

Another *characterization* of the completion $j : X \to \widetilde{X}$, which makes it easy to prove *uniqueness*, is that any metric-preserving map $f : X \to Y$ to a *complete* metric space Y *factors through* $j : X \to \widetilde{X}$, in the sense that there is a *unique* metric-preserving $F : \widetilde{X} \to Y$ such that

$$\begin{tikzcd}
\widetilde{X} \arrow[dr, dashed, "F"] & \\
X \arrow[u, "j"] \arrow[r, "f"] & Y
\end{tikzcd} \qquad \text{(metric-preserving maps)}$$

The ring of **p-adic integers** $\mathbb{Z}_p$ is the completion of $\mathbb{Z}$ with respect to $|*|_p$.

The field of **p-adic rationals** $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $|*|_p$.

We'll also want to be sure that addition, multiplication, and inversion (of non-zero things) are *continuous* on $\mathbb{Q}$ in the p-adic metric, so that it is legitimate to *extend by continuity* to define addition and multiplication on $\mathbb{Q}_p$:

$$\begin{aligned}
(\lim_n a_n) \cdot (\lim_n b_n) &= \lim_n (a_n \cdot b_n) \\
(\lim_n a_n) + (\lim_n b_n) &= \lim_n (a_n + b_n) \\
(\lim_n a_n)^{-1} &= \lim_n (a_n^{-1})
\end{aligned}$$

By design, the sequence of solutions x_n to $f(x_n) = 0 \bmod p^n$,

$$\begin{array}{lcl}
x_1 &=& x_1 \\
x_2 &=& x_1 + py_1 \\
x_3 &=& x_1 + py_1 + p^2 y_2 \\
x_4 &=& x_1 + py_1 + p^2 y_2 + p^3 y_3 \\
& \ldots &
\end{array} \qquad \text{(with } x_1,\ y_i \text{ in } \mathbb{Z})$$

is *Cauchy* in the p-adic metric: for $m \le n$,

$$|x_n - x_m|_p = |p^{m+1} y_{m+1} + \ldots p^n y_n|_p$$

$$= |p^{m+1}|_p \cdot |y_{m+1} + \ldots p^{n-m-1} y_n|_p \le |p^{m+1}|_p \cdot 1 = \frac{1}{p^{m+1}}$$

since $y_{m+1} + \ldots p^{n-m-1} y_n \in \mathbb{Z}$!!!

For example, 2-adically,

$$1 + 2 + 4 + 8 + 16 + \ldots = \lim_n (1 + 2 + \ldots + 2^n)$$

$$= \lim_n \frac{1 - 2^{n+1}}{1 - 2} = \frac{1 - 0}{1 - 2} = -1$$

Generally, p-adically,

$$1 + p + p^2 + p^3 + \ldots = \frac{1}{1 - p}$$

In contrast, the usual exponential series

$$e^x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \ldots$$

converges p-adically only for $|x|_p$ *small*, because the factorials *hurt*, rather than *help* the convergence.

Warning: Yes, it is *possible* to write p-adic integers in a form that makes them look like *power series*:

$$\alpha \;=\; a_o + a_1 p^1 + a_2 p^2 + a_3 p^3 + \ldots \qquad (\text{with } a_i \in \{0, 1, 2, \ldots, p-1\})$$

In fact, this is what Hensel originally emphasized. However, neither addition nor multiplication treat such expressions as power series: the basic discrepancy is that *no* number of x^k's can add up to x^{k+1}, but adding p p^k's gives p^{k+1}.

Hensel's analogy to power series *is correct*, but not quite in the naive way one might think.

Therefore, while the possibility of such expressions is genuine, they do *not* reflect the behavior of p-adic numbers very well!!!

Another viewpoint: Even though the p-adic norm and metric succeed in making the sequences produced by Hensel's lemma *convergent*, there might seem an element of whimsicality.

One ambiguity is that many different metrics can give the same topology.

The true state of affairs, addressed candidly, is that Hensel's recursion produces a sequence x_n fitting into a picture

$$\begin{tikzcd}
\ldots \arrow[r] & x_{n+1} \arrow[r] & \ldots \arrow[r] & x_2 \arrow[r] & x_1 \\
\ldots \arrow[r] & \mathbb{Z}/p^{n+1} \arrow[r, "\text{mod } p^n"] & \ldots \arrow[r, "\text{mod } p^2"] & \mathbb{Z}/p^2 \arrow[r, "\text{mod } p"] & \mathbb{Z}/p
\end{tikzcd}$$

Ultrametric inequality: All p-adic triangles are isosceles!!! Stronger than the *triangle inequality*, the *ultrametric inequality* holds:

$$|x \pm y|_p \;\;\le\;\; \max\big(|x|_p, |y|_p\big) \qquad (\text{with } \textit{equality} \text{ unless } |x|_p = |y|_p!!!)$$

To discuss this the p-adic *valuation* or *ord(er)* is useful:

$$\text{ord}_p(p^\ell \cdot \frac{a}{b}) \;=\; \nu_p(p^\ell \cdot \frac{a}{b}) \;=\; \ell \qquad\qquad (\text{with } a, b \text{ prime to } p)$$

And $\text{ord}_p 0 = \infty$. Then $|x|_p \;=\; p^{-\text{ord}_p x}$.

To see the ultrametric inequality, observe that, for p^m the largest power of p dividing x, and p^n the largest power of p dividing y, taking $m \le n$ without loss of generality, p^m divides $x \pm y$. If $m < n$, then p^m is the *largest* power dividing $x \pm y$. That is,

$$\text{ord}_p(x \pm y) \;\ge\; \min\left(\text{ord}_p x, \text{ord}_p y\right)$$

$$(\text{with } \textit{equality} \text{ unless } \text{ord}_p x = \text{ord}_p y)$$

Rewriting in terms of the norm reverses the inequality, giving the ultrametric inequality.

Ring structure of $\mathbb{Z}_p$ All integers n *prime to* p become p-adic *units!!!*

Proof: Let $f(x) = nx - 1$. Integers a, b with $ap + bn = 1$ give solution $x_1 = b$ to $f(x) = 0 \bmod p$. Since $f'(x) = n \ne 0 \bmod p$, Hensel gives a (compatible!) sequence x_n such that $nx_n = 1 \bmod p^n$. The compatibility $x_{n+1} = x_n \bmod p^n$ assures the sequence is Cauchy, and the limit is the p-adic n^{-1}. ///

Or: computing in $\mathbb{Q}_p$, from $bn = 1 - ap$, $b^{-1}n^{-1} = (1 - ap)^{-1}$ and

$$n^{-1} \;=\; b \cdot (1 - ap)^{-1} \;=\; b \cdot (1 + ap + a^2p^2 + a^3p^3 + \ldots) \;\in\; \mathbb{Z}_p$$

For example, to find 11-adic 7^{-1}, from $2 \cdot 11 - 3 \cdot 7 = 1$,

$$7^{-1} \;=\; (-3) \cdot (1 - 2 \cdot 11)^{-1} \;=\; (-3) \cdot (1 + 2 \cdot 11 + 4 \cdot 11^2 + 8 \cdot 11^3 + \ldots)$$

But wait: zero divisors in $\mathbb{Z}_p$? Is $\mathbb{Q}_p$ really a field? Use the p-adic norm: if $\alpha \cdot \beta = 0$ for p-adic integers α, β, then by multiplicativity

$$0 \;=\; |0|_p \;=\; |\alpha \cdot \beta|_p \;=\; |\alpha|_p \cdot |\beta|_p$$

This is an equality of rational numbers, so either $|\alpha|_p = 0$ or $|\beta|_p = 0$, so either $\alpha = 0$ or $\beta = 0$.

Just to be sure that $|\alpha|_p = 0 \Rightarrow \alpha = 0$: the completion is Cauchy sequences modulo $\{x_n\} \sim \{y_n\}$ when $\lim_n |x_n - y_n|_p = 0$. For non-zero rationals, $|p^\ell \frac{a}{b}|_p \to 0$ requires $\ell \to +\infty$ (with a, b prime to p), and a, b have no impact. Then $|p^\ell \frac{a}{b} - 0|_p \to 0$, and $p^\ell \frac{a}{b} \to 0$ in $\mathbb{Q}_p$. That is, the Cauchy sequence is identified with 0.

[4.4] Claim: On $\mathbb{Q}_p^\times$ the p-adic norm (still) takes only the discrete values p^ℓ with $\ell \in \mathbb{Z}$.

... in contrast to the usual $| * |$'s values on $\mathbb{R}$ versus on $\mathbb{Q}$.

Proof: By definition, for Cauchy $\{\alpha_n\}$, $|\lim_n \alpha_n|_p = \lim_n |\alpha_n|_p$. Let α be the limit. For $0 < \varepsilon < |\alpha|_p$ and $|\alpha_n - \alpha|_p < \varepsilon$, by the *ultrametric* inequality

$$|\alpha_n|_p \;=\; |\alpha_n - \alpha + \alpha|_p \;=\; \max(|\alpha_n - \alpha|_p, |\alpha|_p) \;=\; |\alpha|_p$$

Since $|\alpha_n|_p$ are integer powers of p, so is $|\alpha|_p$. ///

The *discreteness* of values of $| * |_p$ is hugely different from the usual $| * |$.

[4.5] Claim: The p-adic completion $\mathbb{Z}_p$ of $\mathbb{Z}$ has properties:

$$\begin{aligned}
\mathbb{Z}_p &= \{\alpha \in \mathbb{Q}_p : |\alpha|_p \le 1\} &&= \{\alpha \in \mathbb{Q}_p : |\alpha|_p < p\} \\
p\mathbb{Z}_p &= \{\alpha \in \mathbb{Q}_p : |\alpha|_p < 1\} &&= \{\alpha \in \mathbb{Q}_p : |\alpha|_p \le \tfrac{1}{p}\} \\
\mathbb{Z}_p^\times &= \{\alpha \in \mathbb{Q}_p : |\alpha|_p = 1\} &&= \{\alpha \in \mathbb{Q}_p : \tfrac{1}{p} < |\alpha|_p < p\}
\end{aligned}$$

Each of these sets is *both open and closed.*

Proof: Use discreteness of $|*|_p$. When a Cauchy sequence $\alpha_n \in \mathbb{Q}^\times$ has $\lim_n |\alpha_n|_p \le 1$, eventually $|\alpha_n|_p < p$, and then necessarily $|\alpha_n|_p \le 1$ by discreteness. Thus, $\alpha_n \in \mathbb{Z}$ from that point, so $\lim_n \alpha_n \in \mathbb{Z}_p$.

For a Cauchy sequence $\alpha \in \mathbb{Q}^\times$ with $\lim_n |\alpha_n|_p < 1$, by discreteness eventually $|\alpha_n|_p \le \frac{1}{p}$. Thus, eventually $\alpha_n \in p\mathbb{Z}$. Thus, eventually $\alpha_n = p \cdot \frac{\alpha_n}{p}$ with $\alpha_n/p \in \mathbb{Z}$, exhibiting $\lim_n \alpha_n$ as an element of $p \cdot \mathbb{Z}_p$.

For Cauchy sequence $\alpha \in \mathbb{Q}^\times$ with $\lim_n |\alpha_n|_p = 1$, by discreteness eventually $\frac{1}{p} < |\alpha_n|_p < p$, so $|\alpha_n|_p = 1$, and $\alpha_n = \frac{a_n}{b_n}$ with a, b prime to p. We'd already noted that such things are p-adic units.

The topology is metric, and the above shows that $\mathbb{Z}_p$ is both the *closed ball* of radius 1 centered at 0, and also the *open ball* of any radius r with $1 < r < p$.

$\mathbb{Z}_p$ and $\mathbb{Q}_p$ are totally disconnected That is, given $\alpha \ne \beta \in \mathbb{Q}_p$, there are disjoint open-and-closed sets $U \ni \alpha$ and $V \ni \beta$ such that $U \cup V = \mathbb{Q}_p$.

... due to the discreteness of the norm/metric/valuation: Let $p^\ell = |\alpha - \beta|_p$, and consider a ball centered at α

$$B \;=\; \{x \in \mathbb{Q}_p \;:\; |\alpha - x|_p < p^\ell\} \;=\; \{x \in \mathbb{Q}_p \;:\; |\alpha - x|_p \le p^{\ell-1}\}$$

That is, the ball is both open and closed, so its *complement*, containing β, is both open and closed. ///

Another viewpoint: Even though the p-adic norm and metric succeed in making the sequences produced by Hensel's lemma *convergent*, there might seem an element of whim.

One ambiguity is that many different metrics can give the same topology.

The true state of affairs, addressed candidly, is that Hensel's recursion produces a sequence x_n fitting into a picture

$$\begin{tikzcd}
\ldots \arrow[r] & x_{n+1} \arrow[r] & \ldots \arrow[r] & x_2 \arrow[r] & x_1 \\
\ldots \arrow[r] & \mathbb{Z}/p^{n+1} \arrow[r, "\text{mod } p^n"] & \ldots \arrow[r, "\text{mod } p^2"] & \mathbb{Z}/p^2 \arrow[r, "\text{mod } p"] & \mathbb{Z}/p
\end{tikzcd}$$

What we want is not so much a *metric* something-something, but an object X *behind* all the $\mathbb{Z}/p^n$'s, and $x_\infty \in X$,

$$\begin{tikzcd}
x_\infty \arrow[rr, dashed, bend left] \arrow[rrrr, dashed, bend left] \arrow[rrrrr, dashed, bend left] & \ldots \arrow[r] & x_{n+1} \arrow[r] & \ldots \arrow[r] & x_2 \arrow[r] & x_1
\end{tikzcd}$$

making a *commutative diagram* (meaning that the outcome doesn't depend on what route is traversed)

$$\begin{tikzcd}
X \arrow[rr, dashed, bend left] \arrow[rrrr, dashed, bend left] \arrow[rrrrr, dashed, bend left] & \ldots \arrow[r] & \mathbb{Z}/p^{n+1} \arrow[r, "\text{mod } p^n"] & \ldots \arrow[r, "\text{mod } p^2"] & \mathbb{Z}/p^2 \arrow[r, "\text{mod } p"] & \mathbb{Z}/p
\end{tikzcd}$$

We should tell how this X is to *interact* with other things, probably *topological rings*, meaning rings with topologies so that addition and multiplication are continuous. *Hausdorff*, for sanity.

Now *map* will mean *continuous ring hom*. Require that, for every topological ring Y with a collection of compatible maps (meaning the diagram is commutative)

$$\begin{tikzcd}
Y \arrow[rr, bend left] \arrow[rrrr, bend left] \arrow[rrrrr, bend left] & \ldots \arrow[r] & \mathbb{Z}/p^{n+1} \arrow[r, "\text{mod } p^n"] & \ldots \arrow[r, "\text{mod } p^2"] & \mathbb{Z}/p^2 \arrow[r, "\text{mod } p"] & \mathbb{Z}/p
\end{tikzcd}$$

there is a *unique* map $Y \to X$ giving a commutative diagram

$$\begin{tikzcd}
X \arrow[rr, bend left] \arrow[rrrr, bend left] \arrow[rrrrr, bend left] & \ldots \arrow[r] & \mathbb{Z}/p^{n+1} \arrow[r, "\text{mod } p^n"] & \ldots \arrow[r, "\text{mod } p^2"] & \mathbb{Z}/p^2 \arrow[r, "\text{mod } p"] & \mathbb{Z}/p \\
& Y \arrow[ul, dashed] \arrow[ur] \arrow[urrr] \arrow[urrrr] & & & &
\end{tikzcd}$$

A topological ring $X = \lim \mathbb{Z}/p^n$ meeting these conditions is the *(projective) limit* of the $\mathbb{Z}/p^n$'s, and is provably the same $\mathbb{Z}_p$!!!

Note: each finite ring $\mathbb{Z}/p^n$ has a unique Hausdorff topology!!! How to prove *existence* of projective limits? In this and many other situations, limits $\lim_n X_n$ are *subsets* of the (topological) cartesian products $\prod_n X_n$. Specifically, with

$$\begin{tikzcd}
\ldots \arrow[r] & X_{n+1} \arrow[r, "\varphi_{n+1}"] & \ldots \arrow[r, "\varphi_3"] & X_2 \arrow[r, "\varphi_2"] & X_1
\end{tikzcd}$$

a projective limit $X = \lim_n X_n$ can be constructed as

$$X \;=\; \{\{x_n\} \;:\; x_n \in X_n \text{ such that } \varphi_n(x_n) = x_{n-1} \text{ for all } n\}$$

That is, X consists exactly of *compatible sequences*

$$\begin{tikzcd}
\ldots \arrow[r] & x_{n+1} \arrow[r, "\varphi_{n+1}"] & \ldots \arrow[r, "\varphi_3"] & x_2 \arrow[r, "\varphi_2"] & x_1
\end{tikzcd}$$

just as produced by Hensel's recursion. For continuous φ_n and *compact* Hausdorff X_n's, *Tychonoff's theorem* says the product is *compact.* Such a projective limit is a closed subset of a compact Hausdorff space, so is *compact.* This proves compactness of $\mathbb{Z}_p$!!!

Uniqueness (up to unique isomorphism) of projective limits: The diagrammatic characterization can be used to assure that there's *no ambiguity* in what $\mathbb{Z}_p$ is, as long as it functions as a projective limit:

First, claim the only map of $X = \lim_n X_n$ to *itself*, compatible with the maps of it to the X_n, is the *identity.* Certainly the identity map is ok. Then the *uniqueness* of the dotted arrow

$$\begin{tikzcd}
X \arrow[rr, bend left] \arrow[rrrr, bend left] \arrow[rrrrr, bend left] & \ldots \arrow[r] & X_n \arrow[r, "\varphi_n"] & \ldots \arrow[r, "\varphi_3"] & X_2 \arrow[r, "\varphi_2"] & X_1 \\
& X \arrow[ul, dashed] \arrow[ur] \arrow[urrr] \arrow[urrrr] & & & &
\end{tikzcd}$$

proves that the identity is the *only* compatible map. Let X and X' be projective limits. On one hand, there is a unique $f : X' \to X$ giving commutative diagram

$$\begin{tikzcd}
X \arrow[rr, bend left] \arrow[rrrr, bend left] \arrow[rrrrr, bend left] & \ldots \arrow[r] & X_n \arrow[r, "\varphi_n"] & \ldots \arrow[r, "\varphi_3"] & X_2 \arrow[r, "\varphi_2"] & X_1 \\
& X' \arrow[ul, dashed] \arrow[ur] \arrow[urrr] \arrow[urrrr] & & & &
\end{tikzcd}$$

On the other hand, reversing the roles of X and X', there is a unique compatible map $g : X \to X'$ fitting into

$$\begin{tikzcd}
X' \arrow[rr, bend left] \arrow[rrrr, bend left] \arrow[rrrrr, bend left] & \ldots \arrow[r] & X_n \arrow[r, "\varphi_n"] & \ldots \arrow[r, "\varphi_3"] & X_2 \arrow[r, "\varphi_2"] & X_1 \\
& X \arrow[ul, dashed] \arrow[ur] \arrow[urrr] \arrow[urrrr] & & & &
\end{tikzcd}$$

The composites $f \circ g : X \to X$ and $g \circ f : X' \to X'$ are also compatible, so must be the identities on X and X', by the first part. Thus, f, g are mutual inverses. ///

Cauchy's criterion is necessary-and-sufficient: A p-adic infinite sum $a_o + a_1 + a_2 + \ldots$ is convergent if and only if $|a_n| \to 0$.

Proof: Ultrametric property: given $\varepsilon > 0$, let m_o be large enough so that $|a_m|_p < \varepsilon$ for $m \geq m_o$. Then, by the ultrametric property, for $m_o \leq m < n$, the tail between these two indices has size

$$|a_{m+1} + \ldots + a_n|_p \;\leq\; \max_{m<j\leq n} |a_j|_p \;<\; \varepsilon$$

Done.

Don't forget that in $\mathbb{R}$, Cauchy's criterion is *necessary*, but *not* sufficient: the harmonic series $1 + \frac{1}{2} + \frac{1}{3} + \ldots$ diverges.

Observe: The only non-zero proper *ideals* in $\mathbb{Z}_p$ are $p^\ell \cdot \mathbb{Z}_p$ with $\ell > 0$.

Proof: Given a proper, non-zero ideal I in $\mathbb{Z}_p$, let $\sigma = \sup_{x\in I} |x|_p$. By the discreteness of $|*|_p$, for $|x_j|_p \to \sigma \neq 0$, eventually $|x_i|_p = \sigma$.

Thus, we can choose *a* largest element x in I. For all $y \in I$, $|y/x|_p = |y|_p/|x|_p \le 1$. That is, $y/x \in \mathbb{Z}_p$, and $I = x \cdot \mathbb{Z}_p$. ///

Not only are the $p^n\mathbb{Z}_p$ the only ideals in $\mathbb{Z}_p$, but also $\mathbb{Z}_p/p^n\mathbb{Z}_p \approx \mathbb{Z}/p^n\mathbb{Z}$. This is used to compare the *metric completion* version of $\mathbb{Z}_p$ to the *limit* characterization.

[4.6] Claim: For positive integers n, $\mathbb{Z}_p/p^n\mathbb{Z}_p \approx \mathbb{Z}/p^n\mathbb{Z}$.

Proof: Inclusion $\mathbb{Z} \to \mathbb{Z}_p$ compose with $\mathbb{Z}_p \to \mathbb{Z}_p/p^n\mathbb{Z}_p$ has kernel

$$\mathbb{Z} \cap p^n\mathbb{Z}_p \;=\; \mathbb{Z} \cap \{x \in \mathbb{Z}_p : |x|_p \le \frac{1}{p^n}\} \;=\; \{x \in \mathbb{Z} : |x|_p \le \frac{1}{p^n}\}$$

$$= \;\{\text{integers divisible by } p^n\} \;=\; p^n\mathbb{Z}$$

Thus, $\mathbb{Z}/p^n\mathbb{Z}$ *injects* to $\mathbb{Z}_p/p^n\mathbb{Z}_p$. On the other hand, because $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, given $x \in \mathbb{Z}_p$ there is $y \in \mathbb{Z}$ such that $|x - y| \le \frac{1}{p^n}$. That is, $x \in y + p^n\mathbb{Z}_p$. Then

$$x + p^n\mathbb{Z}_p \;=\; y + p^n\mathbb{Z}_p + p^n\mathbb{Z}_p \;=\; y + p^n\mathbb{Z}_p \qquad (\text{with } y \in \mathbb{Z})$$

That is, the map is also *surjective.* ///

5. *Characterizations versus constructions:*

The *ordered pair* formation (a, b) is *characterized* by the property that $(a, b) = (a', b')$ if and only if $a = a'$ and $b = b'$. Straightforward intent!

In contrast, the set-theory *construction* is $(a, b) = \{\{a\}, \{a, b\}\}$. In the early 20th century, this was interesting. The construction is irrelevant to the *use* of ordered pairs.

Or, what is an indeterminate? We tell calculus students that x is a *variable real number.* Or *is arbitrary.* Not bad intuition, but what does that *mean?* This viewpoint is stressed beyond hope in the Cayley-Hamilton theorem: a linear map T on a finite-dimensional real vectorspace V has characteristic polynomial $\chi_T(x) = \det(x \cdot 1_V - T)$. The CH theorem says $\chi_T(T) = 0$.

We are substituting a *matrix* for x. The CH theorem helps illustrate that x has the property that we can *substitute anything* for it... within reason.

One way to say this: working over $\mathbb{C}$, for example, the polynomial ring $\mathbb{C}[x]$ should have the property that, for every ring R containing a copy of $\mathbb{C}$, and for every $r_o \in R$, there is a unique ring hom $\mathbb{C}[x] \to R$ mapping $x \to r_o$ (and mapping $\mathbb{C}$ to the copy inside R).

That is, $\mathbb{C}[x]$ is the *free* $\mathbb{C}$*-algebra on one generator. Set*-maps $\{x\} \to R$ become $\mathbb{C}$*-algebra* maps $\mathbb{C}[x] \to R$.

(The functor $\{x\} \dashrightarrow \mathbb{C}[x]$ is *adjoint to* the forgetful functor taking R to its underlying set.)

Quotient groups: The *quotient* G/N of a group G by a normal subgroup N is usually *defined* to be the set of cosets gN. This is easy to say, but conceals the *purpose.* With hindsight, the real purpose is to make a group Q with a group hom $q : G \to Q$ such that every group hom $f : G \to H$ with $\ker f \supset N$ *factors through*

$q : G \to Q$, in the sense of giving a commutative diagram

$$\begin{tikzcd}
Q \arrow[rd, dashed] & \\
G \arrow[u, "q"] \arrow[r, "f"] & H
\end{tikzcd}$$

Existence of Q is proven by the usual *construction* by cosets.

A form of simplest *isomorphism theorem* is really the *characterization* of the quotient.

Simple example: products: A *product* $X = \prod_i X_i$ of objects X_i has maps $p_i : X \to X_i$ such that, for every object Y with maps $q_i : Y \to X_i$, there is a *unique* $f : Y \to X$ such that $q_i = p_i \circ f$. A picture:

$$\begin{tikzcd}
& X \arrow[dd, "p_i"] & \\
Y \arrow[ru, dashed, "f"] \arrow[rd, "q_i"'] & & \\
\ldots & X_i & \ldots
\end{tikzcd}$$

This characterization explains why the *product topology* of an infinite collection of topological spaces is coarser than we might expect: the following general fact (proven just below) shows that there is *no choice* of how to make a sensible product object!

This diagrammatic characterization determines the product $\prod_i X_i$ *uniquely up to unique isomorphism.*

Proof: First, show that the only map $X \to X$ compatible with the diagram

$$\begin{tikzcd}
& X \arrow[dd, "p_i"] & \\
X \arrow[ru, dashed] \arrow[rd, "p_i"'] & & \\
\ldots & X_i & \ldots
\end{tikzcd}$$

is the *identity* map. Indeed, the identity map fits, and the assertion that there is *only one* map fitting into the diagram finishes it.

Next, show that, given two products X, X' with projections p_i, p'_i to X_i, there is a unique isomorphism $X' \to X$ fitting into the diagram

$$\begin{tikzcd}
& X \arrow[dd, "p_i"] & \\
X' \arrow[ru, dashed, "\text{isom } f"] \arrow[rd, "p'_i"'] & & \\
\ldots & X_i & \ldots
\end{tikzcd}$$

First, since X is a product, in any case there is a *unique* map f fitting into the diagram. We must prove it is an isomorphism.

On the other hand, reversing the roles of X, X', using the fact that X' is a product, there is *some* map g fitting into the diagram

$$\begin{tikzcd}
 & X \arrow[dl, dashed, "g"'] \arrow[dd, "p'_i"] & \\
X' \arrow[dr, "p'_i"'] & & \\
\cdots & X_i & \cdots
\end{tikzcd}$$

Then $g \circ f : X' \to X'$ and $f \circ g : X \to X$ respect the projections, so must be the respective identity maps, and are isomorphisms. ///

Coproducts are characterized by reversing the arrows: A *coproduct* $X = \coprod_i X_i$ of objects X_i has maps $j_i : X_i \to X$ such that, for every object Y with maps $k_i : X_i \to Y$, there is a *unique* $f : X \to Y$ such that $q_i = f \circ p_i$. A picture:

$$\begin{tikzcd}
 & X \arrow[dl, dashed, "f"'] & \\
Y & & \\
\cdots & X_i \arrow[uu, "j_i"'] \arrow[ul, "k_i"] & \cdots
\end{tikzcd}$$

The same argument shows this diagrammatic characterization determines the coproduct *uniquely up to unique isomorphism.*

Note: In *concrete* categories, where objects more-or-less are constructible as *sets* with additional structure, *products* are typically constructible as *set*-products with the corresponding additional structure.

Product groups' underlying sets are product sets, as are topological spaces, vector spaces, etc .

In contrast, set-*coproducts* are *disjoint unions*, which is *not* the underlying set for coproducts of groups or vector spaces.

Colimit (inductive limit) $\mathbb{Q}_p$ As topological *rings*, $\mathbb{Q}_p$ is the *field of fractions* of $\mathbb{Z}_p$. Good, but we need more flexibility. Forgetting multiplication for a moment, $\mathbb{Q}_p$ is a *nested union*

$$\mathbb{Q}_p \;=\; \mathbb{Z}_p \cup \frac{1}{p}\mathbb{Z}_p \cup \frac{1}{p^2}\mathbb{Z}_p \cup \ldots$$

That is, it is a *colimit*, where all maps are inclusions,

$$\begin{tikzcd}
\mathbb{Z}_p \arrow[r] \arrow[rrrr, bend left=40] \arrow[drrr] & \frac{1}{p}\mathbb{Z}_p \arrow[r] \arrow[rrr, bend left=30] \arrow[drr] & \frac{1}{p^2}\mathbb{Z}_p \arrow[r] \arrow[rr, bend left=20] \arrow[dr] & \ldots & \mathbb{Q}_p \arrow[dl, dashed] \\
 & & & X &
\end{tikzcd}$$

The defining property of the colimit is that all compatible collections of maps from another object X to the limitands give a unique compatible map $X \to \mathbb{Q}_p$. Colimits are unique up to unique isomorphism, as usual.

To *construct* $\mathbb{Q}_p$ as a colimit, we can't divide $\mathbb{Z}_p$ by p^n's, since this begs the question. We avoid that by converting *inclusions* to *multiplications*:

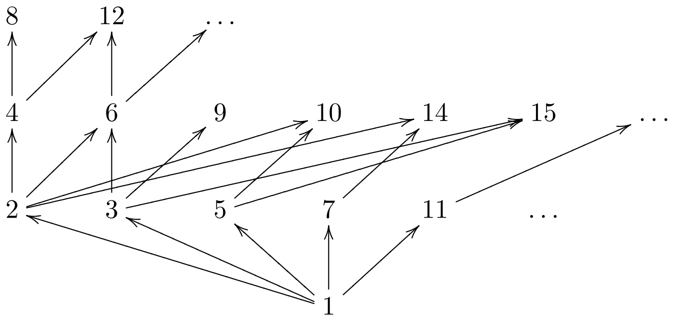
$$\begin{tikzcd}
\mathbb{Z}_p \arrow[r, "\text{inc}"] \arrow[d, "\times 1"'] & \frac{1}{p}\mathbb{Z}_p \arrow[r, "\text{inc}"] \arrow[d, "\times p"'] & \frac{1}{p^2}\mathbb{Z}_p \arrow[r, "\text{inc}"] \arrow[d, "\times p^2"'] & \ldots \\
\mathbb{Z}_p \arrow[r, "\times p"] & \mathbb{Z}_p \arrow[r, "\times p"] & \mathbb{Z}_p \arrow[r, "\times p"] & \ldots
\end{tikzcd}$$

All the squares *commute*, so there is a unique natural isomorphism of the colimits. Thus, we have a (second) colimit description of $\mathbb{Q}_p$ which avoids begging the question:

$$\begin{tikzcd}
\mathbb{Z}_p \arrow[r, "\times p"] \arrow[rrrr, bend left] & \mathbb{Z}_p \arrow[r, "\times p"] \arrow[rrr, bend left] & \mathbb{Z}_p \arrow[r, "\times p"] \arrow[rr, bend left] & \ldots & \mathbb{Q}_p
\end{tikzcd}$$

Toward adeles: $\widehat{\mathbb{Z}}$ An immediate definition is $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$, but this doesn't tell how $\widehat{\mathbb{Z}}$ arises in nature.

Better: instead of considering the dinky (directed) posets $\{p^n : n = 1, 2, 3, \ldots\}$ of powers of single primes, consider the (directed) poset of *all* integers, ordered by *divisibility*:



A robust definition:

$$\widehat{\mathbb{Z}} = \lim_N \mathbb{Z}/N \qquad \text{(proj lim over } N \text{ ordered by divisibility)}$$

Projective limits and products fall into a broader class of "limits", which allows proof of their compatibility with each other... Using Sun-Ze, factoring each N into primes $N = \prod_p p^{e_p(N)}$,

$$\widehat{\mathbb{Z}} = \lim_N \mathbb{Z}/N \approx \lim_N \Big(\prod_p \mathbb{Z}/p^{e_p(N)} \Big) \approx \prod_p \lim_e \mathbb{Z}/p^e \approx \prod_p \mathbb{Z}_p$$

Recalling the (second) colimit description of $\mathbb{Q}_p$,

$$\begin{tikzcd}
\mathbb{Z}_p \arrow[r, "\times p"] \arrow[rrrr, bend left] & \mathbb{Z}_p \arrow[r, "\times p"] \arrow[rrr, bend left] & \mathbb{Z}_p \arrow[r, "\times p"] \arrow[rr, bend left] & \ldots & \mathbb{Q}_p
\end{tikzcd}$$

we could do the analogous thing with $\widehat{\mathbb{Z}}$ and *all* multiplications. Since the ring $\widehat{\mathbb{Z}}$ has many zero divisors, there's no option to talk about fields-of-fractions! For $0 < n \in \mathbb{Z}$, let $X_n \approx \widehat{\mathbb{Z}}$, and for $m|n$, let $\varphi_{mn} : X_m \to X_n$ by $\varphi_{mn}(x) = \frac{n}{m}x$. With these transition maps $\varphi_{m,n}$ implied,

$$\text{finite rational adeles } \mathbb{A}^{\text{fin}} = \text{colim}_N X_N$$

$$\begin{tikzcd}
\widehat{\mathbb{Z}} \arrow[r, "\times 2"] \arrow[dr, "\times 3"] \arrow[ddr, "\times 5"'] \arrow[rrrr, bend left] & \widehat{\mathbb{Z}} \arrow[r, "\times 2"] \arrow[dr, "\times 3"] \arrow[ddr, "\times 5"'] \arrow[rrr, bend left] & \ldots & & \mathbb{A}^{\text{fin}} \\
& \widehat{\mathbb{Z}} & {} & & \\
& \widehat{\mathbb{Z}} & {} & &
\end{tikzcd}$$

The common/immediate description of $\mathbb{A}^{\text{fin}}$: you will hear $\mathbb{A}^{\text{fin}}$ described [sic] as a *restricted direct product* [sic], meaning

$$\mathbb{A}^{\text{fin}} \;=\; \{\{x_p\} \in \prod_p \mathbb{Q}_p \;:\; x_p \in \mathbb{Z}_p \text{ for all but finitely-many primes } p\}$$

Since restricted direct products [sic] do not occur anywhere else, this is not an illuminating description. Its motivation is certainly completely obscure.

The **rational adeles** are $\mathbb{A} = \mathbb{R} \times \mathbb{A}^{\text{fin}}$. This captures all the p-adic stuff, and also archimedean (real-number) stuff.

The subgroup $\mathbb{R} \times \widehat{\mathbb{Z}}$ is both open and closed. One last point: imbed $\mathbb{Q}$ *diagonally* in $\mathbb{A}$, meaning into each $\mathbb{Q}_p$ and into $\mathbb{R}$ in the usual way. For $m|n$, let $\mathbb{R}/n\mathbb{Z} \to \mathbb{R}/m/Z$ by $r + n\mathbb{Z} \to r + m\mathbb{Z}$. Then [proof later]

$$\mathbb{A}/\mathbb{Q} \;=\; \lim_N \; \mathbb{R}/N\mathbb{Z} \;=\; \text{compact}$$

---

6. *Algebraic integers, Dedekind domains*

An *algebraic integer* $\alpha \in \overline{\mathbb{Q}}$ satisfies $f(\alpha) = 0$, for $f \in \mathbb{Z}[x]$ *monic.*

Also say α is *integral over* $\mathbb{Z}$, or simply *integral.* In a finite algebraic field extension k of $\mathbb{Q}$, the *ring* (why!?!?) $\mathfrak{o} = \mathfrak{o}_k$ of algebraic integers in k is

$$\mathfrak{o} \;=\; \{\alpha \in k \;:\; \alpha \text{ is integral over } \mathbb{Z}\}$$

[6.1] Example: Inside quadratic field extensions $k = \mathbb{Q}(\sqrt{D})$ of $\mathbb{Q}$, with D a square-free integer. Reasonably-enough, $\alpha = a + b\sqrt{D}$ with $a, b \in \mathbb{Z}$ is integral, satisfying

$$\alpha^2 - 2a\alpha + (a^2 - b^2 D) \;=\; 0$$

For $D = 1 \bmod 4$, there are *more* algebraic integers in $\mathbb{Q}(\sqrt{D})$ ...

Let tr and N be Galois trace and norm $k \to \mathbb{Q}$. In terms of these, we know the minimal polynomial for α is $x^2 - \text{tr}\alpha \cdot x + N\alpha$. Thus, in a quadratic extension, α is an algebraic integer if and only both *trace* and *norm* are in $\mathbb{Z}$. Write $\alpha = a + b\sqrt{D}$ with $a, b \in \mathbb{Q}$.

The integrality condition is that $2a \in \mathbb{Z}$ and $a^2 - b^2 D \in \mathbb{Z}$. Try to *solve* for *rational integrality* conditions on a, b.

From the first condition, at worst $a \in \frac{1}{2}\mathbb{Z}$. With $a = a'/2$ and $b = b'/2$, the second condition becomes $a'^2 - b'^2 D \in 4\mathbb{Z}$.

Since the only squares mod 4 are $0, 1$, for $D = 2, 3 \bmod 4$ actually $a', b' \in 2\mathbb{Z}$, so $a, b \in \mathbb{Z}$.

But for $D = 1 \bmod 4$, the condition is met for $a' = b' \bmod 2$!!! That is, the ring $\mathfrak{o}$ of algebraic integers in $k = \mathbb{Q}(\sqrt{D})$ for square-free integer D is

$$\mathfrak{o} \;=\; \begin{cases} \mathbb{Z}[\sqrt{D}] & (\text{for } D = 2, 3 \bmod 4) \\ \mathbb{Z}[\frac{1+\sqrt{D}}{2}] & (\text{for } D = 1 \bmod 4) \end{cases}$$

Indeed, we already knew an example of the sense of this: the cube root of unity $\omega = \frac{-1+\sqrt{-3}}{2}$ satisfies $\omega^2 + \omega + 1 = 0$.

Caution: We will see that *ignoring* these 'extra' algebraic integers would be a fatal mistake: the resulting rings are very bad, *not* Dedekind rings, exactly because they are *not integrally closed*, that is, they omit elements of their *fraction fields* integral over $\mathbb{Z}$.

[6.2] Example: Cyclotomic fields $k = \mathbb{Q}(\omega)$, where ω is a primitive n^{th} root of unity. Since cyclotomic polynomials Φ_n are monic with integer coefficients, certainly ω is an algebraic integer.

So the ring $\mathfrak{o}$ of algebraic integers in $k = \mathbb{Q}(\omega)$ *contains* $\mathbb{Z}[\omega]$.

In fact, $\mathfrak{o} = \mathbb{Z}[\omega]$, but this is not so easy to prove for $n \geq 5$. The sane proof uses ideas about *localization*, *completion*, *discriminant*, *different* [sic], and *ramification*.

It is a fool's errand to try to prove $\mathfrak{o} = \mathbb{Z}[\omega]$ by writing out the minimal polynomial of $a + b\omega + c\omega^2 + \ldots$ and examining the integrality conditions.

[6.3] Example: Adjoining roots, for example, prime p-order roots $k = \mathbb{Q}(\sqrt[p]{D})$ of square-free integers D. Certainly $\sqrt[p]{D}$ is an algebraic integer, so the ring $\mathfrak{o}$ of algebraic integers *contains* $\mathbb{Z}[\sqrt[p]{D}]$.

For $D \neq 1 \bmod p^2$, in fact, $\mathfrak{o} = \mathbb{Z}[\sqrt[p]{D}]$. For $D = 1 \bmod p^2$, in parallel with the square-root story, $\mathfrak{o}$ is of index p above $\mathbb{Z}[\sqrt[3]{D}]$, also containing

$$\frac{1 + \sqrt[p]{D} + \ldots + \sqrt[p]{D}^{p-1}}{p}$$

For example, the ring $\mathfrak{o}$ of integers in $\mathbb{Q}(\sqrt[3]{10})$ is

$$\mathfrak{o} \;=\; \mathbb{Z} \;+\; \mathbb{Z} \cdot \sqrt[3]{10} \;+\; \mathbb{Z} \cdot \frac{1 + \sqrt[3]{10} + \sqrt[3]{10}^2}{3}$$

As with cyclotomic fields, it is unwise to try prove this *directly*.

Why are these ***rings*****?** Why are sums and products of algebraic integers again integral?

This issue is similar to the issue of proving that sums and products of *algebraic* numbers α, β (over $\mathbb{Q}$, for example) are again *algebraic*. Specifically, do *not* try to explicitly find a polynomial P with rational coefficients and $P(\alpha + \beta) = 0$, in terms of the minimal polynomials of α, β.

The methodological point in the latter is first that it is not *required* to explicitly determine the minimal polynomial of $\alpha + \beta$.

Second, about algebraic extensions, to *avoid* computation, *recharacterization* of the notion of *being algebraic over...* is needed: an element α of a field extension K/k is *algebraic* over k if $k[\alpha]$, the ring of values of polynomials on α, is a finite-dimensional k-vectorspace.

Recharacterization of integrality: Let K/k be a field extension, $\mathfrak{o}$ a ring in k with field of fractions k.

We already know that $\alpha \in K$ is *integral over* $\mathfrak{o}$ if $f(\alpha) = 0$ for *monic* f in $\mathfrak{o}[x]$.

[6.4] Claim: Integrality of α over $\mathfrak{o}$ is equivalent to the condition that there is a non-zero, finitely-generated $\mathfrak{o}$-module M inside K such that $\alpha M \subset M$.

Proof: On one hand, for α integral, with $n = [k(\alpha) : k]$, the $\mathfrak{o}$-module generated by $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ is finitely-generated and is stabilized by α...

On the other hand, suppose $\alpha M \subset M$, where M has $\mathfrak{o}$-generators $m_1, \ldots, m_n$. Then there are $c_{ij} \in \mathfrak{o}$ such that $\alpha m_i = \sum_j c_{ij} m_j$, giving a system of n linear equations inside the field K:

$$\left\{\begin{array}{lcccccc} \alpha m_1 & = & c_{11} m_1 & + & c_{12} m_2 & + \ldots + & c_{1n} m_n \\ & \ldots & & & & & \\ \alpha m_n & = & c_{n1} m_1 & + & c_{n2} m_2 & + \ldots + & c_{nn} m_n \end{array}\right.$$

or

$$\left\{\begin{array}{lcccccc} 0 & = & (c_{11} - \alpha) m_1 & + & c_{12} m_2 & + \ldots + & c_{1n} m_n \\ \ldots & & & & & & \\ 0 & = & c_{n1} m_1 & + & c_{12} m_2 & + \ldots + & (c_{nn} - \alpha) m_n \end{array}\right.$$

Existence of a non-zero solution $m_1, \ldots, m_n$ implies vanishing of determinant of

$$\begin{pmatrix} (c_{11} - \alpha) & c_{12} & \ldots & c_{1n} \\ & \ldots & & \\ c_{n1} & c_{12} & \ldots & (c_{nn} - \alpha) \end{pmatrix}$$

giving a monic equation satisfied by α !!! ///

[6.5] Corollary: In an algebraic field extension K/k, where k is the field of fractions of a ring $\mathfrak{o}$, the set $\mathfrak{O}$ of elements of K *integral* over $\mathfrak{o}$ is a *ring.*

Proof: Let $\alpha, \beta \in \mathfrak{O}$, stabilizing non-zero, finitely-generated $\mathfrak{o}$-modules $M = \langle m_1, \ldots, m_\mu \rangle$ and $N = \langle n_1, \ldots, n_\nu \rangle$. Then the $\mathfrak{o}$-module $M \cdot N$ generated by all products $m_i n_j$ is non-zero, finitely-generated, and is stabilized by $\alpha + \beta$ and by $\alpha \cdot \beta$ (!) ///

[6.6] Corollary: In the field extension $\overline{\mathbb{Q}}/\mathbb{Q}$, the collection of all algebraic integers really is a *ring.* ///

For a ring $\mathfrak{o}$ inside a field K, the ring $\mathfrak{O}$ of all elements of K *integral over* $\mathfrak{o}$ is the **integral closure** of $\mathfrak{o}$ in K.

Somewhat in parallel to development of the basics of *algebraic field theory*, some unexciting things need to be checked. First, from the monic-polynomial definition,

- For $\alpha \in K$, an algebraic field extension of the field of fractions k of $\mathfrak{o}$, for some $0 \neq c \in \mathfrak{o}$ the multiple $c \cdot \alpha$ is *integral* over $\mathfrak{o}$.
- For $\mathfrak{O}$ integral over $\mathfrak{o}$, for any ring hom f sending $\mathfrak{O}$ somewhere, $f(\mathfrak{O})$ is integral over $f(\mathfrak{o})$.
- For $\mathfrak{O}$ integral over $\mathfrak{o}$, if $\mathfrak{O}$ is finitely-generated as an $\mathfrak{o}$-*algebra*, then it is finitely-generated as an $\mathfrak{o}$-*module.*
- *Transitivity:* For rings $A \subset B \subset C$ with B is integral over A and C integral over B, C is integral over A.

Let's prove the less-intuitive facts that need the recharacterization: For $\mathfrak{O}$ finitely-generated as an $\mathfrak{o}$-*algebra*, use induction on the number of algebra generators. This reduces to the step where $\mathfrak{O} = \mathfrak{o}[\alpha]$, and α is integral over $\mathfrak{o}$. Ah! But proving that $\mathfrak{o}[\alpha]$ is a finitely-generated $\mathfrak{o}$-*module* in this induction step is exactly the recharacterization of integrality! Ha. ///

Use the previous to prove the more interesting-sounding *transitivity* of integrality. In $A \subset B \subset C$, any $z \in C$ satisfies an integral equation $z^n + b_{n-1}z^{n-1} + \ldots + b_1 z + b_o = 0$ with $b_i \in B$. The ring $B' = A[b_{n-1}, \ldots, b_o]$ is a finitely-generated A-*algebra*, so by the previous it is a finitely-generated A-*module*. Since z satisfies that monic, $B'[z]$ is also a finitely-generated A-*module*. And since z satisfies that monic, multiplication by z stabilizes $B'[z]$. The latter is finitely-generated over A, so z is integral over A. ///

Caution: Returning to the point that it would be a fatal mistake to ignore the notion of integrality, for example, by discarding algebraic numbers that *are* integral over $\mathbb{Z}$, but meet naive expectations:

[6.7] Claim: UFD's $\mathfrak{o}$ are *integrally closed* (in their fraction fields k).

Proof: Let a/b be integral over $\mathfrak{o}$, satisfying

$$(a/b)^n + c_{n-1}(a/b)^{n-1} + \ldots + c_o \;=\; 0$$

with $c_i \in \mathfrak{o}$. Multiplying out,

$$a^n + c_{n-1}a^{n-1}b + \ldots + b^n c_o \;=\; 0$$

If a prime π in $\mathfrak{o}$ divides b, then it divides a, by unique factorization. Thus, taking a/b *in lowest terms* shows that b is a unit. ///

[6.8] Example: Inside quadratic field extensions $k = \mathbb{Q}(\sqrt{D})$ of $\mathbb{Q}$, with D a square-free integer.

$$\mathfrak{o} \;=\; \begin{cases} \mathbb{Z}[\sqrt{D}] & \text{(for } D = 2, 3 \bmod 4) \\ \\ \mathbb{Z}[\frac{1+\sqrt{D}}{2}] & \text{(for } D = 1 \bmod 4) \end{cases}$$

[6.9] Claim: For a PID $\mathfrak{o}$ with fraction field k, for a finite *separable* field extension K/k, the integral closure $\mathfrak{O}$ of $\mathfrak{o}$ in K is a free $\mathfrak{o}$-module of rank $[K : k]$.

Preliminary view of proof: $\mathfrak{O}$ is certainly torsion-free as $\mathfrak{o}$-module, but how to get finite-generation, to invoke the structure theorem? The presence of the separability hypothesis is a hint that something is more complicated than one might imagine. In fact, it is wise to prove a technical-sounding thing:

[6.10] Claim: For an integrally closed (in its fraction field k), *Noetherian* [reviewed below] ring $\mathfrak{o}$, the integral closure $\mathfrak{O}$ of $\mathfrak{o}$ in a finite *separable* [reviewed below] field extension K/k is a finitely-generated $\mathfrak{o}$-module.

[6.11] Remark: For such reasons, *Dedekind domains* (below) need Noetherian-ness. Once things are not quite PIDs, Noetherian-ness is needed. *Separability* of field extensions is essential, too!

Separability: This is 'just' field theory... Recall: α in an algebraic field extension K/k is *separable* over k when its minimal polynomial over k has no repeated factors. Equivalently, there are $[k(\alpha) : k]$ *different* imbeddings of $k(\alpha)$ into an algebraic closure $\overline{k}$.

A finite field extension K/k is *separable* when there are $[K : k]$ different imbeddings of K into $\overline{k}$.

The *theorem of the primitive element* asserts that a finite separable extension can be generated by a single element.

A less-often emphasized, but important, result:

[6.12] Claim: For a finite separable field extension K/k, the *trace pairing* $\langle \alpha, \beta \rangle = \mathrm{tr}_{K/k}(\alpha\beta)$ is *non-degenerate*, in the sense that, given $0 \neq \alpha \in K$, there is $\beta \in K$ such that $\mathrm{tr}_{K/k}(\alpha\beta) \neq 0$.

Equivalently, $\mathrm{tr}_{K/k} : K \to k$ is not the 0-map. For fields of characteristic 0, this non-degeneracy is easy: for $[K : k] = n$ and for $\alpha \in k$,

$$\mathrm{tr}_{K/k} \frac{1}{n}\alpha \;=\; \frac{1}{n}\mathrm{tr}_{K/k}\alpha \;=\; \frac{1}{n}(\underbrace{\alpha + \ldots + \alpha}_{n}) \;=\; \alpha$$

But we need/want this non-degeneracy for finite fields $\mathbb{F}_q$ and for *function fields* $\mathbb{F}_q(x)$, in positive characteristic.

The decisive preliminary is *linear independence of characters*: given $\chi_1, \ldots, \chi_n$ distinct group homomorphisms $K^\times \to \Omega^\times$ for fields K, Ω, for any coefficients α_j's in Ω,

$$\alpha_1\chi_1 + \ldots + \alpha_n\chi_n = 0 \implies \text{all } \alpha_j = 0$$

Proof: Suppose $\alpha_1\chi_1 + \ldots + \alpha_n\chi_n = 0$ is the *shortest* such non-trivial relation, renumbering so that no $\alpha_j = 0$. The meaning of the equality is that

$$\alpha_1\chi_1(x) + \ldots + \alpha_n\chi_n(x) \;=\; 0 \in \Omega \qquad\qquad (\text{for all } x \in K^\times)$$

Since $\chi_1 \neq \chi_2$, there is $y \in K^\times$ such that $\chi_1(y) \neq \chi_2(y)$. Replace x by xy:

$$\alpha_1\chi_1(y)\chi_1(x) + \ldots + \alpha_n\chi_n(y)\chi_n(x) \;=\; 0 \qquad\qquad (\text{for all } x \in K^\times)$$

Divide the latter relation by $\chi_1(y)$, and subtract from the first:

$$\alpha_2\big(1 - \chi_2(y)\big)\chi_2 + \ldots + \alpha_n\big(1 - \chi_n(y)\big)\chi_n \;=\; 0$$

This is shorter, contradiction. ///

To prove that the Galois trace map on a finite separable K/k is not identically 0, observe that the distinct field imbeddings $\sigma_j : K \to \overline{k}$ *are* (distinct) multiplicative characters $K^\times \to \overline{k}^\times$.

Trace is $\mathrm{tr}_{K/k} = \sum_j \sigma_j = \sum_j 1 \cdot \sigma_j$. This linear combination is not identically 0. ///

Recall that a commutative ring R is *Noetherian* when any of the following equivalent conditions is met:

- Any ascending chain of ideals $I_1 \subset I_2 \subset \ldots$ in R *stops*, in the sense that there is n_o such that $I_n = I_{n_o}$ for $n \geq n_o$.
- Every ideal in R is a finitely-generated R-module

[6.13] Example: PIDs R are Noetherian!

Proof: Let $\bar{x}_1\rangle \subset \langle x_2\rangle \subset \ldots$ be a chain of (principal!) ideals. Let I be the *union* I. It is a principal ideal $\langle y\rangle$. There is a *finite* expression $y = r_1x_{i_1} + \ldots + r_nx_{i_n}$ with $r_i \in R$. Letting j be the max of the i_ℓ's, all x_{i_j}'s are in $\langle x_j\rangle$, so $y \in \langle x_j\rangle$, and the chain stabilizes at $\langle x_j\rangle$. ///

We will eventually need a big theorem: **Hilbert Basis Theorem:** For Noetherian commutative R, the polynomial ring $R[x]$ is Noetherian.

The tangible case $R = k[x_1, \ldots, x_n]$ with a field k was treated by Hilbert pre-1900. The Noetherian condition was abstracted 20+ years later by Noether.

Proof: that the integral closure $\mathfrak{O}$ of Noetherian, integrally closed $\mathfrak{o}$ (in its fraction field k) in a finite, separable field extension K/k is a *finitely-generated* $\mathfrak{o}$-module... *not* assuming $\mathfrak{o}$ is a PID or Dedekind... but assuming things about Noetherian rings and modules for a moment...

Subclaim: non-degeneracy of the trace pairing $\langle\alpha, \beta\rangle = \mathrm{tr}_{K/k}(\alpha\beta)$ as a non-degenerate k-valued k-bilinear form on $K \times K$, viewing K as a k-vectorspace, implies that

$$\alpha \longrightarrow \Big(\beta \longrightarrow \langle\alpha, \beta\rangle\Big)$$

gives an *isomorphism* $K \to K^* = \mathrm{Hom}_k(K,k)$, the k-linear *dual* of K. Indeed, the non-degeneracy proves that the kernel of the map is $\{0\}$, and then dimension-counting proves it's an isomorphism.

Let $\alpha_1, \ldots, \alpha_n$ be a k-basis for K. Multiplying each α_i by a suitable $0 \neq c_i \in \mathfrak{o}$, we can assume $\alpha_i \in \mathfrak{O}$. Let α'_j be the dual basis, that is, $\langle \alpha'_i, \alpha_j \rangle = \delta_{ij}$. Let $0 \neq c \in \mathfrak{o}$ be such that $c\alpha'_i \in \mathfrak{O}$ for all i.

For $\beta \in \mathfrak{O}$, $\beta \cdot c\alpha'_i \in \mathfrak{O}$, and $\mathrm{tr}(\beta \cdot c\alpha) \in \mathfrak{o}$. The coefficients $c_i \in k$ in an expression $\beta = \sum_i c_i \alpha_i$ are picked off by $\mathrm{tr}_{K/k}(\beta \cdot c\alpha'_j) = cc_j$. Since $\mathfrak{o}$ is integrally closed, $cc_j \in \mathfrak{o}$. This holds for all $\beta \in \mathfrak{O}$, so

$$\mathfrak{O} \;\subset\; c^{-1} \cdot \Big(\mathfrak{o} \cdot \alpha_1 + \ldots + \mathfrak{o} \cdot \alpha_n\Big)$$

Finitely-generated modules over Noetherian rings are Noetherian, and submodules $\mathfrak{O}$ of Noetherian are Noetherian, so $\mathfrak{O}$ is a finitely-generated $\mathfrak{o}$-module. ///

Better prove those last points about Noetherian-ness! ... Important features of modules over Noetherian rings! ...

So, step back...: as in many sources, e.g., Lang's *Algebra*, ... This algebra is *important* in algebraic number theory, and in all forms of algebraic geometry... because Noetherian-ness is the non-negotiable thing that makes many *other* things work...

A *module* M over a commutative ring R (itself not necessarily Noetherian) is *Noetherian* when it satisfies any of the following (provably, below) equivalent conditions:

• Every submodule of M is finitely-generated.
• Every ascending chain of submodules $M_1 \subset M_2 \subset \ldots$ eventually *stabilizes*, that is, $M_i = M_{i+1}$ beyond some point.
• Any non-empty set S of submodules has a *maximal element*, that is, an element $M_o \in S$ such that $N \supset M_o$ and $N \in S$ implies $N = M_o$.

Proof: of equivalence: Assume the first condition, and prove the second. By assumption, the $N = \bigcup_i M_i$ is finitely-generated, by some $m_1, \ldots, m_n$. Each m_i occurs in some one of the M_j, so there is some index j so that *all* m_i are in M_j. Thus, $M_j = M_{j+1} = \ldots$.

Assume the second condition, and prove the third. Take $M_1 \in S$. If it is maximal, we're done. If not, let $M_2 \supset M_1$ be strictly larger. By induction, either construct an infinite ascending chain, which is assumed impossible, or find a maximal element.

Assume the third condition, and prove the first. Fix a submodule N of M. If a given element $n_1 \in N$ generates N, we're done, otherwise choose $n_2 \in N$ but not in $\langle n_1 \rangle$. Continuing, either we find a finite set of generators for N, or obtain a ascending chain

$$\langle n_1 \rangle \subset \langle n_1, n_2 \rangle \subset \ldots$$

By assumption, the set of these has a maximal element, some $\langle n_1, \ldots, n_j \rangle$, which is N, proving finite generation. ///

[6.14] Claim: Submodules and quotient modules of Noetherian modules are Noetherian. Conversely, for $M \subset N$, if M and N/M are Noetherian, then N is.

Proof: The first characterization of Noetherian-ness gives the assertion for submodules. For quotients $q : N \to Q$, for any chain $Q_1 \subset Q_2 \subset \ldots$ inside Q, the inverse images $q^{-1}Q_i$ make a chain in N, which must stabilize, proving that the images stabilize.

Conversely, attach to $X \subset N$ the pair $pX = (X \cap M, (X+M)/M)$. We claim that a chain $X_1 \subset X_2 \subset \ldots$ stabilizes if and only if $X_i \cap M$ and $(X_i + M)/M$ stabilize: *Subclaim:* if $X \subset Y$ and $pX = pY$, then $X = Y$.

Indeed, for $y \in Y$, $(X+M)/M = (Y+M)/M)$ implies existence of $m \in M$ and $x \in X$ such that $x+m=y$. Thus,

$$x - y \;=\; -m \;\;\in\;\; Y \cap M \;=\; X \cap M$$

Then $y = x + m \in X + (X \cap M) \subset X$, proving the subclaim. For $X_1 \subset X_2 \subset \ldots$, the associated pairs are ascending chains in M and N/M, so stabilize, and then X_i stabilizes. ///

That is, in a *short exact sequence*

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

(meaning that $A \to B$ is *injective*, that the image of $A \to B$ is the kernel of $B \to C$, and that $B \to C$ is *surjective*), Noetherian-ness of B is equivalent to Noetherian-ness of A and C.

[6.15] Corollary: For M, N Noetherian, $M \oplus N$ is Noetherian. Arbitrary finite sums of Noetherian modules are Noetherian.

Proof: $0 \to M \to M \oplus N \to N \to 0$ is exact. Induction. ///

Now we need to connect to (probably finitely-generated) modules over a *Noetherian ring.* The Noetherian-ness of the ring itself has a (not-surprising) impact on the behavior of modules over it.

Again, a commutative *ring* R is Noetherian if it is Noetherian as a module over itself. This is equivalent to the property that every submodule, that is, every ideal, is finitely-generated.

[6.16] Claim: A finitely-generated module M over a Noetherian ring R is a Noetherian module.

Proof: Let $m_1, \ldots, m_n$ generate M, so there is a surjection $\underbrace{R \oplus \ldots \oplus R}_{n} \longrightarrow M$ by

$$r_1 \oplus \ldots \oplus r_n \;\longrightarrow\; \sum_i r_i \cdot m_i$$

The sum $R \oplus \ldots \oplus R$ is Noetherian, and the image/quotient is Noetherian. ///

Don't forget: this completes the discussion of the proof that *The integral closure $\mathfrak{O}$ of Noetherian, integrally closed $\mathfrak{o}$ in a finite, separable field extension K/k is a* **finitely-generated** *$\mathfrak{o}$-module.*

The end of the proof had $\mathfrak{O}$ sitting inside a finitely-generated module:

$$\mathfrak{O} \;\subset\; c^{-1} \cdot \Big(\mathfrak{o} \cdot \alpha_1 + \ldots + \mathfrak{o} \cdot \alpha_n\Big)$$

Finitely-generated modules over Noetherian rings $\mathfrak{o}$ are Noetherian, and submodules $\mathfrak{O}$ of Noetherian modules are Noetherian, so $\mathfrak{O}$ is finitely-generated. ///

Finally, this returns to the proof that, for $\mathfrak{o}$ a PID, $\mathfrak{O}$ is a *free* $\mathfrak{o}$-module of rank $[K:k]$.

By now, we know that $\mathfrak{O}$ is *finitely-generated* over $\mathfrak{o}$. It is *torsionless* because $\mathfrak{o} \subset \mathfrak{O} \subset K$, a field. Invoking the structure theory of finitely-generated modules over PIDs, $\mathfrak{O}$ is *free.* Let $\alpha_1, \ldots, \alpha_n$ be an $\mathfrak{o}$-basis.

We claim that $\{\alpha_i\}$ is also a k-basis for K, which would prove $[K:k]=n$. They *span*, because, given $\beta \in K$, there is $0 \neq c \in \mathfrak{o}$ such that $c\beta \in \mathfrak{O}$. There are $c_j \in \mathfrak{o}$ such that $c\beta = \sum_i c_j \alpha_j$. Then $\beta = \sum_i c^{-1} c_j \alpha_i$.

They are *linearly independent* over k: for $\sum_i x_i \alpha_i = 0$ with $x_i \in k$, take $0 \neq c \in k$ such that all $cx_i \in \mathfrak{o}$. Then $\sum_i (cx_i)\alpha_i = 0$ is a non-trivial relation over $\mathfrak{o}$, contradiction. ///

[6.17] Example: Function fields in one variable (over finite fields): The polynomial rings $\mathbb{F}_q[X]$ are as well-behaved as $\mathbb{Z}$. Their fields of fractions $\mathbb{F}_q(X)$, rational functions in X with coefficients in $\mathbb{F}_q$, are as well-behaved as $\mathbb{Q}$.

For that matter, for *any* field E, $E[X]$ is Euclidean, so is a PID and a UFD. E *finite* is most similar to $\mathbb{Z}$, especially that the *residue fields are finite:* quotient $\mathbb{F}_q[X]/\langle f\rangle$ with f a *prime* (=positive-degree monic polynomial) are finite fields.

The algebra of integral closures of $\mathfrak{o} = \mathbb{F}_q[X]$ in finite separable fields extensions of $k = \mathbb{F}_q(X)$ is identical to that with $\mathbb{Z}$ and $\mathbb{Q}$ at the bottom.

But to talk about the *geometry*, it is useful to think about $\mathbb{C}[X]$...

Since $\mathbb{C}$ is algebraically closed, the non-zero prime ideals in $\mathbb{C}[X]$ are $\langle X - z\rangle$, for $z \in \mathbb{C}$.

That is, the point $z \in \mathbb{C}$ is the simultaneous vanishing set of the ideal $\langle X - z\rangle$.

The *point at infinity* ∞ is the vanishing set of $1/X$, but $1/X$ is not in $\mathbb{C}[X]$, so we can't talk about the ideal generated by it...

Revise: points $z \in \mathbb{C}$ are in bijection with *local rings* $\mathfrak{o} \subset \mathbb{C}(X)$, meaning $\mathfrak{o}$ has a *unique maximal (proper) ideal* $\mathfrak{m}$, by

$$z \longleftrightarrow \mathfrak{o}_z = \{\frac{P}{Q} \;:\; P, Q \in \mathbb{C}[X],\ Q(z) \neq 0\}$$

$$\mathfrak{m}_z \;=\; \{\frac{P}{Q} \;:\; P, Q \in \mathbb{C}[X],\ Q(z) \neq 0,\ P(z) = 0\}$$

That is, $\mathfrak{o}_z$ is the ring of rational functions *defined at* z, and its unique maximal ideal $\mathfrak{m}_z$ is the functions *(defined and) vanishing at* z. These are also referred to as

$$\mathfrak{o}_z \;=\; \textit{localization} \text{ at } \langle X - z\rangle \text{ of } \mathbb{C}[X] \;=\; S^{-1}\cdot\mathbb{C}[X] \qquad\qquad (\text{where } S = \mathbb{C}[X] - (X - z)\mathbb{C}[X])$$

These *localizations* of the PID $\mathbb{C}[X]$ are still PIDs. In fact, again, each such has a single non-zero prime ideal $\langle X - z\rangle$. In $\mathfrak{o}_z$ every proper ideal is of the form $(X - z)^n \cdot \mathfrak{o}_z$ for some $0 < n \in \mathbb{Z}$.

As usual, instead of trying to evaluate something at $X = \infty$, evaluate $1/X$ at 0:

$$\mathfrak{o}_\infty \;=\; \{f(X) = g(1/X) \;:\; g \text{ is defined at } 0\} \;=\; \{\frac{P(1/X)}{Q(1/X)} \;:\; P, Q \in \mathbb{C}[X],\ Q(0) \neq 0\}$$

$$\mathfrak{m}_\infty \;=\; \{f(X) = g(1/X) \in \mathfrak{o}_\infty \;:\; g(0) = 0\} \;=\; \{\frac{P(1/X)}{Q(1/X)} \;:\; P, Q \in \mathbb{C}[X],\ Q(0) \neq 0,\ P(0) = 0\}$$

From one viewpoint, a (compact, connected) *Riemann surface* M is/corresponds (!?) to a finite field extension K of $k = \mathbb{C}(X)$. The finite points of the Riemann surface M are the zero-sets of non-zero prime ideals of the *integral closure* $\mathfrak{O}$ of $\mathfrak{o} = \mathbb{C}[X]$ in K. (In fact, the ring $\mathfrak{O}$ is *Dedekind*.)

[6.18] Claim: For *typical* $z \in \mathbb{C}$, the prime ideal $\langle X - z\rangle = (X - z)\mathbb{C}[X]$ gives rise to $(X - z)\mathfrak{O} = \mathfrak{P}_1 \ldots \mathfrak{P}_n$, where $n = [K : k]$. That is, n points on M *lie over* $z \in \mathbb{C}$:

Proof: We can reduce to the case that $K = \mathbb{C}(X, Y)$ with Y satisfying a *monic* polynomial equation $f(X, Y) = 0$ with coefficients in $\mathbb{C}[X]$, and f of degree $[K : k]$. Do the usual computation

$$\mathfrak{O}/(X - z)\mathfrak{O} \;=\; \mathbb{C}[X, T]/\langle X - z,\ f(X, T)\rangle \;\approx\; \mathbb{C}[T]/\langle f(z, T)\rangle \;\approx\; \mathbb{C}[T]/\langle (T - w_1)(T - w_2)\ldots(T - w_n)\rangle$$

$$\approx\; \frac{\mathbb{C}[T]}{\langle T - w_1\rangle} \oplus \frac{\mathbb{C}[T]}{\langle T - w_2\rangle} \oplus \ldots \oplus \frac{\mathbb{C}[T]}{\langle T - w_n\rangle} \;\approx\; \mathbb{C} \oplus \mathbb{C} \oplus \ldots \oplus \mathbb{C}$$

for distinct w_j. By the Lemma proven earlier, $\mathfrak{O}/(X - z)\mathfrak{O}$ is a product of n prime ideals. ///

For example, for the *elliptic curve*

$$Y^2 \;=\; X^3 + aX + b \qquad\qquad (\text{with } a, b \in \mathbb{C})$$

where $X^3 + aX + b = 0$ has distinct roots, we have (!?) $\mathfrak{O} = \mathbb{C}[X, Y] \approx \mathbb{C}[X, T]/\langle T^2 - X^3 - aX - b\rangle$ with a further indeterminate T, and the usual trick gives

$$\mathfrak{O}/(X-z)\mathfrak{O} \;=\; \mathbb{C}[X,T]/\langle X-z,\; T^2 - X^3 - aX - b\rangle \;\approx\; \mathbb{C}[T]/\langle T^2 - z^3 - az - b\rangle \;\approx\; \mathbb{C}[T]/\langle (T-w_1)(T-w_2)\rangle$$

$$\approx\; \frac{\mathbb{C}[T]}{\langle T - w_1\rangle} \oplus \frac{\mathbb{C}[T]}{\langle T - w_2\rangle} \;\approx\; \mathbb{C} \oplus \mathbb{C}$$

for distinct w_j: $\mathfrak{O}/(X-z)\mathfrak{O}$ is a product of 2 prime ideals.

To talk about *points at infinity*, either replace $\mathfrak{o} = \mathbb{C}[X]$ by $\mathfrak{o} = \mathbb{C}[1/X]$, or use the *local ring* description: given a *local* ring $\mathfrak{o}_z \subset k = \mathbb{C}(X)$ corresponding to either $z \in \mathbb{C}$ or $z = \infty$, let $\mathfrak{O}$ be the integral closure of $\mathfrak{o}_z$ in $K = \mathbb{C}(X, Y)$. The maximal ideal $\mathfrak{m}_z$ of $\mathfrak{o}_z$ generates a product of prime (maximal) ideals in $\mathfrak{O}$:

$$\mathfrak{m}_z \cdot \mathfrak{O} \;=\; \mathfrak{P}_1 \ldots \mathfrak{P}_n \qquad\qquad (\text{with } n = [K : k])$$

Pick a constant $C > 1$. Doesn't matter much... For each $z \in \mathbb{C} \cup \{\infty\}$, there is the $(X - z)$-adic, or just z-adic, norm

$$\Big|(X-z)^n \cdot \frac{P(X)}{Q(X)}\Big| \;=\; C^{-n}$$

The z-adic completions of $\mathbb{C}[X]$ and $\mathbb{C}(X)$ are defined as usual. Hensel's lemma applies.

7. *Coverings of the affine line over* $\mathbb{C}$

With a finite field as scalars, instead of $\mathbb{C}$, for $\mathbb{F}_q[X]$, the *zeta function* is

$$Z(s) \;=\; \sum_{\text{monic } f} \frac{1}{(\#\mathbb{F}_p[X]/\langle f\rangle)^s} \;=\; \sum_{\text{monic } f} \frac{1}{q^{s \deg f}}$$

where

$$\#\text{irred monics deg } d \;=\; \frac{\#\text{ elements degree } d \text{ over } \mathbb{F}_q}{\#\text{in each Galois conjugacy class}}$$

$$=\; \frac{1}{d}\Big(q^d - \sum_{\text{prime } p|d} q^{d/p} + \sum_{\text{distinct } p_1,p_2|d} q^{d/p_1p_2} - \sum_{\text{distinct } p_1,p_2,p_3|d} q^{d/p_1p_2p_3} + \ldots\Big)$$

The idea is that the geometry and function theory of compact, connected Riemann surfaces (finite-degree coverings of the affine line) suggests attributes in the finite-field case. Therefore, we consider some ideas about compact, connected Riemann surfacesin this context.

$\mathbb{C}$ is *the affine complex line* (not *plane*). Since $\mathbb{C}$ is algebraically closed, the non-zero prime ideals in $\mathbb{C}[X]$ are $\langle X - z\rangle$, for $z \in \mathbb{C}$. The point $z \in \mathbb{C}$ is the simultaneous vanishing set of the ideal $\langle X - z\rangle$.

Discussion of *the point at infinity* ∞ is postponed a bit: arguably, ∞ is the vanishing set of $1/X$ .... but *where???* Also, $1/X$ is not in $\mathbb{C}[X]$, so we can't talk about the ideal generated by it...

From one viewpoint, a (compact, connected) *Riemann surface* M is/corresponds (!?) to a finite field extension K of $k = \mathbb{C}(X)$.

Since $\mathbb{C}(X)$ has characteristic 0, K/k is *separable*, so is generated by a single element Y, satisfying a monic $f(Y) = 0$, where f has coefficients in $\mathbb{C}(X)$: with $a_j(X), b_j(X) \in \mathbb{C}[X]$, assuming $a_j(X)/b_j(X)$ in lowest terms,

$$Y^n + \frac{a_{n-1}(X)}{b_{n-1}(X)} Y^{n-1} + \ldots + \frac{a_1(X)}{b_1(X)} Y + \frac{a_o(X)}{b_o(X)} \;=\; 0$$

To get rid of the denominators, replace Y by $Y/b_{n-1}(X)\ldots b_1(X)b_o(X)$ and multiply through by

$$\big(b_{n-1}(X)\ldots b_1(X)b_o(X)\big)^n$$

After relabelling, without loss of generality, with $a_j(X) \in \mathbb{C}[X]$,

$$Y^n + a_{n-1}(X)Y^{n-1} + \ldots + a_1(X)Y + a_o(X) \;=\; 0$$

Note that these normalizations make Y *integral* over $\mathbb{C}[X]$.

The most immediate description of (the not-at-infinity points of) the Riemann surface associated to

$$f(X,Y) \;=\; Y^n + a_{n-1}(X)Y^{n-1} + \ldots + a_1(X)Y + a_o(X) \;=\; 0$$

is that, for each $z \in \mathbb{C}$, the n solutions $w_1, \ldots, w_n \in \mathbb{C}$ to

$$f(z,w) \;=\; w^n + a_{n-1}(z)w^{n-1} + \ldots + a_1(z)w + a_o(z) \;=\; 0$$

specify the points *above* z, or *over* z. That is, the Riemann surface is the graph of $f(z,w) = 0$ in $(z,w) \in \mathbb{C}^2$, and the normalizations above arrange the projection to the first coordinate an everywhere-defined at-most-n-to-one map.

The values of z for which the equation has *multiple roots* are the *ramified points.*

Ramification refers to the projection $\{(z,w) : f(z,w) = 0\} \to \mathbb{C}$ to the z-plane.

$F(w) = f(z,w)$ has repeated roots exactly when F, F' have a common factor. Apply *Euclidean algorithm* in $\mathbb{C}(X)[Y]$:

[7.1] Example: Ramification of $F(Y) = f(X,Y) = Y^5 - 5XY + 4$. Here $F'(Y) = 5Y^4 - 5X$, but discard the unit 5. One step of Euclid is

$$(Y^5 - 5XY + 4) - Y(Y^4 - X) \;=\; -4XY + 4$$

$-4X \in \mathbb{C}(X)^\times$, so replace $-4XY + 4$ with $Y - \frac{1}{X}$. The next step of Euclid would divide $Y^4 - X$ by $Y - \frac{1}{X}$. By the division algorithm, the remainder is the *value* of $Y^4 - X$ at $Y = 1/X$, namely, $\frac{1}{X^4} - X$.

Thus, the five ramified points of $f(z,w) = 0$ are where $z^5 = 1$. But, also, ... The (not-at-infinity) points of the Riemann surface M are the zero-sets of non-zero prime ideals of the *integral closure* $\mathfrak{O}$ of $\mathfrak{o} = \mathbb{C}[X]$ in K. (In fact, the ring $\mathfrak{O}$ is *Dedekind.*) As above, we have

Fact: For *typical* $z \in \mathbb{C}$, the prime ideal $\langle X - z\rangle = (X - z)\mathbb{C}[X]$ gives rise to $(X - z)\mathfrak{O} = \mathfrak{P}_1 \ldots \mathfrak{P}_n$, where $n = [K : k]$. That is, n points on M *lie over* $z \in \mathbb{C}$. ///

The *ramified* points are exactly those z such that $(X - z) \cdot \mathfrak{O}$ has a *repeated factor!!!* (We're not set up to address that yet...)

For example, for the *elliptic curve*

$$Y^2 \;=\; X^3 + aX + b \qquad\qquad \text{(with } a, b \in \mathbb{C}\text{)}$$

where $X^3 + aX + b = 0$ has distinct roots, we have (!?) $\mathfrak{O} = \mathbb{C}[X,Y] \approx \mathbb{C}[X,T]/\langle T^2 - X^3 - aX - b\rangle$ with a second indeterminate T, and the usual trick gives

$$\begin{aligned}
\mathfrak{O}/(X-z)\mathfrak{O} \;&=\; \mathbb{C}[X,T]/\langle X - z,\ T^2 - X^3 - aX - b\rangle \\
&\approx\; \mathbb{C}[T]/\langle T^2 - z^3 - az - b\rangle \\
&\approx\; \mathbb{C}[T]/\langle (T - w_1)(T - w_2)\rangle \\
&\approx\; \frac{\mathbb{C}[T]}{\langle T - w_1\rangle} \oplus \frac{\mathbb{C}[T]}{\langle T - w_2\rangle} \\
&\approx\; \mathbb{C} \oplus \mathbb{C}
\end{aligned}$$

for distinct w_j: $(X-z)\mathfrak{O}$ is an intersection of 2 prime ideals.

Example computation of integral closure: *hyperelliptic curves* (quadratic extensions of $\mathbb{C}(X)$)

$$Y^2 \;=\; P(X) \;=\; (X-z_1)\ldots(X-z_n) \qquad\qquad (\text{distinct } z_j)$$

[7.2] Claim: The integral closure $\mathfrak{O}$ of $\mathfrak{o} = \mathbb{C}[X]$ in $K = \mathbb{C}(X,Y)$ is $\mathfrak{O} = \mathbb{C}[X,Y]$.

Proof: Obviously $\mathbb{C}[X,Y] \subset \mathfrak{O}$. An element of $K = \mathbb{C}(X,Y)$ can be written uniquely as $a + bY$ with $a,b \in \mathbb{C}(X)$. For $b \neq 0$, the minimal polynomial of $a+bY$ is *monic*, with coefficients *trace* and *norm*, so integrality over $\mathfrak{o} = \mathbb{C}[X]$ is equivalent to *trace* and *norm* in $\mathbb{C}[X]$. The Galois conjugate of Y is $-Y$, so

$$2a \;\in\; \mathbb{C}[X] \qquad\qquad a^2 - b^2\cdot P \;\in\; \mathbb{C}[X]$$

$2 \in \mathbb{C}[X]^\times$, so $a \in \mathbb{C}[X]$. Thus, $b^2 \cdot P \in \mathbb{C}[X]$. Since P is square-free, writing $b = C/D$ with relatively prime polynomials C, D, we find $D \in \mathbb{C}[X]^\times$. Thus, $a, b \in \mathbb{C}[X]$. ///

Completions! Pick a constant $C > 1$. Doesn't matter much... For each $z \in \mathbb{C} \cup \{\infty\}$, there is the $(X-z)$-adic, or just z-adic, norm

$$\Big|(X-z)^n \cdot \frac{P(X)}{Q(X)}\Big|_z \;=\; C^{-n}$$

The z-adic completions of $\mathbb{C}[X]$ and of $\mathbb{C}(X)$ are defined as usual, denoted $\mathbb{C}[[X-z]]$ and $\mathbb{C}((X-z))$. High powers of $X-z$ are tiny, and *any* infinite sum

$$c_0 + c_1(X-z) + c_2(X-z)^2 + c_3(X-z)^3 + \ldots \qquad\qquad (\text{with } c_j \in \mathbb{C})$$

is *convergent*, by the ultrametric inequality. This warrants calling $\mathbb{C}[[X-z]]$ a *formal power series ring*, and $\mathbb{C}((X-z))$ the field of *formal finite Laurent series*. But the convergence is *genuine*.

Hensel's lemma applies: With monic $F(T) \in \mathbb{C}[[X]][T]$, given $\alpha_1 \in \mathbb{C}[[X-z]]$ with $F(\alpha_1) = 0 \bmod X-z$ with $F'(\alpha_1) \neq 0 \bmod X-z$, the recursion

$$\alpha_{n+1} \;=\; \alpha_n - \frac{F(\alpha_n)}{F'(\alpha_n)} \bmod (X-z)^{n+1}$$

gives $\alpha_\infty = \lim_n \alpha_n \in \mathbb{C}[[X-z]]$ with $F(\alpha_\infty) = 0$ in $\mathbb{C}[[X-z]]$, and α_∞ is the unique solution congruent to $\alpha_1 \bmod X-z$.

[7.3] Example: Any $\beta = c_0 + c_1(X-z) + c_2(X-z)^2 + \ldots$ with $c_o \neq 0$ is a *unit* in $\mathbb{C}[[X-z]]$.

Proof: Take $F(T) = \beta \cdot T - 1$ (actually, not monic, but nevermind...) and $\alpha_1 = c_o^{-1}$. ///

[7.4] Example: Any $\beta = c_0 + c_1(X-z) + c_2(X-z)^2 + \ldots$ with $c_o \neq 0$ has an n^{th} *root* in $\mathbb{C}[[X-z]]$.

Proof: Take $F(T) = T^n - \beta$ and $\alpha_1 \in \mathbb{C}$ any $\sqrt[n]{c_o}$. ///

[7.5] Example: For $f(X,T) \in \mathbb{C}[X,T]$, for $z, w_o \in \mathbb{C}$ such that $f(z,w_o) = 0$ but $\frac{\partial}{\partial w} f(z,w_o) \neq 0$, there is a unique $\alpha \in \mathbb{C}[[X-z]]$ of the form

$$\alpha \;=\; w_o + \text{higher powers of } X - z$$

giving

$$f(z,\alpha) \;=\; 0$$

Proof: The hypothesis is a very slight paraphrase of the hypothesis of Hensel's lemma. ///

[7.6] Theorem: All finite field extensions of $\mathbb{C}((X-z))$ are by adjoining solutions to $Y^e = X-z$ for $e = 2,3,4,\ldots$. [Pf later.]

These are (formal) *Puiseux expansions.* The simplicity of the theorem is suprising. It approximates the assertion that, *locally*, Riemann surfaces are either *covering spaces* of the z-plane, or concatenations of $w^e = z$.

The *local ring* inside the field $\mathbb{C}(X)$ corresponding to $z \in \mathbb{C}$, consisting of all rational functions *defined* at z, is

$$\mathfrak{o}_z \;=\; \mathbb{C}(X) \;\cap\; \mathbb{C}[[X-z]]$$

with unique maximal ideal

$$\mathfrak{m}_z \;=\; \mathbb{C}(X) \;\cap\; (X-z)\cdot\mathbb{C}[[X-z]]$$

The *point at infinity* can be discovered by noting a further local ring and maximal ideal:

$$\mathfrak{o}_\infty \;=\; \mathbb{C}(X) \cap \mathbb{C}[[1/X]] \qquad\qquad \mathfrak{m}_\infty \;=\; \mathbb{C}(X) \cap \frac{1}{X}\mathbb{C}[[1/X]]$$

Note that using $1/(X+1)$ achieves the same effect, because

$$\frac{1}{X+1} \;=\; \frac{1}{X}\cdot\frac{1}{1+\frac{1}{X}} \;=\; \frac{1}{X}\cdot\Big(1-\frac{1}{X}+(\frac{1}{X})^2-\ldots\Big) \;\in\; \frac{1}{X}\cdot\mathbb{C}[[1/X]]^\times$$

Puiseux expansions and field extensions of $\mathbb{C}((X-z))$. Introduction to Newton polygons!?

Completions of $\mathbb{C}[X]$ **and** $\mathbb{C}(X)$ Fix a constant $C > 1$...

For each $z \in \mathbb{C}$, there is the $(X-z)$-adic, or just z-adic, norm

$$\Big|(X-z)^n\cdot\frac{P(X)}{Q(X)}\Big|_z \;=\; C^{-n} \qquad\quad (P, Q \text{ prime to } X-z)$$

Completions of $\mathbb{C}[X]$ and of $\mathbb{C}(X)$ are $\mathbb{C}[[X-z]]$ and $\mathbb{C}((X-z))$, *formal power series ring*, and *field formal finite Laurent series.*

Hensel's lemma: With monic $F(T) \in \mathbb{C}[[X]][T]$, given $\alpha_1 \in \mathbb{C}[[X-z]]$ with $F(\alpha_1) = 0 \bmod X-z$, $F'(\alpha_1) \neq 0 \bmod X-z$, the recursion

$$\alpha_{n+1} \;=\; \alpha_n - \frac{F(\alpha_n)}{F'(\alpha_n)} \bmod (X-z)^{n+1}$$

gives $\alpha_\infty = \lim_n \alpha_n \in \mathbb{C}[[X-z]]$ with $F(\alpha_\infty) = 0$ in $\mathbb{C}[[X-z]]$, and α_∞ is the *unique* solution congruent to $\alpha_1 \bmod X-z$.

[7.7] Example: $\beta = c_0 + c_1(X-z) + \ldots$ with $c_o \neq 0$ is in $\mathbb{C}[[X-z]]^\times$.

Proof: $F(T) = \beta\cdot T - 1$ (not monic, nevermind) and $\alpha_1 = c_o^{-1}$. ///

[7.8] Example: Any $\beta = c_0 + c_1(X-z) + \ldots$ with $c_o \neq 0$ has an n^{th} *root* in $\mathbb{C}[[X-z]]$.

Proof: Take $F(T) = T^n - \beta$ and $\alpha_1 = \sqrt[n]{c_o}$. ///

[7.9] Example: For $f(X,T) \in \mathbb{C}[X,T]$, for $z, w_o \in \mathbb{C}$ with $f(z,w_o) = 0$ but $\frac{\partial}{\partial w}f(z,w_o) \neq 0$, there is a unique $\alpha \in \mathbb{C}[[X-z]]$ of the form

$$\alpha \;=\; w_o + \big(\text{higher powers of } X-z\big)$$

giving $f(z, \alpha) = 0$.

Proof: Hypothesis and conclusion are those of Hensel. ///

[7.10] Theorem: All finite field extensions of $\mathbb{C}((X-z))$ are by adjoining solutions to $Y^e = X - z$ for $e = 2, 3, 4, \ldots$. [Proof below.]

These are (formal) *Puiseux expansions.* The simplicity of the theorem is suprising. It approximates the assertion that, *locally*, Riemann surfaces are either *covering spaces* of the z-plane, or concatenations of $w^e = z$.

The proof invites extending Hensel's lemma to cover *factorization of polynomials.*

Paraphrase of Hensel: Consider

$$f(X,T) = T^n + a_{n-1}(X)T^{n-1} + \ldots + a_1(X)T + a_o(X)$$

with $a_j(X) \in \mathbb{C}[X]$ and such that the equation

$$f(0,w) = w^n + a_{n-1}(0)w^{n-1} + \ldots + a_1(0)w + a_o(0) \ = \ 0$$

has *distinct roots* in $\mathbb{C}$. Then there are n distinct solutions $\varphi_j \in \mathbb{C}[[X]]$ to $f(X,Y) = 0$. That is, $f(X,T)$ factors into *linear* factors:

$$T^n + a_{n-1}(X)T^{n-1} + \ldots + a_o(X) \ = \ (T-\varphi_1)(T-\varphi_2)\ldots(T-\varphi_n)$$

Proof: To have a single factor $T - \varphi_1$ is the content of Hensel. Then do induction on n. ///

Hensel's Lemma II: Let R be a UFD, and π a prime element in R. Given $a \in R$, suppose $b_1, c_1 \in R$ such that

$$a \ = \ b_1 \cdot c_1 \bmod \pi \qquad \textit{and} \qquad Rb_1 + Rc_1 + R\pi \ = \ R$$

Then there are b, c in the π-adic completion $R_\pi = \lim_n R/\pi^n$ such that $b = b_1 \bmod \pi$, $c = c_1 \bmod \pi$, and

$$a \ = \ b \cdot c \qquad\qquad (\text{in } \lim_n R/\pi^n = R_\pi)$$

[7.11] Remark: We'll apply this to $R = \mathbb{C}[[X-z]][T]$ or $R = \mathbb{C}[X,T]$ and $\pi = X - z$ to talk about field extensions of $\mathbb{C}((X-z))$.

Proof: With $a = b_1 \cdot c_1 \bmod \pi$, try to adjust b_1, c_1 by multiples of π to make the equation hold mod π^2: require

$$a \ = \ \big(b_1 + x\pi\big)\cdot\big(c_1 + y\pi\big) \ \bmod \pi^2$$

Simplify: the π^2 term $\pi^2 xy$ disappears, and

$$\frac{a - b_1c_1}{\pi} \ = \ xc_1 + yb_1 \ \bmod \pi$$

By hypothesis, expressions $xc_1 + yb_1 + z\pi$ with $x, y, z \in R$ give R, so there exist (non-unique!) x, y to make the equation hold.

Thus, the genuine induction step involves $a = b_nc_n \bmod \pi^n$, and trying to solve for x, y in

$$a \ = \ \big(b_n + x\pi^n\big)\cdot\big(c_n + y\pi^n\big) \ \bmod \pi^{n+1}$$

which gives

$$\frac{a - b_n c_n}{\pi^n} \;=\; x c_n + y b_n \mod \pi$$

Inductively, $c_n = c_1 \bmod \pi$ and $b_n = b_1 \bmod \pi$, so

$$R b_n + R c_n + R\pi \;=\; R c_1 + R b_1 + R\pi \;=\; R$$

and there are x, y satisfying the condition. Induction succeeds. ///

Caution: By Gauss' lemma, *polynomial* rings $\mathfrak{o}[X]$ over UFDs $\mathfrak{o}$ are UFDs, but what about $\mathfrak{o}[[X]]$?

We don't really need the more general case, since we only care about $\mathbb{C}[[X]] = \lim_n \mathbb{C}[X]/X^n$, which is completely analogous to $\mathbb{Z}_p$, where we recall that the ideals in $\mathbb{Z}_p$ are just $p^\ell \cdot \mathbb{Z}_p$. Many fewer than in $\mathbb{Z}$, and all *coming from* $\mathbb{Z}$.

Thus, $\mathbb{C}[[X]]$ is a PID, with a unique non-zero prime ideal $X \cdot \mathbb{C}[[X]]$, and *all* ideals are of the form $X^n \cdot \mathbb{C}[[X]]$.

Even though $\mathfrak{o}[[X]]$ is much bigger than $\mathfrak{o}[X]$, it has many more *units*, for example.

At the same time, UFDs like $\mathbb{Z}[x, y]$ are not PIDs, so we have to be careful what we imagine...

Maybe proving $\mathbb{Z}[[X]]$ and $\mathbb{C}[[X]][T]$ are UFDs is a good exercise.

[7.12] Corollary: (Now $z = 0$ and $X - z = X$.) Consider

$$f(X,T) = T^n + a_{n-1}(X)T^{n-1} + \ldots + a_1(X)T + a_o(X)$$

with $a_j(X) \in \mathbb{C}[[X]]$ and such that the equation

$$f(0,Y) \;=\; (Y - w_1)^{\nu_1}(Y - w_2)^{\nu_2} \ldots (Y - w_m)^{\nu_m}$$

with $w_i \neq w_j$ for $i \neq j$. Then $f(X,T)$ factors in $\mathbb{C}[[X]][T]$ into m monic-in-T factors, of degrees ν_j in T:

$$T^n + a_{n-1}(X)T^{n-1} + \ldots + a_o(X) \;=\; f_1(X,T) \ldots f_m(X,T)$$

with

$$f_j(0,T) \;=\; (T - w_j)^{\nu_j}$$

That is,

$$f_j(X,T) \;=\; (T - w_j)^{\nu_j} \mod X$$

Proof: In Hensel II, take $R = \mathbb{C}[[X]][T]$, $\pi = X$, and

$$b_1 \;=\; (T - w_1)^{\nu_1} \qquad\qquad c_1 \;=\; (T - w_2)^{\nu_2} \ldots (T - w_m)^{\nu_m}$$

An equality of polynomials $g(X) = h(X) \bmod X$ is equality of complex numbers $g(0) = h(0)$. Since w_1 is distinct from $w_2, \ldots, w_m$, there are r_1, r_2 in the PID $\mathbb{C}[T]$ such that $r_1 b_1 + r_2 c_1 = 1$, so certainly $Rb_1 + Rc_1 + R\pi = R$. By Hensel II,

$$f(X,T) \;=\; g(X,T) \,\cdot\, h(T,X) \qquad\qquad (\text{in } \mathbb{C}[[X]][T])$$

and

$$g(X,T) \;=\; (T - w_1)^{\nu_1} \mod X$$

$$h(X,T) \;=\; (T - w_2)^{\nu_2} \ldots (T - w_m)^{\nu_m} \mod X$$

Since $1 + c_1 X + \ldots \in \mathbb{C}[[X]]^\times$, we can make g, h *monic* in T. Induction on m. ///

[7.13] Corollary: Unless $f(0,w)=0$ has just a single (distinct) root in $\mathbb{C}$, $f(X,T)$ has a proper factor in $\mathbb{C}[[X]][T]$. ///

That is, over scalars $\mathbb{C}[[X]]$, the irreducible factors of $f(X,T)$ are (factors of) the groupings-by-*distinct*-factors mod X.

Now consider $w_1 = 0$, and $f(X,T) = T^n$ mod X. That is, $f(X,T)$ is of the form

$$f(X,T) \;=\; T^n \;+\; X\cdot a_{n-1}(X)\cdot T^{n-1} \;+\; \ldots \;+\; X\cdot a_o(X)$$

In the simplest case $a_o(0)\neq 0$, Eisenstein's criterion in $\mathbb{C}[[X]][T]$ gives *irreducibility* of $f(X,T)$. Let's consider this case.

Extend $\mathbb{C}[[X]]$ by adjoining $X^{1/n}$. Replacing T by $X^{1/n}\cdot T$, the polynomial becomes

$$X\cdot T^n + X^{1+\frac{n-1}{n}}a_{n-1}(X)\cdot T^{n-1} \;+\; \ldots \;+\; X^{1+\frac{1}{n}}a_1(X)\cdot T \;+\; Xa_o(X)$$

Taking out the common factor of X gives

$$T^n + (X^{1/n})^{n-1}a_{n-1}(X)\cdot T^{n-1} \;+\; \ldots \;+\; X^{1/n}a_1(X)\cdot T \;+\; a_o(X)$$

Mod $X^{1/n}$, this is

$$T^n + 0 + \ldots + 0 + a_o(0) \;=\; T^n + a_o(0) \mod X^{1/n}$$

For $a_o(0)\neq 0$, $w^n + a_o(0) = 0$ has *distinct* linear factors in $\mathbb{C}$. By the Hensel paraphrase, $f(X, X^{1/n}T)$ factors into linear factors in $\mathbb{C}[[X^{1/n}]][T]$. *We're done in this case:* the field extension is

$$\mathbb{C}((X))(Y) \;=\; \mathbb{C}((X^{1/n}))$$

[7.14] Example: To warm up to Newton polygons and the general case, consider $(T-X^{1/3})^3(T-X^{1/2})^2$. Write $\mathrm{ord}(X^{a/b}) = a/b$. The symmetric functions of roots have ords

$$\begin{array}{lcllcl}
\mathrm{ord}\,\sigma_1 &=& \mathrm{ord}(3X^{1/3}+2X^{1/2}) &&=& \frac{1}{3}\\[2ex]
\mathrm{ord}\,\sigma_2 &=& \mathrm{ord}(3X^{\frac{1}{3}+\frac{1}{3}}+6X^{\frac{1}{3}+\frac{1}{2}}+X^{\frac{1}{2}+\frac{1}{2}}) &&=& \frac{2}{3}\\[2ex]
\mathrm{ord}\,\sigma_3 &=& \mathrm{ord}(X^{3\cdot\frac{1}{3}}+6X^{2\cdot\frac{1}{3}+\frac{1}{2}}+3X^{\frac{1}{3}+2\cdot\frac{1}{2}}) &&=& 1\\[2ex]
\mathrm{ord}\,\sigma_4 &=& \mathrm{ord}(2X^{3\cdot\frac{1}{3}+\frac{1}{2}}+3X^{2\cdot\frac{1}{3}+2\cdot\frac{1}{2}}) &&=& \frac{3}{2}\\[2ex]
\mathrm{ord}\,\sigma_5 &=& \mathrm{ord}(X^{3\cdot\frac{1}{3}+2\cdot\frac{1}{2}}) &&=& 2
\end{array}$$

That is, the *increments* in $\mathrm{ord}\,\sigma_\ell$ are $\frac{1}{3},\frac{1}{3},\frac{1}{3},\frac{1}{2},\frac{1}{2}$.

Variant: Varying the example, take

$$f(X,T) \;=\; (T-z_1X^{\frac{1}{3}})(T-z_2X^{\frac{1}{3}}(T-z_3X^{\frac{1}{3}}(T-z_4X^{\frac{1}{2}})(T-z_5X^{\frac{1}{2}})$$

with non-zero $z_i\in\mathbb{C}$. Now we mostly have *inequalities* for ords:

$$\begin{array}{lcll}
\mathrm{ord}\,\sigma_1 &=& \mathrm{ord}((z_1+z_2+z_3)X^{1/3}+(z_4+z_5)X^{1/2}) & \geq \frac{1}{3}\\[2ex]
\mathrm{ord}\,\sigma_2 &=& \mathrm{ord}((z_1z_2+\ldots)X^{\frac{1}{3}+\frac{1}{3}}+(\ldots)X^{\frac{1}{3}+\frac{1}{2}}+z_4z_5X^{\frac{1}{2}+\frac{1}{2}}) & \geq \frac{2}{3}\\[2ex]
\mathrm{ord}\,\sigma_3 &=& \mathrm{ord}(z_1z_2z_3X^{3\cdot\frac{1}{3}}+(\ldots)X^{2\cdot\frac{1}{3}+\frac{1}{2}}+3X^{\frac{1}{3}+2\cdot\frac{1}{2}}) & =1\\[2ex]
\mathrm{ord}\,\sigma_4 &=& \mathrm{ord}(z_1z_2z_3(z_4+z_5)X^{3\cdot\frac{1}{3}+\frac{1}{2}}+(\ldots)X^{2\cdot\frac{1}{3}+2\cdot\frac{1}{2}}) & \geq \frac{3}{2}\\[2ex]
\mathrm{ord}\,\sigma_5 &=& \mathrm{ord}(z_1z_2z_3z_4z_5X^{3\cdot\frac{1}{3}+2\cdot\frac{1}{2}}) & =2
\end{array}$$

A stark example of the latter is

$$f(X,T) \;=\; T^5 - XT^2 + X^2$$

The crucial mechanism is that the *smallest* ord is 1/3, and replacing T by $X^{1/3}\cdot T$ will distinguish the two sizes of roots:

$$f(X, X^{1/3}\cdot T) \;=\; X^{\frac{5}{3}}T^5 - X^{\frac{5}{3}}T^2 + X^2$$

Dividing through by $X^{5/3}$ gives

$$T^5 - T^2 + X^{\frac{1}{3}}$$

Mod $X^{\frac{1}{3}}$, this has 3 *non-zero* factors, and 2 *zero* factors, so by Hensel II *factors properly* into cubic and quadratic.

More generally, consider

$$f(X,T) \;=\; (T - X^{1/e_1})^{\nu_1}\ldots(T - X^{1/e_m})^{\nu_m} \qquad (\text{with } \tfrac{1}{e_1} \le \ldots \le \tfrac{1}{e_m})$$

By the ultrametric inequality,

$$\mathrm{ord}(\sigma_\ell) \;\ge\; \mathrm{ord}\big(\text{sum of ords of the } \ell \text{ smallest-ord zeros}\big)$$

$$\ge \begin{cases} \ell\cdot\frac{1}{e_1} & \text{for } 1\le \ell\le \nu_1 \\ \frac{\nu_1}{e_1} + (\ell-\nu_1)\cdot\frac{1}{e_2} & \text{for } \nu_1 \le \ell \le \nu_1+\nu_2 \\ \frac{\nu_1}{e_1} + \frac{\nu_2}{e_2} + (\ell-\nu_1-\nu_2)\cdot\frac{1}{e_3} & \text{for } \nu_1+\nu_2 \le \ell \le \nu_1+\nu_2+\nu_3 \\ \qquad\ldots & \qquad\ldots \end{cases}$$

with *equality* at $\ell = 0, \nu_1, \nu_1+\nu_2, \ldots,\ \nu_1+\ldots+\nu_m$.

Since $\frac{1}{e_1} \le \ldots \le \frac{1}{e_m}$, the *convex hull* (downward) of the points $(\ell, \mathrm{ord}\,\sigma_\ell)$ has boundary the polygon of lines connecting the points in $\mathbb{R}^2$

$$\begin{aligned} &(0,0) \\ &(\nu_1, \tfrac{\nu_1}{e_1}) = (\nu_1, \mathrm{ord}\,\sigma_{\nu_1}) \\ &(\nu_1+\nu_2, \tfrac{\nu_1}{e_1}+\tfrac{\nu_2}{e_2}) = (\nu_1+\nu_2, \mathrm{ord}\,\sigma_{\nu_1+\nu_2}) \\ &\qquad\qquad\qquad\ldots \\ &(\nu_1+\ldots+\nu_m, \tfrac{\nu_1}{e_1}+\ldots+\tfrac{\nu_m}{e_m}) = (\nu_1+\ldots+\nu_m, \mathrm{ord}\,\sigma_{\nu_1+\ldots\nu_m}) \end{aligned}$$

This convex hull is the *Newton polygon* of the polynomial. For $f(X,T) \in \mathbb{C}[[X]][T]$, the ords are in $\mathbb{Z}$. Eisenstein's criterion is the case $\nu_1 = n$, and $\mathrm{ord}\,\sigma_n = 1$, and all the exponents are $1/n$.

The general case was reduced to $f(X,T) = T^n + \ldots + a_o(X)$ with an n-fold multiple zero w_o at $X = 0$. Replacing T by $T + w_o$, without loss of generality, this root is 0, so $a_j(0) = 0$ for all j.

Replace T by $X^\rho\cdot T$ with ρ the *slope* of the first segment from $(0,0)$ to $(\ell, \mathrm{ord}\,\sigma_\ell)$ on the Newton polygon. That is, disregard any $(\ell', \mathrm{ord}\,\sigma_{\ell'})$ with $\ell' < \ell$ lying *above* that segment.

Replacing T by $X^\rho\cdot T$ and dividing through by $X^{n\rho}$ gives

$$T^n + \ldots + \frac{a_{n-\ell}(X)}{X^{\ell\rho}}\cdot T^{n-\ell} + \ldots$$

The Newton polygon says the *ord* of the coefficient of T^j for $n \geq j > n - \ell$ is *non-negative*, at $T^{n-\ell}$ the ord is 0, and for $n - \ell > j$ it is *strictly positive.*

That is, mod X,

$$f(0,T) \;=\; T^n + \ldots + \underbrace{b_{n-\ell}(0)}_{\text{non}-\text{zero}} \cdot T^{n-\ell}$$

Thus, $f(0,w) = 0$ has ℓ non-zero complex roots, and $n - \ell$ roots 0.

Hensel II says that there are degree ℓ factor and degree $n - \ell$ factors in $\mathbb{C}[[X^\rho]][T]$.

Note that $\mathbb{C}[[X^\rho]] \approx \mathbb{C}[[X]]$, so the argument can be repeated. Induction on degree. ///

[7.15] Theorem: All finite field extensions of $\mathbb{C}((X-z))$ are by adjoining solutions to $Y^e = X - z$ for $e = 2, 3, 4, \ldots$. [Done]

Few examples of explicit parametrization of an *algebraic closure* of a field are known: *not* $\overline{\mathbb{Q}}$, for sure.

Finite fields, yes: the *cyclic-ness* of $\mathbb{F}_q^\times$ and the *uniqueness* of the extension $\mathbb{F}_{q^d}$ of a given degree d say that the degree-d extension is the collection of roots of $x^{q^d - 1} = 1$.

The Galois group of $\mathbb{F}_{q^d}/\mathbb{F}_q$ is *cyclic* of order d, generated by the *Frobenius* element $\alpha \to \alpha^q$. Thus, there is the decisive

$$\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \;=\; \lim_{d} \mathbb{Z}/d \;=\; \widehat{\mathbb{Z}} \;\approx\; \prod_p \mathbb{Z}_p$$

Remarks What *about* $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$? In Wiles' and Wiles-Taylor' mid-1990s proof of Fermat's Last Theorem, they proved part of the Taniyama-Shimura (1950s) conjecture: certain *two-dimensional representations* of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ attached to elliptic curves defined over $\mathbb{Q}$ are *parametrized* by *holomorphic modular forms...* (!?!)

A *representation* ρ of a group G is simply a group homomorphism

$$\rho \;:\; G \;\longrightarrow\; GL_n(k) \;=\; \{k-\text{linear autos of } k^n\}$$

Quadratic reciprocity is the simplest analogue of the Taniyama-Shimura conjecture: a Galois-related thing (quadratic symbol) is a harmonic-analysis thing (Dirichlet character). Those are representations on GL_1, with ±1 construed as trivial-or-not:

$$p \;\longrightarrow\; \left(\frac{\sqrt{D}}{p}\right)_2 \;\in\; \text{Gal}(\mathbb{Q}(\sqrt{D})/\mathbb{Q}) \;\approx\; \frac{\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}{\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\sqrt{D}))}$$

The proof that this has a *conductor* $N = 4D$, that is, depends only on $p \bmod 4D$, is the proof that the Galois-object is analytic.

About 1980, Y. Hellegouarch and G. Frey observed that a non-trivial rational solution of Fermat's equation gives a non-singular cubic curve defined over $\mathbb{Q}$:

$$a^n + b^n = c^n \quad\longrightarrow\quad y^2 = x(x - a^n)(x + b^n) \qquad\qquad (\text{with } abc \neq 0)$$

1985-6, Frey suggested, and Serre partly proved, that Taniyama-Shimura would imply Fermat. 1986/90 K. Ribet proved this implication.

(Slightly more specifically: the *conductor* N of the elliptic curve is the product of distinct primes dividing abc. If the elliptic curve is known to be *modular*, there is a *descent* argument reducing the conductor/level (!?!), removing all odd primes from the conductor. But the modular curve $\Gamma_0(2)\backslash\mathfrak{H}$ has genus 0, that is, has no maps to an elliptic curve. Contradiction.)

In fact, Wiles-Taylor only need a *part* of T-S-W, and that was completed 1995.

The complete T-S-W theorem was proven by Diamond, B. Conrad, Diamond-Taylor, and Breuil.

A tangent: **Why representations?** Sometimes a group G and its smallest (=irreducible) representations, *are* well-understood, shedding light on *large* representations arising in practice, by breaking them into atomic pieces.

[7.16] Example: the *circle* $G = S^1 = \mathbb{R}/\mathbb{Z}$ has one-dimensional representations $x \to e^{2\pi i n x}$ indexed by integers n. *Fourier series* express *functions* on the circle as sums of exponential functions.

Similarly, $G = \mathbb{R}$ has one-dimensional representations $x \to e^{2\pi i n x}$ indexed by integers n. *Fourier inversion* expresses *functions* on the line as integrals of exponential functions.

Fourier expansions facilitate analysis on $[a, b]$ or $\mathbb{R}$, because d/dx *commutes* with the group action (by *translation*), so (!!) acts by a scalar on each irreducible. (This is *Schur's lemma*.)

That is, writing a Fourier expansion *diagonalizes* the linear operator d/dx.

For example, constant-coefficient *differential* equations are converted to *algebraic* equations.

[7.17] Example: Unitary groups $G = U(n) = \{g \in GL_n(\mathbb{C}) : g^*g = 1_n\}$ have irreducibles parametrized simply by sequences of integers

$m_1 \geq m_2 \geq \ldots m_n$ (theory of *highest weights*). For example, $G = U(2)$ acts by *rotations* on the 3-sphere S^3. Various collections of (nice...) functions on S^3 thereby are *representation spaces* of G, and express functions as sums of functions belonging to irreducible subrepresentations.

The *Casimir* element (of the universal enveloping algebra of the Lie algebra of G!?!) *commutes* with the group action, so (Schur's lemma!) acts by a scalar on irreducibles. The Casimir element is manifest (!?!) as a rotation-invariant *Laplacian* Δ on S^3.

The important differential equation $(\Delta - \lambda)u = f$ *on the sphere* is solved by this decomposition into irreducible representations.

Decomposition of function spaces on the two-sphere S^2 was understood by Laplace pre-1800 for purposes of celestial mechanics. The corresponding representation-theoretic decompositions are *Fourier-Laplace* expansions.

[7.18] Example: $SL_2(\mathbb{R})$ has irreducible *unitary* representations on *Hilbert spaces*, nicely parametrized by $k = \pm 2, \pm 3, \pm 4, \pm 5, \ldots$, by the interval $(\frac{1}{2}, 1]$, and by *the critical line* $\frac{1}{2} + i\mathbb{R}$.

The *discretely* parametrized repns $\pm 2, \pm 3, \ldots$ correspond (!?!) to representations generated by *holomorphic modular forms*, for example, entering the Taniyama-Shimura-Weil conjecture.

The *continuously* parametrized representations correspond (!?!) to eigenfunctions of an invariant Laplacian on the upper half-plane $\mathfrak{H}$, studied by Maaß(1949), Selberg, Roelcke, Avakumovic (all 1956 *et seq*), and many others since.

In both cases, the Casimir element (in the center of the enveloping algebra) acts as a scalar (Schur's lemma!), the scalar depending only on the representation class.

That is, the representation theory *diagonalizes* Laplacian/Casimir. Oppositely, sometimes a group G itself is mysterious, but events produce a stock of *representations of it*, from which we make inferences.

For example, *algebraic* aspects of representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on *cohomology of algebraic varieties* (!?!) defined over $\mathbb{Q}$ are better understood than $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ itself.

The Taniyama-Shimura-Weil conjecture was difficult: neither the group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *nor* the *analytical* aspects of its more-than-one-dimensional representations were understood.

Note: parametrization in terms of *modular forms* is *not elementary.*

The Langlands program is an umbrella-name covering such things, and many more...

8. *Extensions of local fields*

This is the assertion for $\mathbb{Z}_p[T]$ corresponding to $\mathbb{C}[[X]][T]$ above: $\mathbb{C}[[X]]$ is replaced by $\mathbb{Z}_p$.

The *Newton polygon* of a polynomial $f(T) = T^n + a_{n-1}T^{n-1} + \ldots + a_o \in \mathbb{Z}_p[T]$ is the (downward) convex hull of the points

$$(0,0),\ (1, \operatorname{ord}_p a_{n-1}),\ (2, \operatorname{ord}_p a_{n-2}),\ \ldots\ (n, \operatorname{ord}_p a_o)$$

If we believe that $\operatorname{ord}_p(p^n \cdot \frac{a}{b}) = n$ extends to algebraic *extensions* of $\mathbb{Q}_p$, then we would anticipate proving that the *slopes* of the line segments on the Newton polygon are the *ords*, with multiplicities, of the zeros.

The extreme case that $\operatorname{ord}_p a_0 = 1$ would be *Eisenstein's criterion.*

We will get to this... **That point at infinity** The *local ring* (having a single maximal ideal) inside the field $\mathbb{C}(X)$ corresponding to $z \in \mathbb{C}$, consisting of all rational functions *defined* at z, is

$$\mathfrak{o}_z = \mathbb{C}(X) \cap \mathbb{C}[[X - z]]$$

with unique maximal ideal

$$\mathfrak{m}_z = \mathbb{C}(X) \cap (X - z) \cdot \mathbb{C}[[X - z]]$$

The *point at infinity* can be discovered by noting a further local ring and maximal ideal:

$$\mathfrak{o}_\infty = \mathbb{C}(X) \cap \mathbb{C}[[1/X]] \qquad \mathfrak{m}_\infty = \mathbb{C}(X) \cap \frac{1}{X}\mathbb{C}[[1/X]]$$

Note that using $1/(X+1)$ achieves the same effect, because

$$\frac{1}{X+1} = \frac{1}{X} \cdot \frac{1}{1+\frac{1}{X}} = \frac{1}{X} \cdot \Big(1 - \frac{1}{X} + (\frac{1}{X})^2 - \ldots\Big) \in \frac{1}{X} \cdot \mathbb{C}[[1/X]]^\times$$

On Riemann surface M of extension K of $k = \mathbb{C}(X)$... *Points at infinity* on M correspond to local rings in K intersecting k in the local ring $\mathbb{C}[[1/X]]$.

For example, on hyperelliptic curves $Y^2 = f(X)$, with $f(X)$ a monic polynomial, there are either *one* or *two* points at infinity, depending whether $\deg f$ is *odd*, or *even*:

For $n = 2m$, rewrite $Y^2 = X^n + \ldots + a_o$ as

$$Y^2/X^n = 1 + \ldots + a_p(1/X)^n$$

replace Y by $Y \cdot X^m$, and relabel $1/X = Z$, obtaining

$$Y^2 = 1 + \ldots + a_p Z^n \qquad (n \text{ even})$$

which has 2 solutions $Y = \pm 1 + (\text{h.o.t.})$ near $Z = 0$. For $n = 2m + 1$, similarly,

$$Y^2 = Z \cdot (1 + \ldots)$$

so there is a single, ramified, point-at-infinity, $Y = \sqrt{Z} + (\text{h.o.t.})$.

[8.1] Examples: *(cont'd) Function fields* in one variable... as algebraic parallels to $\mathbb{Z}$ and $\mathbb{Q}$.

[8.2] Theorem: All finite field extensions of $\mathbb{C}((X-z))$ are by adjoining solutions to $Y^e = X - z$ for $e = 2, 3, 4, \ldots$. [Done]

Thus,

$$\mathrm{Gal}\big(\,\overline{\mathbb{C}((X))}/\mathbb{C}((X))\,\big) \;=\; \lim_{d} \mathbb{Z}/d \;=\; \widehat{\mathbb{Z}} \;\approx\; \prod_p \mathbb{Z}_p$$

Few explicit parametrizations of *algebraic closures* of fields are known: *not* $\overline{\mathbb{Q}}$, for sure. But we *do* also know

$$\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \;=\; \lim_{d} \mathbb{Z}/d \;=\; \widehat{\mathbb{Z}} \;\approx\; \prod_p \mathbb{Z}_p$$

Returning to *finite* scalars in place of $\mathbb{C}$... a key point is the finiteness of residue fields $\mathfrak{o}/\mathfrak{p}$.

Infinitude of primes: Because the algebraic closure of $\mathbb{F}_q$ is of infinite degree over $\mathbb{F}_q$, by *separability* there are single elements α of arbitrarily large degree, whose minimal polynomials in $\mathbb{F}_q[X]$ give prime elements of arbitrarily large degree, thus, *infinitely-many.*

Also, we can mimic Euclid's proof. Use the fact that $\mathbb{F}_q[X]$ is a PID. Given any finite collection $P_1, \ldots, P_n$ of monic irreducibles in $\mathbb{F}_q[X]$, the element $N = X \cdot P_1 \ldots P_n + 1$ is of positive degree, so has *some* irreducible factor, but is not divisible by any P_j. ///

One should contemplate what it would take to prove an analogue of *Dirichlet's Theorem* on primes in arithmetic progressions.

The finiteness of residue fields allows definition of the *zeta function* of $\mathfrak{o} = \mathbb{F}_q[X]$:

$$Z(s) \;=\; \sum_{0 \neq \mathfrak{a} \text{ ideal} \subset \mathbb{F}_p[X]} \frac{1}{(N\mathfrak{a})^s} \;=\; \sum_{0 \neq \mathfrak{a} \text{ ideal} \subset \mathbb{F}_p[X]} \frac{1}{(\#\mathbb{F}_p[X]/\mathfrak{a})^s} \;=\; \sum_{\text{monic } f} \frac{1}{(\#\mathbb{F}_p[X]/\langle f \rangle)^s}$$

$$= \sum_{\text{monic } f} \frac{1}{(q^{\deg f})^s} \;=\; \sum_{\text{degrees } d} \frac{\#\{\text{monic } f : \deg f = d\}}{q^{ds}} \;=\; \sum_{\text{degrees } d} \frac{q^d}{q^{ds}} \;=\; \frac{1}{1 \,-\, \dfrac{1}{q^{s-1}}}$$

Since $\mathbb{F}_q[X]$ is a PID, there is an *Euler product*

$$Z(s) \;=\; \prod_{0 \neq \mathfrak{p} \text{ prime}} \frac{1}{1 \,-\, (N\mathfrak{p})^{-s}} \;=\; \prod_{\text{monic irred } f} \frac{1}{1 \,-\, q^{-s \cdot \deg f}} \;=\; \prod_d \Big(\frac{1}{1 \,-\, q^{-sd}}\Big)^{\#\text{monic irred } f \;\; \deg = d}$$

convergent for $\Re(s) > 1$. Observe that

$$\#\text{irred monics deg } d \;=\; \frac{\#\text{ elements degree } d \text{ over } \mathbb{F}_q}{\#\text{each Galois conjugacy class}}$$

$$= \frac{1}{d}\Big(q^d - \sum_{\text{prime } p | d} q^{d/p} + \sum_{\text{distinct } p_1, p_2 | d} q^{d/p_1 p_2} - \sum_{\text{distinct } p_1, p_2, p_3 | d} q^{d/p_1 p_2 p_3} + \ldots\Big)$$

The fact that $Z(s) = 1/(1 - q^{1-s})$ is not obvious from the Euler factorization.

Example: in $\mathbb{F}_3[x]$, monic irreducibles of low degrees are

$x,\ x+1,\ x+2$	(3 (irred) monic linear)
$x^2+1,\ \ x^2+2x+2,$ x^2-2x+2	($\frac{3^2-3}{2}=3$ irred monic quadratics)
$x^3-x+1,\ \ x^3-x+2,\ \ldots$ (all x^3-a's are *reducible*!?!)	($\frac{3^3-3}{3}=8$ irred monic cubics)
$x^4-2x+1,\ \ldots$ (all x^4-a's are *reducible*!?!)	($\frac{3^4-3^2}{4}=18$ irred monic quartics)
??? (all x^5-a's are *reducible*!?!)	($\frac{3^5-3}{5}=48$ irred monic quintics)

No simple conceptual argument, but some reusable tricks... :

Since $\mathbb{F}_3^\times$ is a cyclic 2-group, there is no 4^{th} root of unity, so the 4^{th} cyclotomic polynomial x^2+1 is irreducible.

Then $(x+j)^2+1$ is irreducible for $j=1,2$. This *happens* to give all 3 irreducible monic quadratics.

Since $x^3-a=(x-a)^3$ for $a\in\mathbb{F}_3$, none of these cubics is irreducible.

The two cubics x^3-x+a with $a\neq 0$ are *Artin-Schreier* polynomials over $\mathbb{F}_3$. Since $\alpha^3-\alpha=0$ for $\alpha\in\mathbb{F}_3$, these have no linear factors, so are irreducible. With $j\in\mathbb{F}_3$, $x\to x+j$ leaves these unchanged!

No quartic $x^4-a\in\mathbb{F}_3[x]$ is irreducible: $\mathbb{F}_{3^4}^\times$ is cyclic of order $3^4-1=80=2^4\cdot 5$, so every $a\in\mathbb{F}_3^\times$ is an 8^{th} power.

Since $(3^2-1)/4=2$, fourth powers of $\alpha\in\mathbb{F}_{3^2}^\times$ have order 2, so are in $\mathbb{F}_3^\times$. Thus, $\alpha^4\neq a\alpha+b$ for non-zero $a,b\in\mathbb{F}_3$. Thus, the four polynomials x^4-ax-b with non-zero $a,b\in\mathbb{F}_3$ are irreducible.

Artin-Schreier polynomials: Taking p^{th} roots is problematical in characteristic p... Already the *quadratic formula* fails in characteristic 2. A root of $x^2+x+1=0$ in $\mathbb{F}_{2^2}$ *cannot* be expressed in terms of square roots!

Over $\mathbb{F}_p$ with prime p, the *Artin-Schreier* polynomials are x^p-x+a, with $a\in\mathbb{F}_p^\times$.

[8.3] Claim: Artin-Schreier polynomials are *irreducible*, with Galois group cyclic of order p.

Proof: For a root $\alpha\in\overline{\mathbb{F}}_p$ of $x^p-x+a=0$,

$$(\alpha+1)^p-(\alpha+1)+a\ =\ \alpha^p-\alpha+a\ =\ 0$$

Thus, any field extension containing *one* root contains *all* roots. That is, the splitting field is $\mathbb{F}_p(\alpha)$ for any root α. But the Frobenius automorphism $\alpha\to\alpha^p$ generates the Galois group, whatever it is, and $\alpha^p=\alpha-a$, which is of order p. Thus, the Galois group is cyclic of order p. ///

For $\mathfrak{o}=\mathbb{F}_p[x]$, *completions* are

$$\begin{aligned} x\text{-adic completion of } \mathfrak{o} &= \mathbb{F}_p[[x]] \\ (x+1)\text{-adic completion of } \mathfrak{o} &= \mathbb{F}_p[[x+1]] \\ (x^2+1)\text{-adic completion of } \mathfrak{o} &= \mathbb{F}_p[[x^2+1]][x] \end{aligned}$$

$$=\ \{(a_ox+b_o)+(x^2+1)(a_1x+b_1)+(x^2+1)^2(a_2x+b_2)+\ldots\}$$

Generally, for P irreducible monic

$$\begin{aligned}&P\text{-adic completion of } \mathfrak{o}\\ &\quad = \; c_o(x) + c_1(x)\cdot P + c_2(x)\cdot P^2 + \ldots \qquad\qquad (\deg c_j < \deg P)\end{aligned}$$

Also, corresponding to the *point at infinity* and its local ring $\mathbb{F}_p[[1/x]] \cap \mathbb{F}_p(x)$ inside $\mathbb{F}_p(x)$,

$$\frac{1}{x} - \text{adic completion of } \mathfrak{o} \;=\; \mathbb{F}_p[[1/x]]$$

Let k be a *global field*, that is, either a *number field* (=finite extension of $\mathbb{Q}$) or *function field* (=finite separable extension of $\mathbb{F}_q(X)$), with integers $\mathfrak{o}$.

Let v index the *completions* k_v of k. Let K be a *quadratic* extension of k, and put

$$K_v \;=\; K \otimes_k k_v$$

K_v is two copies of k_v when the prime indexed by v *splits* or *ramifies*, and is a quadratic field extension of k_v otherwise:

$$K \otimes_k k_v \;\approx\; k[x]/\langle f\rangle \otimes_k k_v \;\approx\; k_v[x]/\langle f\rangle \;\approx\; \begin{cases} k_v \times k_v \quad (\text{when } f \text{ has a zero in } k_v) \\ \text{a quadratic extension (when } f \text{ has no zero in } k_v) \end{cases}$$

The Galois norm $N : K \to k$ certainly gives $N : K^\times \to k^\times$, and by *extension of scalars* $N : K_v^\times \to k_v^\times$.

Define the **local norm residue symbol** $\nu_v : k_v^\times \to \{\pm 1\}$ by

$$\nu_v(\alpha) \;=\; \begin{cases} +1 & (\text{for } \alpha \in N(K_v^\times)) \\ -1 & (\text{for } \alpha \notin N(K_v^\times)) \end{cases}$$

[8.4] Example: of the three quadratic extensions of $\mathbb{Q}_p$ with p odd, the extension $\mathbb{Q}_p(\sqrt{\eta})$, obtained by adjoining a square root of a non-square *local unit* $\eta \in \mathbb{Z}_p^\times$, has the property that *norm is a surjection on local units:*

$$N(\mathbb{Z}_p[\sqrt{\eta}]^\times) \;=\; \mathbb{Z}_p^\times$$

Proof: Let D be an integer so that D is a non-square mod p, and $E = \mathbb{Q}_p(\sqrt{D})$. First, show that norm is a surjection $\mathbb{F}_{p^2}^\times \to \mathbb{F}_p^\times$. Indeed,

$$N(x) \;=\; x \cdot x^p \;=\; x^{1+p} \qquad\qquad (\text{for } \mathbb{F}_{p^2}^\times \to \mathbb{F}_p^\times)$$

The multiplicative group $\mathbb{F}_{p^2}^\times$ is cyclic of order p^2-1, so taking $(p+1)^{th}$ powers surjects to the *unique* cyclic subgroup of order $p-1$, which must be $\mathbb{F}_p^\times$.

Given $\alpha \in \mathbb{Z}_p^\times$, take $a \in \mathbb{Z}$ such that $a = \alpha \bmod p\mathbb{Z}_p$, so $a^{-1}\alpha = 1 \bmod p\mathbb{Z}_p$. Norms are surjective mod p, so there is $\beta \in \mathbb{Z}_p[\sqrt{D}]$ such that $N\beta = a + p\mathbb{Z}_p$, and $N\beta^{-1}\cdot\alpha \in 1 + p\mathbb{Z}_p$.

The p-adic exp and log show that for odd p the subgroup $1 + p\mathbb{Z}_p$ of $\mathbb{Z}_p^\times$ consists entirely of *squares*. Thus, there is $\gamma \in \mathbb{Z}_p^\times$ such that $\gamma^2 = N\beta^{-1}\cdot\alpha$, and then $\alpha = N(\beta\gamma)$. ///

A small *local* Theorem:

$$[k_v^\times : N(K_v^\times)] \;=\; \begin{cases} 2 & (\text{when } K_v \text{ is a field}) \\ 1 & (\text{when } K_v \approx k_v \times k_v) \end{cases}$$

About the proof: when K_v is $k_v \times k_v$, the extended local norm is just *multiplication* of the two components, so is certainly surjective. The interesting case is when K_v is a (separable) quadratic extension of k_v.

We call the assertion *local* because it only refers to *completions*, which, in fact, is much easier.

Let's postpone proof of this auxiliary result, but note a corollary, similar to *Euler's criterion* for things being squares:

[8.5] Corollary: ν_v is a group homomorphism $k_v^\times \to \{\pm 1\}$. ///

An immediate, if opaque, definition of *ideles*:

$$\mathbb{J} \;=\; \mathbb{J}_k \;=\; (\text{ideles of } k) \;=\; \{\{\alpha_v\} \in \prod_v k_v^\times \;:\; \alpha_v \in \mathfrak{o}_v^\times \text{ for all but finitely-many } v\}$$

Let

$$\nu = \prod_v \nu_v \;:\; \mathbb{J} \longrightarrow \{\pm 1\}$$

A big *global* Theorem: ν is a $k^\times$-invariant function on $\mathbb{J}$. That is, it *factors through* $\mathbb{J}/k^\times$. Other nomenclature: ν is a *Hecke character*, and/or a *grossencharakter*.

Granting this perhaps-unexciting-sounding feature, we can make some interesting deductions: ...

Quadratic Hilbert symbols For $a, b \in k_v$ the (quadratic) **Hilbert symbol** is

$$(a,b)_v \;=\; \begin{cases} 1 & (\text{if } ax^2 + by^2 = z^2 \text{ has non-trivial solution in } k_v) \\ -1 & (\text{otherwise}) \end{cases}$$

Memorable theorem: For $a, b \in k^\times$

$$\Pi_v\; (a,b)_v \;=\; 1$$

Proof: We prove this from the fact that the quadratic norm residue symbol is a Hecke character. When b (or a) is a square in $k^\times$, the equation

$$ax^2 + by^2 \;=\; z^2$$

has a solution over k. There is a solution over k_v for all v, so all the Hilbert symbols are 1, and reciprocity holds in this case. For b *not* a square in $k^\times$, rewrite the equation

$$ax^2 \;=\; z^2 - by^2 \;=\; N(z + y\sqrt{b})$$

and $K = k(\sqrt{b})$ is a quadratic field extension of k. At a prime v of k *split* (or ramified) in K, the local extension $K \otimes_k k_v$ is not a field, and the norm is a surjection, so $\nu_v \equiv 1$ in that case. At a prime v of k *not* split in K, the local extension $K \otimes_k k_v$ *is* a field, so

$$ax^2 \;=\; z^2 - by^2$$

can have no (non-trivial) solution x, y, z even in k_v unless $x \neq 0$. In that case, divide by x and find that a is a norm if and only if this equation has a solution.

That is, $(a,b)_v$ is $\nu_v(a)$ for the field extension $k(\sqrt{b})$, and the reciprocity law for the norm residue symbol gives the result for the Hilbert symbol. ///

Now obtain the most traditional quadratic reciprocity law from the reciprocity law for the quadratic Hilbert symbol. Define the quadratic symbol

$$\left(\frac{x}{v}\right)_2 \;=\; \begin{cases} 1 & \text{(for } x \text{ a non-zero square mod } v\text{)} \\ 0 & \text{(for } x = 0 \text{ mod } v\text{)} \\ -1 & \text{(for } x \text{ a non-square mod } v\text{)} \end{cases}$$

Quadratic Reciprocity ('main part'): For π and ϖ two elements of $\mathfrak{o}$ generating distinct odd prime ideals,

$$\left(\frac{\varpi}{\pi}\right)_2 \left(\frac{\pi}{\varpi}\right)_2 \;=\; \Pi_v\,(\pi,\varpi)_v$$

where v runs over all *even or infinite* primes, and $(,)_v$ is the (quadratic) Hilbert symbol.

Proof: (of main part) We claim that, since $\pi\mathfrak{o}$ and $\varpi\mathfrak{o}$ are odd primes,

$$(\pi,\varpi)_v \;=\; \begin{cases} \left(\frac{\varpi}{\pi}\right)_2 & \text{for } v = \pi\mathfrak{o} \\ \left(\frac{\pi}{\varpi}\right)_2 & \text{for } v = \varpi\mathfrak{o} \\ 1 & \text{for } v \text{ odd and } v \neq \pi\mathfrak{o}, \varpi\mathfrak{o} \end{cases}$$

Let $v = \pi\mathfrak{o}$. Suppose that there is a solution x, y, z in k_v to

$$\pi x^2 + \varpi y^2 \;=\; z^2$$

Via the ultrametric property, $\mathrm{ord}_v y$ and $\mathrm{ord}_v z$ are identical, and less than $\mathrm{ord}_v x$, since ϖ is a v-unit and $\mathrm{ord}_v \pi x^2$ is *odd.* Multiply through by π^{2n} so that $\pi^n y$ and $\pi^n z$ are v-units. Then that ϖ must be a square modulo v.

On the other hand, when ϖ is a square modulo v, use Hensel's lemma to infer that ϖ is a square in k_v. Then

$$\varpi y^2 \;=\; z^2$$

certainly has a non-trivial solution.

For v an odd prime distinct from $\pi\mathfrak{o}$ and $\varpi\mathfrak{o}$, π and ϖ are v-units. When ϖ is a square in k_v, $\varpi = z^2$ has a solution, so the Hilbert symbol is 1. For ϖ not a square in k_v, $k_v(\sqrt{\varpi})$ is an *unramified* field extension of k_v, since v is odd. Thus, the norm map is surjective to units in k_v. Thus, there are $y, z \in k_v$ so that

$$\pi \;=\; N(z + y\sqrt{\varpi}) \;=\; z^2 - \varpi y^2$$

Thus, all but even-prime and infinite-prime quadratic Hilbert symbols are quadratic symbols. ///

Simplest examples Let's recover quadratic reciprocity for two (positive) odd prime numbers p, q:

$$\left(\frac{q}{p}\right)_2 \left(\frac{p}{q}\right)_2 \;=\; (-1)^{(p-1)(q-1)/4}$$

We have

$$\left(\frac{q}{p}\right)_2 \left(\frac{p}{q}\right)_2 \;=\; (p,q)_2 (p,q)_\infty$$

Since both p, q are positive, the equation

$$px^2 + qy^2 \;=\; z^2$$

has non-trivial *real* solutions x, y, z. That is, the 'real' Hilbert symbol $(p, q)_\infty$ for the archimedean completion of $\mathbb{Q}$ has the value 1. Therefore, only the 2-adic Hilbert symbol contributes to the right-hand side of Gauss' formula:

$$\left(\frac{q}{p}\right)_2 \left(\frac{p}{q}\right)_2 = (p, q)_2$$

Hensel's lemma shows that the solvability of the equation above (for p, q both 2-adic units) depends only upon their residue classes mod 8. The usual formula is but one way of interpolating the 2-adic Hilbert symbol by elementary-looking formulas. ///

For contrast, let us derive the analogue for $\mathbb{F}_q[T]$ with q odd: for distinct *monic* irreducible polynomials π, ϖ in $\mathbb{F}_q[T]$,

$$\left(\frac{\varpi}{\pi}\right)_2 \left(\frac{\pi}{\varpi}\right)_2 = \left(\frac{-1}{\mathbb{F}_q}\right)_2^{(\deg \pi)(\deg \varpi)}$$

Proof: From the general assertion above,

$$\left(\frac{\varpi}{\pi}\right)_2 \left(\frac{\pi}{\varpi}\right)_2 = (\pi, \varpi)_\infty$$

where ∞ is the prime (valuation)

$$P \longrightarrow q^{\deg P}$$

This norm has local ring consisting of rational functions in t writable as power series in the local parameter $t_\infty = t^{-1}$. Then

$$\pi = t_\infty^{-\deg \pi}(1 + t_\infty(\ldots))$$

where $(1 + t_\infty(\ldots))$ is a power series in t_∞. A similar assertion holds for ϖ. Thus, if either degree is *even*, then one of π, ϖ is a local square, so the Hilbert symbol is $+1$.

When $t_\infty^{-\deg \pi}(1 + t_\infty(\ldots))$ is a non-square, $\deg \pi$ is odd. Nevertheless, *any* expression of the form

$$1 + t_\infty(\ldots)$$

is a local square (by Hensel). Thus, without loss of generality, we are contemplating the equation

$$t_\infty(x^2 + y^2) = z^2$$

The t_∞-order of the right-hand side is even.

If there is no $\sqrt{-1}$ in $\mathbb{F}_q$, then the left-hand side is t_∞-times a norm from the unramified extension

$$\mathbb{F}_q(\sqrt{-1})(T) = \mathbb{F}_q(T)(\sqrt{-1})$$

so has odd order. This is impossible. On the other hand if there is a $\sqrt{-1}$ in $\mathbb{F}_q$ then the equation has non-trivial solutions.

Thus, if neither π nor ϖ is a local square (i.e., both are of odd degree), then the Hilbert symbol is 1 if and only if there is a $\sqrt{-1}$ in $\mathbb{F}_q$. The formula given above is an elementary interpolation of this assertion (as for the case $k = \mathbb{Q}$). ///

9. *Primes lying over/under*

[9.1] Theorem: For $\mathfrak{O}$ *integral* over $\mathfrak{o}$ and prime ideal $\mathfrak{p}$ of $\mathfrak{o}$, there is at least one prime ideal $\mathfrak{P}$ of $\mathfrak{O}$ such that $\mathfrak{P} \cap \mathfrak{o} = \mathfrak{p}$. That is, $\mathfrak{P}$ *lies over* $\mathfrak{p}$. $\mathfrak{P}$ is maximal if and only if $\mathfrak{p}$ is maximal. Further, $\mathfrak{p} \cdot \mathfrak{O} \neq \mathfrak{O}$, keeping in mind that

$$\mathfrak{p} \cdot \mathfrak{O} \;=\; \{\sum_j p_j \cdot y_j \;:\; p_j \in \mathfrak{p},\; y_j \in \mathfrak{O}\}$$

There a natural commutative diagram

$$\begin{tikzcd} \mathfrak{O} \arrow[r] & \mathfrak{O}/\mathfrak{P} \\ \mathfrak{o} \arrow[u, "\text{inj}"] \arrow[r] & \mathfrak{o}/\mathfrak{p} \arrow[u, "\text{inj}"'] \end{tikzcd}$$

We do not necessarily assume $\mathfrak{o}$ or $\mathfrak{O}$ is a domain.

Proof: This is reducible to *local* questions. The set $S = \mathfrak{o} - \mathfrak{p}$ is *multiplicative* because $\mathfrak{p}$ is prime. It is easy that $S^{-1}\mathfrak{O}$ is integral over $S^{-1}\mathfrak{o}$, and that $S^{-1}\mathfrak{o}$ has the unique maximal ideal $\mathfrak{m} = \mathfrak{p} \cdot S^{-1}\mathfrak{o}$.

To show $\mathfrak{p}\mathfrak{O} \neq \mathfrak{O}$, it suffices to consider the local version, and show $\mathfrak{m} \cdot S^{-1}\mathfrak{O} \neq S^{-1}\mathfrak{O}$, because

$$\mathfrak{p} \cdot S^{-1}\mathfrak{O} \;=\; \mathfrak{p} \cdot S^{-1}\mathfrak{o} \cdot S^{-1}\mathfrak{O} \;=\; \mathfrak{m} \cdot S^{-1}\mathfrak{O}$$

That is, it suffices to prove $\mathfrak{m} \cdot \mathfrak{O} \neq \mathfrak{O}$, with $\mathfrak{o}$ *local*.

For local $\mathfrak{o}$, if $\mathfrak{m} \cdot \mathfrak{O} = \mathfrak{O}$, then $1 \in \mathfrak{O}$ has an expression $1 = m_1 y_1 + \ldots + m_n y_n$, with $m_j \in \mathfrak{m}$ and $y_j \in \mathfrak{O}$. Let $\mathfrak{O}_1$ be the ring $\mathfrak{O}_1 = \mathfrak{o}[y_1, \ldots, y_n]$. It is a finitely-generated $\mathfrak{o}$-*algebra*, so by integrality is a finitely-generated $\mathfrak{o}$-*module*.

Nakayama's Lemma says that if $\mathfrak{a}M = M$ for an ideal contained in all maximal ideals of $\mathfrak{o}$, and M a finitely-generated $\mathfrak{o}$-module, then $M = \{0\}$.

Proof: (of Lemma) For M generated by $m_1, \ldots, m_n$, the hypothesis gives

$$m_1 \;=\; a_1 m_1 + \ldots + a_n m_n \qquad\qquad (\text{for some } a_j \in \mathfrak{a})$$

$$(1 - a_1) m_1 \;=\; a_2 m_2 + \ldots + a_n m_n$$

Either $1 - a_1$ is a unit, or it is contained in some maximal ideal. But $\mathfrak{a}$ is contained in *all* maximal ideals, so $1 - a_1$ is a unit. Thus, m_1 is expressible in terms of the other generators. Induction. ///

Applying this to $\mathfrak{O}_1$ gives $\mathfrak{O}_1 = \{0\}$, contradiction. Thus, $\mathfrak{m} \cdot \mathfrak{O} \neq \mathfrak{O}$.

Reverting to not-necessarily-local $\mathfrak{o}$, in

$$\begin{tikzcd} \mathfrak{O} \arrow[r] & S^{-1}\mathfrak{O} \\ \mathfrak{o} \arrow[u] \arrow[r] & S^{-1}\mathfrak{o} \arrow[u] \end{tikzcd}$$

$\mathfrak{m} \cdot S^{-1}\mathfrak{O} \neq S^{-1}\mathfrak{O}$, so is in some maximal ideal $\mathfrak{M}$ of $S^{-1}\mathfrak{O}$, and $\mathfrak{M} \cap S^{-1}\mathfrak{o} \supset \mathfrak{m}$. By maximality of $\mathfrak{m}$, $\mathfrak{M} \cap S^{-1}\mathfrak{o} = \mathfrak{m}$.

$\mathfrak{M}$ is non-zero prime, so $\mathfrak{P} = \mathfrak{M} \cap \mathfrak{O}$ is prime, because intersecting a prime ideal with a subring gives a prime ideal. $\mathfrak{P}$ is not $\{0\}$, because of integrality: $0 \neq m \in \mathfrak{M}$ satisfies $m^n + a_{n-1}m^{n-1} + \ldots + a_o = 0$ with $a_i \in \mathfrak{o}$ and $0 \neq a_o \in \mathfrak{o} \cap \mathfrak{M}$. Then

$$\mathfrak{o} \cap \mathfrak{P} \;=\; \mathfrak{o} \cap (\mathfrak{O} \cap \mathfrak{M}) \;=\; \mathfrak{o} \cap \mathfrak{M} \;=\; \mathfrak{o} \cap (S^{-1}\mathfrak{o} \cap \mathfrak{M}) \;=\; \mathfrak{o} \cap \mathfrak{m} \;=\; \mathfrak{p}$$

Finally, prove $\mathfrak{P}$ maximal if and only if $\mathfrak{p}$ is. For $\mathfrak{p}$ maximal, $\mathfrak{o}/\mathfrak{p}$ is a field, and $\mathfrak{O}/\mathfrak{P}$ is an integral domain, in any case. Show that an integral domain R *integral over* a field k is a field. Indeed, for $f(y) = 0$ minimal, with $a_i \in k$ and $0 \neq y \in R$, $k[y]$ is the field $k[Y]/\langle f(Y)\rangle$. In particular, y is invertible.

On the other hand, for $\mathfrak{P}$ maximal, the field $\mathfrak{O}/\mathfrak{P}$ is integral over $\mathfrak{o}/\mathfrak{p}$. If $\mathfrak{o}/\mathfrak{p}$ were not a field, it would have a maximal ideal $\mathfrak{m}$, which would be prime. By lying-over, there would be a prime of $\mathfrak{O}/\mathfrak{P}$ lying over $\mathfrak{m}$, impossible. Thus, $\mathfrak{p}$ is maximal. ///

Opportunistic calculation device: *If* $\mathfrak{O} = \mathfrak{o}[y]$, with y satisfying minimal (monic) $f(y) = 0$, have a bijection

$$\{\text{irreducible factors of } f \bmod \mathfrak{p}\} \longleftrightarrow \{\text{primes over } \mathfrak{p}\}$$

by

$$\text{factor } \overline{f}_j \text{ of } f(Y) \bmod \mathfrak{p} \quad \longrightarrow \quad \ker\big(\mathfrak{O} \to \mathfrak{o}/\mathfrak{p}[Y] \,/\, \langle \overline{f}_j(Y)\rangle\big)$$

[9.2] Remark: For $\mathfrak{o}$ the ring of algebraic integers in a number field k (=integral closure of $\mathbb{Z}$ in k), it is *not* generally true that the integral closure $\mathfrak{O}$ of $\mathfrak{o}$ in a further finite extension K is of the form $\mathfrak{o}[y]$, although this *is true* for cyclotomic fields and some other examples.

Nevertheless, the *local* rings $S^{-1}\mathfrak{o}$ for $S = \mathfrak{o} - \mathfrak{p}$ *do have* the form $S^{-1}\mathfrak{O} = S^{-1}\mathfrak{o}[y]$ for almost all $\mathfrak{o}$, so the calculational device applies *almost everywhere locally.*

Proof: Localizing, reduce to $\mathfrak{p}$ maximal. As earlier,

$$\mathfrak{O} \longrightarrow \mathfrak{O}/\mathfrak{p} \approx \mathfrak{o}[y]/\mathfrak{p} \approx \mathfrak{o}[Y]\Big/\langle f(Y),\mathfrak{p}\rangle \approx \mathfrak{o}/\mathfrak{p}[Y]\Big/\langle f(Y) \bmod \mathfrak{p}\rangle \approx \bigoplus_j \mathfrak{o}/\mathfrak{p}[Y]\Big/\overline{f}_j(Y)^{e_j}$$

where $\overline{f}_j$ are the distinct irreducible factors. Typically, the exponents e_j will be 1. In any case, this maps to $\mathfrak{o}/\mathfrak{p}[Y]/\overline{f}_j(Y)$, which is a *field*. Thus, the kernel is a maximal, hence prime, ideal $\mathfrak{P}$ containing $\mathfrak{p}$.

On the other hand, $\mathfrak{o}[y] = \mathfrak{O} \to \mathfrak{O}/\mathfrak{P}$ sends y to a root of some irreducible factor $\overline{f}_j$ of f mod $\mathfrak{p}$. Two roots of $\overline{f}$ are Galois-conjugate over $\mathfrak{o}/\mathfrak{p}$ if and only if they are roots of the same irreducible mod $\mathfrak{p}$. ///

Sun-Ze's theorem: For ideals $\mathfrak{a}_j$ in $\mathfrak{o}$ such that $\mathfrak{a}_i + \mathfrak{a}_j = \mathfrak{o}$ for $i \neq j$, given x_j, there is $x \in \mathfrak{o}$ such that $x = x_j \bmod \mathfrak{a}_j$ for all j.

Proof: The hypothesis gives $a_1 \in \mathfrak{a}_1, a_2 \in \mathfrak{a}_2$ such that $a_1 + a_2 = 1$. Then $x = x_2a_1 + x_1a_2$ solves the problem for two ideals. Induction: for $j > 1$, let $b_j \in \mathfrak{a}_1$ and $c_j \in \mathfrak{a}_j$ such that $b_j + c_j = 1$. Then

$$1 = \prod_{j>1}(b_j + c_j) \in \mathfrak{a}_1 + \prod_{j>1}\mathfrak{a}_j$$

That is, $\mathfrak{a}_1 + \prod_{j>1}\mathfrak{a}_j = \mathfrak{o}$. Thus, there is $y_1 \in \mathfrak{o}$ such that $y_1 = 1 \bmod \mathfrak{a}_1$ and $y_1 = 0 \bmod \prod_{j>1}\mathfrak{a}_j$. Similarly, find $y_i = 1 \bmod \mathfrak{a}_i$ and $y_i = 0 \bmod \prod_{j\neq i}\mathfrak{a}_j$. Then $x = \sum_j x_jy_j$ is $x_i \bmod \mathfrak{a}_i$. ///

[9.3] Transitivity of Galois groups on primes lying over $\mathfrak{p}$ Let K/k be finite *Galois*, $\mathfrak{o}$ integrally closed in k, $\mathfrak{O}$ its integral closure in K. Let $\mathfrak{p}$ be prime in $\mathfrak{o}$. The Galois group $G = \mathrm{Gal}(K/k)$ is *transitive* on primes lying over $\mathfrak{p}$ in $\mathfrak{O}$.

Proof: Localize to assume $\mathfrak{p}$ *maximal.* For two primes $\mathfrak{P}, \mathfrak{Q}$ over $\mathfrak{p}$, if no Galois image $\sigma\mathfrak{P}$ is $\mathfrak{Q}$, then there is a solution to

$$x = \begin{cases} 0 \bmod \mathfrak{Q} \\ \\ 1 \bmod \sigma\mathfrak{P} \ \text{ for all } \sigma \in G \end{cases}$$

The norm $N_k^K(x)$ is in $k \cap \mathfrak{O} = \mathfrak{o}$, by integral closure of $\mathfrak{o}$, and then is in $\mathfrak{Q} \cap \mathfrak{o} = \mathfrak{p}$. On the other hand, $\sigma^{-1}x \notin \mathfrak{P}$, for all $\sigma \in G$, so $N_k^K(x) \notin \mathfrak{P}$, contradicting $N_k^K(x) \in \mathfrak{p} \subset \mathfrak{P}$. ///

[9.4] Corollary: In $\mathfrak{O}/\mathfrak{o}$ in K/k, there are only finitely-many prime ideals lying over a given prime of $\mathfrak{o}$.

Proof: If we can reduce to the Galois-extension case, we're done, by the previous.

Let K' be a Galois closure of K/k, with integral closure $\mathfrak{O}'$, and $\mathfrak{Q}_1, \mathfrak{Q}_2$ prime ideals in K' lying over $\mathfrak{P}_1, \mathfrak{P}_2$ in $\mathfrak{O}$ lying over $\mathfrak{p}$ in $\mathfrak{o}$. For $\mathfrak{P}_1 \neq \mathfrak{P}_2$, since (from above) $\mathfrak{Q}_j \cap \mathfrak{O} = \mathfrak{P}_j$, necessarily $\mathfrak{Q}_1 \neq \mathfrak{Q}_2$. Thus, the finitude of primes in $\mathfrak{O}'$ lying over $\mathfrak{p}$ implies that in $\mathfrak{O}$. ///

In Galois K/k, since $\mathfrak{O}$ is integrally closed, it is stable under $\mathrm{Gal}(K/k)$.

For maximal $\mathfrak{P}$ lying over $\mathfrak{p}$ in $\mathfrak{o}$, the *decomposition group* [sic] $G_{\mathfrak{P}}$ is the *stabilizer* of $\mathfrak{P}$.

The *decomposition field* of $\mathfrak{P}$ is

$$K^{\mathfrak{P}} \;=\; \text{subfield of } K \text{ fixed by } G_{\mathfrak{P}}$$

Let

$$\mathfrak{o}' \;=\; \text{integral closure of } \mathfrak{o} \text{ in } K^{\mathfrak{P}} \qquad\qquad \mathfrak{q} \;=\; K^{\mathfrak{P}} \cap \mathfrak{P} \;=\; \mathfrak{o}' \cap \mathfrak{P}$$

[9.5] Corollary: $\mathfrak{P}$ is the only prime of $\mathfrak{O}$ lying above $\mathfrak{q}$.

Proof: $\mathrm{Gal}(K/K^{\mathfrak{P}}) = G_{\mathfrak{P}}$ doesn't move $\mathfrak{P}$, but is transitive on primes lying over $\mathfrak{q}$. ///

10. *Localization*

Simplest case: field-of-fractions k of an integral domain $\mathfrak{o}$. We know what is intended: $\mathfrak{o}$ injects to k, every non-zero element of $\mathfrak{o}$ becomes invertible, and there's nothing extra.

A mapping characterization proves uniqueness: for *any* ring hom $\varphi : \mathfrak{o} \to K$ to a field K, there is a unique $\Phi : k \to K$ giving a commutative diagram

$$\begin{tikzcd}
k \arrow[rd, dashed, "\exists\Phi"] & \\
\mathfrak{o} \arrow[u, "i"] \arrow[r, "\forall\varphi"] & K
\end{tikzcd}$$

Existence is proven by (the usual) construction: ...

The candidate for k is pairs $(a, b) =$ " $\dfrac{a}{b}$ " with $b \neq 0$, modulo the equivalence derived from equality of fractions: $(a, b) \sim (a', b')$ when $ab' - a'b = 0$, and $j : \mathfrak{o} \to k$ by $j(x) = (x, 1)$.

Thus, the *value* of a fraction is unchanged when top and bottom are multiplied by the same (non-zero) element of $\mathfrak{o}$, or when the same (non-zero) factor is removed. However, for non-UFDs $\mathfrak{o}$ the equivalence relation is more complicated.

Addition, multiplication, and inversion are defined as expected:

$$(a, b) + (c, d) \;=\; (ad, bd) + (bc, bd) \;=\; (ad + bc, bd)$$

$$(a, b) \cdot (c, d) \;=\; (ac, bd) \qquad\qquad (a, b)^{-1} \;=\; (b, d)$$

... but well-definedness, commutativity, associativity, and distributivity need proof.

For well-definedness of addition, suppose $(a,b) \sim (a',b')$ and $(c,d) \sim (c',d')$, and show $(ad+bc,bd) \sim (a'd'+b'c',b'd')$:

$$b'd'(ad+bc) - bd(a'd'+b'c') \;=\; (ab')dd' + (cd')bb' - (a'b)dd' - (c'd)bb'$$

$$=\; (ab'-a'b)dd' + (cd'-c'd)bb' \;=\; 0 \cdot dd' + 0 \cdot bb' \;=\; 0$$

Then, commutativity and associativity are as usual, by putting things over a common denominator. Commutativity follows from the formula and from commutativity of addition and multiplication in $\mathfrak{o}$:

$$\frac{a}{b} + \frac{a'}{b'} \;=\; \frac{ab'}{bb'} + \frac{a'b}{bb'} \;=\; \frac{ab'+a'b}{bb'}$$

Associativity of addition:

$$\frac{a}{b} + (\frac{a'}{b'} + \frac{a''}{b''}) \;=\; \frac{a}{b} + (\frac{a'b''}{b'b''} + \frac{a''b'}{b'b''}) \;=\; \frac{a}{b} + \frac{a'b''+a''b'}{b'b''} \;=\; \frac{ab'b''}{bb'b''} + \frac{ba'b''+a''bb''}{bb'b''}$$

$$=\; \frac{ab'b''+a'bb''+a''bb''}{bb'b''} \;=\; \text{symmetrical}$$

Commutativity and associativity of multiplication are easier. Distributivity is similar.

If well-defined, $\Phi(a/b) = \varphi(a)\varphi(b)^{-1}$ fits into the diagram. For well-definedness, with $ab' = a'b$,

$$\varphi(a)\varphi(b)^{-1} - \varphi(a')\varphi(b')^{-1} \;=\; \big(\varphi(a)\varphi(b') - \varphi(a')\varphi(b)\big) \cdot \varphi(b)^{-1}\varphi(b')^{-1}$$

$$=\; \varphi(ab'-a'b) \cdot \varphi(b)^{-1}\varphi(b')^{-1} \;=\; \varphi(0) \cdot \varphi(b)^{-1}\varphi(b')^{-1} \;=\; 0$$

Finally, verify that the constructed $\Phi(a/b) = \varphi(a)\varphi(b)^{-1}$ truly is a ring hom. For example, addition is respected:

$$\Phi(\frac{a}{b} + \frac{a'}{b'}) \;=\; \Phi(\frac{ab'+a'b}{bb'}) \;=\; \varphi(ab'+a'b)\varphi(bb')^{-1}$$

$$=\; \Big(\varphi(a)\varphi(b') + \varphi(a')\varphi(b)\Big)\varphi(b)^{-1}\varphi(b')^{-1} \;=\; \varphi(a)\varphi(b)^{-1} + \varphi(a')\varphi(b')^{-1} \;=\; \Phi(\frac{a}{b}) + \Phi(\frac{a'}{b'})$$

[10.1] Remark: The point is *not* the formulas for arithmetic of fractions, *nor* the checking that the construction succeeds, but that these formulas *succeed* in proving *existence*, by construction, of the field-of-fractions. Its *properties* are unequivocally determined by the mapping characterization.

Important special case: Localization at a prime. For $\mathfrak{o}$ be a commutative ring with 1, and $\mathfrak{p}$ a prime ideal, we want to modify $\mathfrak{o}$ so that it has a unique maximal ideal $\mathfrak{m}$ coming from $\mathfrak{p}$, while all *other* ideals $\mathfrak{a}$ *not* contained in $\mathfrak{p}$ *disappear.*

More precisely, $\mathfrak{o}$-*localized-at*-$\mathfrak{p}$ should be a ring $\mathfrak{o}_\mathfrak{p}$ (subscript does *not* denote completion here) with ring hom $i : \mathfrak{o} \to \mathfrak{o}_\mathfrak{p}$ such that $i(\mathfrak{q}) \cdot \mathfrak{o}_\mathfrak{p} = \mathfrak{o}_\mathfrak{p}$ for all primes $\mathfrak{q}$ not contained in $\mathfrak{p}$, $i(\mathfrak{p}) \cdot \mathfrak{o}_\mathfrak{p}$ is the unique maximal ideal $\mathfrak{m}$ of $\mathfrak{o}_\mathfrak{p}$, and $j^{-1}\big(j(\mathfrak{o}) \cap \mathfrak{m}\big) = \mathfrak{p}$.

$\mathfrak{o}_\mathfrak{p}$ should be neither *needlessly big* nor *needlessly small*, so should be *characterized* by a *universal property*: for *any* ring hom $\varphi : \mathfrak{o} \to R$ with $\varphi(\mathfrak{a}) \cdot R = R$ for ideals $\mathfrak{a}$ not contained in $\mathfrak{p}$, there is a unique Φ giving a commutative diagram

$$\begin{tikzcd}
\mathfrak{o}_\mathfrak{p} \arrow[rd, dashed, "\exists\Phi"] & \\
\mathfrak{o} \arrow[u, "i"] \arrow[r, "\forall\varphi"] & R
\end{tikzcd}$$

Characterization by a universal property proves uniqueness..., when *existence* is proven, probably by a *construction.*

The property $j^{-1}\big(j(\mathfrak{o}) \cap \mathfrak{m}\big) = \mathfrak{p}$ should *follow.*

[10.2] Example: An *integral domain* $\mathfrak{o}$ sits inside its *field of fractions* k, and localizing at $\mathfrak{p}$ simply allows all denominators not in $\mathfrak{p}$

$$\mathfrak{o}_p \;=\; \big\{\frac{x}{a} \;:\; a \notin \mathfrak{p},\; x \in \mathfrak{o}\big\} \qquad\qquad \text{(integral domain } \mathfrak{o}\text{)}$$

The requisite map $\mathfrak{o} \to \mathfrak{o}_\mathfrak{p}$ is just *inclusion.*

Proof: On one hand, any ideal $\mathfrak{a}$ not contained in $\mathfrak{p}$ contains an element s not in $\mathfrak{p}$, which therefore becomes a *unit* in the candidate $\mathfrak{o}_\mathfrak{p}$. That is, the ideal generated by $\mathfrak{a}$ in the candidate $\mathfrak{o}_\mathfrak{p}$ is the whole ring. In particular, the ideal generated by $\mathfrak{p}$ becomes the unique maximal ideal.

On the other hand, let $\varphi : \mathfrak{o} \to R$ with $\varphi(\mathfrak{a}) \cdot R = R$ for $\mathfrak{a}$ not contained in $\mathfrak{p}$. That is, $\varphi(\mathfrak{a})$ contains a unit in R. This hypothesis applied to principal ideals $\langle a \rangle$ shows that $\varphi(x)\varphi(a) = \varphi(xa) \in R^\times$ for some $x \in \mathfrak{o}$, and $\varphi(a)$ is a unit. That is, *every* $\varphi(a)$ for $a \notin \mathfrak{p}$ is a unit in R.

Try to define $\Phi(x/a) = \varphi(x) \cdot \varphi(a)^{-1}$ for $a \notin \mathfrak{p}$. Check well-definedness: $x/a = x'/a'$ in k gives

$$\varphi(a)\varphi(a')\big(\varphi(x)\varphi(a)^{-1} - \varphi(x')\varphi(a')^{-1}\big)$$

$$=\; \varphi(a'x) - \varphi(ax') \;=\; \varphi(a'x - ax') \;=\; \varphi(0) \;=\; 0$$

Units $\varphi(a)$ and $\varphi(a')$ have inverses, giving well-definedness.

Multiplicativeness of Φ is easy. Addition is preserved: via re-expression with a common denominator, as expected:

$$\Phi(\frac{x}{a} + \frac{x'}{a'}) \;=\; \Phi(\frac{xa' + x'a}{aa'}) \;=\; \Phi(xa' + x'a)\varphi(aa')^{-1}$$

$$=\; \big(\varphi(x)\varphi(a') + \varphi(x')\varphi(a)\big) \cdot \varphi(a)^{-1}\varphi(a')^{-1}$$

$$=\; \varphi(x)\varphi(a)^{-1} + \varphi(x')\varphi(a')^{-1} \;=\; \Phi(\frac{x}{a}) + \Phi(\frac{x'}{a'})$$

This proves that the usual construction succeeds for *integral domains*, proving *existence* of the localization.

Localization in general: For non-integral-domains $\mathfrak{o}$, *collapsing* can occur in localizations $j : \mathfrak{o} \to \mathfrak{o}_\mathfrak{p}$.

[10.3] Example: Localizing $\mathfrak{o} = \mathbb{Z}/30$ at the prime ideal $\mathfrak{p} = 3 \cdot \mathbb{Z}/30$ requires that $10 \notin \mathfrak{p}$ become a unit in the image $j : \mathfrak{o} \to \mathfrak{o}_\mathfrak{p}$. Thus,

$$j(3) \;=\; j(3) \cdot j(10) \cdot j(10)^{-1} \;=\; j(30) \cdot j(10)^{-1} \;=\; 0 \cdot j(10)^{-1}$$

Thus (!) $\mathfrak{o}_\mathfrak{p} = \mathbb{Z}/3$, and $\mathbb{Z}/30 \to \mathbb{Z}/3$ is the quotient map. Generally, $j : \mathfrak{o} \to \mathfrak{o}_\mathfrak{p}$ sends zero-divisors $x \in \mathfrak{p}$ with $xy = 0$ for $y \notin \mathfrak{p}$ to 0:

$$0 \;=\; j(0) \cdot j(y)^{-1} \;=\; j(xy)j(y)^{-1} \;=\; j(x)j(y)j(y)^{-1} \;=\; j(x)$$

This explains the more complicated equivalence relation in the general proof-of-existence-by-construction of localization:

[10.4] Claim: The localization $j : \mathfrak{o} \to \mathfrak{o}_\mathfrak{p}$ *exists*: it can be constructed as pairs $\{(a,b) : x \in \mathfrak{o},\; b \notin \mathfrak{p}\}$, identifying $(a.b)$, (a',b') when $c \cdot (ab' - a'b) = 0$ for some $c \in \mathfrak{o} - \mathfrak{p}$, with addition and multiplication as usual. Given $\varphi : \mathfrak{o} \to R$, the corresponding $\Phi : \mathfrak{o}_\mathfrak{p} \to R$ is $\Phi(\frac{a}{b}) = \varphi(a)\varphi(b)^{-1}$.

Proof: There is a slight novelty in the well-definedness of Φ: for $c \cdot (ab' - a'b) = 0$,

$$0 \;=\; \varphi(0) \;=\; \varphi(c) \cdot \Big(\varphi(a)\varphi(b') - \varphi(a')\varphi(b)\Big)$$

$\varphi(c)$, $\varphi(b)$, $\varphi(b') \in R^\times$. Divide by the product of their inverses:

$$0 \;=\; \varphi(a)\varphi(b)^{-1} - \varphi(a')\varphi(b')^{-1} \;=\; \Phi(\frac{a}{b}) - \Phi(\frac{a'}{b'}) \qquad ///$$

[10.5] **Remark:** Now it becomes interesting so check that $\mathfrak{o}_\mathfrak{p}$ is not accidentally the degenerate ring $\{0\}$! This would use the hypothesis that no product of elements of $S = \mathfrak{o} - \mathfrak{p}$ is 0.

[10.6] **Remark:** It would be reasonable to be impatient with, or even repelled by, the (tedious!) details involved in verification that things are well-defined, and that the construction really produces a *ring*, and that Φ is a ring homomorphism, etc.

What's the alternative?

First, we may as well formulate the most general case: For an arbitrary subset S (not just the complement of a prime ideal) of a commutative ring with identity $\mathfrak{o}$, the localization $j : \mathfrak{o} \to S^{-1}\mathfrak{o}$ can be characterized by a *universal property*: for *any* ring hom $\varphi : \mathfrak{o} \to R$ with $\varphi(S) \subset R^\times$, there is a unique Φ giving a commutative diagram

$$\begin{tikzcd}
S^{-1}\mathfrak{o} \arrow[rd, dashed, "\exists\Phi"] & \\
\mathfrak{o} \arrow[u, "i"] \arrow[r, "\forall\varphi"'] & R
\end{tikzcd}$$

Characterization by a universal property proves uniqueness..., when *existence* is proven, probably by a (hopefully graceful) *construction*.

Consider an expression as a quotient of a polynomial ring with indeterminates x_s for all $s \in S$:

$$S^{-1}\mathfrak{o} \;=\; \mathfrak{o}[\{x_s : s \in S\}] \Big/ \Big(\text{ideal generated by } \; sx_s - 1, \; \forall s \in S\Big)$$

with $j : \mathfrak{o} \to S^{-1}\mathfrak{o}$ induced by the inclusion $\mathfrak{o} \to \mathfrak{o}[\ldots, x_s, \ldots]$.

This produces a *ring*, for any $S \subset \mathfrak{o}$. Given $\varphi : \mathfrak{o} \to R$ with $\varphi(S) \subset R^\times$, the universal mapping properties of polynomial rings give a unique $\widetilde{\varphi}$ extending φ to the polynomial ring by

$$\widetilde{\varphi}(x_s) \;=\; \varphi(s)^{-1}$$

Then $\widetilde{\varphi}$ factors uniquely through the *quotient*, since

$$\widetilde{\varphi}(sx_s - 1) \;=\; \varphi(s)\widetilde{\varphi}(x_s) - \varphi(1) \;=\; 1 - 1 \;=\; 0$$

The diagram of well-defined, uniquely-determined ring homs:

$$\begin{tikzcd}
\mathfrak{o}[\ldots, x_s, \ldots] \arrow[rr, "\exists\,!\,\mathrm{quot}"] \arrow[rrd, dotted, "\exists!\,\widetilde{\varphi}"] & & \dfrac{\mathfrak{o}[\ldots, x_s, \ldots]}{\langle \ldots, sx_s - 1, \ldots \rangle} \arrow[d, dashed, "\exists!\,\Phi"] \\
& \mathfrak{o} \arrow[lu] \arrow[ru, bend left, "j"] \arrow[r, "\forall\varphi"] & R
\end{tikzcd}$$

with $\widetilde{\varphi}$ uniquely induced by $\widetilde{\varphi}(x_s) = \varphi(s)^{-1}$, and Φ uniquely induced by $\widetilde{\varphi}$.

What more is needed? When the ring $\mathfrak{o}$ has 0-divisors, it is not clear that there *are* any such rings R (with $0 \neq 1$!!!) over which to quantify, and/or that $S^{-1}\mathfrak{o}$ is not the trivial ring $\{0\}$ with $0 = 1$.

Indeed, if any product of elements of S is 0, $S^{-1}\mathfrak{o} = \{0\}$, but the above construction seems to succeed without this hypothesis.

[10.7] Claim: In $S^{-1}\mathfrak{o}$, $0 \neq 1$ if and only if no product of elements of S is 0.

Proof: The degeneration $1 = 0$ in the quotient is equivalent to existence of an expression

$$\sum_{i=1}^{n} f_i(x_1, \ldots, x_n) \cdot (s_i x_i - 1) \;=\; 1 \;\in\; \mathfrak{o}[x_1, \ldots, x_n]$$

where $x_i = x_{s_i}$, for some *finite* subset $S_o = \{s_1, \ldots, s_n\}$ of S, where $f_i(x_1, \ldots, x_n)$ is a polynomial with coefficients in $\mathfrak{o}$.

One direction is easy: if $st = 0$ for $s, t \in S$, then in the quotient

$$S^{-1}\mathfrak{o} \;=\; \mathfrak{o}[x, y]/\langle sx - 1,\, ty - 1\rangle$$

we compute

$$1 \;=\; 1 \cdot 1 \;=\; sx \cdot ty \;=\; st \cdot xy \;=\; 0 \cdot xy \;=\; 0 \qquad\qquad (\text{in } S^{-1}\mathfrak{o})$$

That is, in $\mathfrak{o}[x, y]$ itself,

$$\begin{aligned} 1 \;&=\; (1 - sx + sx)(1 - ty + ty) \\ &=\; (1 - sx)(1 - ty) + sx(1 - ty) + ty(1 - sx) + sxty \\ &=\; (1 - sx)(1 - ty) + sx(1 - ty) + ty(1 - sx) + 0 \end{aligned}$$

which is in the ideal generated by $1 - sx$ and $(1 - ty)$.

For the other direction, for $S = \{s\}$ with a single element, a condition

$$(c_\ell x^\ell + \ldots + c_1 x + c_o) \cdot (sx - 1) \;=\; 1$$

gives $c_o = -1$ and $c_k = -s^k$, and $s^{\ell+1} = 0$.

Inductively, suppose we have the claim for $|S| \leq n - 1$. Let $S = \{s_1, \ldots, s_n\}$, and suppose $S^{-1}\mathfrak{o} = \{0\}$.

From the mapping characterization, it is immediate that localization can be done stepwise: there is a natural isomorphism

$$(S_1 \cup S_2)^{-1}\mathfrak{o} \;\approx\; S_1^{-1}\Big(S_2^{-1}\mathfrak{o}\Big)$$

Let $\mathfrak{o}' = \{s_n\}^{-1}\mathfrak{o}$ and $S' = \{s_1, \ldots, s_{n-1}\}$. Then $0 = 1$ in $S'^{-1}\mathfrak{o}'$ implies that $s_1^{\ell_1} \ldots s_{n-1}^{\ell_{n-1}} = 0$ in $\mathfrak{o}'$, for some non-negative integer exponents. Since $\mathfrak{o}' = \mathfrak{o}[x]/\langle s_n x - 1\rangle$, for some coefficients c_i

$$s_1^{\ell_1} \ldots s_{n-1}^{\ell_{n-1}} \;=\; (c_\ell x^\ell + \ldots + c_o)(s_n x - 1)$$

Then $c_o = -s_1^{\ell_1} \ldots s_{n-1}^{\ell_{n-1}}$, and $s_1^{\ell_1} \ldots s_{n-1}^{\ell_{n-1}} \cdot s_n^{\ell+1} = 0$. ///

Corresponding localization of modules and algebras: Let $i : \mathfrak{o} \to \mathfrak{o}_\mathfrak{p}$ be the localization. For an $\mathfrak{o}$-module M, it should not be surprising that the useful notion of *localization* of M creates an $\mathfrak{o}_\mathfrak{p}$-module $M_\mathfrak{p}$ by

$$M_\mathfrak{p} \;=\; \mathfrak{o}_\mathfrak{p} \otimes_\mathfrak{o} M$$

Similarly, for a (commutative) $\mathfrak{o}$-algebra A,

$$A_{\mathfrak{p}} \;=\; \mathfrak{o}_{\mathfrak{p}} \otimes_{\mathfrak{o}} A$$

Or, why not the *other* extension of scalars, $M_{\mathfrak{p}} = \mathrm{Hom}_{\mathfrak{o}}(\mathfrak{o}_{\mathfrak{p}}, M)$? **Last:** $S^{-1}\mathfrak{o}$ is not the trivial ring $\{0\}$ with $0 = 1$ if and only if no product of elements of S is 0. [Proven last time.]

Localization of modules and algebras: For an $\mathfrak{o}$-module M or (commutative) $\mathfrak{o}$-algebra A, it should not be surprising that the useful notions of *localization* of M and A are by

$$M_{\mathfrak{p}} \;=\; \mathfrak{o}_{\mathfrak{p}} \otimes_{\mathfrak{o}} M \qquad\qquad A_{\mathfrak{p}} \;=\; \mathfrak{o}_{\mathfrak{p}} \otimes_{\mathfrak{o}} A$$

Though, why not the *other* extensions of scalars, $M_{\mathfrak{p}} = \mathrm{Hom}_{\mathfrak{o}}(\mathfrak{o}_{\mathfrak{p}}, M)$ and $A_{\mathfrak{p}} = \mathrm{Hom}_{\mathfrak{o}}(\mathfrak{o}_{\mathfrak{p}}, A)$? Recall what we needed in the argument.

$$\begin{tikzcd}
\mathfrak{O} \arrow[r] \arrow[d, dash] & S^{-1}\mathfrak{P} \arrow[d, dash] & \supset \mathfrak{M} \\
\mathfrak{o} \arrow[r] & S^{-1}\mathfrak{o} & \supset \mathfrak{m}
\end{tikzcd}$$

11. *More about primes-lying-over*

The picture is

$$\begin{tikzcd}
K \arrow[r, dash, "\supset"] \arrow[dd, dash, "G_{\mathfrak{P}}"'] & \mathfrak{O} \arrow[r, dash, "\supset"] \arrow[dd, dash] \arrow[drr] & \mathfrak{P} \arrow[dd, dash] & \\
& & & \mathfrak{O}/\mathfrak{P} = \tilde{\kappa} \arrow[dd, dash] \\
K^{\mathfrak{P}} \arrow[r, dash, "\supset"] \arrow[dd, dash] & \mathfrak{O}^{\mathfrak{P}} \arrow[r, dash, "\supset"] \arrow[dd, dash] \arrow[drr] & \mathfrak{Q} = \mathfrak{P} \cap K^{\mathfrak{P}} \arrow[dd, dash] & \\
& & & \mathfrak{O}^{\mathfrak{P}}/\mathfrak{Q} \arrow[dd, dash, "="', "\text{[pf below]}"] \\
k \arrow[r, dash, "\supset"] & \mathfrak{o} \arrow[r, dash, "\supset"] \arrow[drr] & \mathfrak{p} & \\
& & & \mathfrak{o}/\mathfrak{p} = \kappa
\end{tikzcd}$$

[11.1] Claim: The inclusion $\mathfrak{o}/\mathfrak{p} \to \mathfrak{O}^{\mathfrak{P}}/\mathfrak{Q}$ is an isomorphism.

[11.2] Claim: $\tilde{\kappa} = \mathfrak{O}/\mathfrak{P}$ is *normal* over $\kappa = \mathfrak{o}/\mathfrak{p}$, and $G_{\mathfrak{P}}$ surjects to $\mathrm{Aut}(\tilde{\kappa}/\kappa)$.

More named objects: The **inertia group**: $I_{\mathfrak{P}}$ is the kernel of $G_{\mathfrak{P}} \to \mathrm{Gal}(\tilde{\kappa}/\kappa)$. The fixed field of $I_{\mathfrak{P}}$ is the **inertia subfield** of K. These will not be used much here.

$\mathfrak{p}$ **splits completely** in K when there are $[K : k]$ distinct primes lying over $\mathfrak{p}$ in $\mathfrak{O}$.

[11.3] Corollary: For an *abelian* K/k, the decomposition subfield $K^{\mathfrak{P}}$ is the maximal subfield of K (containing k) in which $\mathfrak{p}$ splits completely.

Frobenius map/automorphism in the number field (or function field) case is anything that maps to $x \to x^q$ in the residue class field extension $\tilde{\kappa}/\kappa = \mathbb{F}_{q^n}/\mathbb{F}^q$.

Artin map/automorphism ... is Frobenius for *abelian* extensions. A **fractional ideal** $\mathfrak{a}$ of $\mathfrak{o}$ in its fraction field k is an $\mathfrak{o}$-submodule of k such that there is $0 \neq c \in \mathfrak{o}$ such that $c\mathfrak{a} \subset \mathfrak{o}$.

[11.4] Theorem: In Noetherian, integrally closed ring $\mathfrak{o}$ in which every non-zero prime ideal is *maximal*, every non-zero ideal is uniquely a product of prime ideals, and the non-zero fractional ideals form a *group* under multiplication. [Below...]

Noetherian, integrally-closed commutative rings in which every non-zero prime ideal is maximal are **Dedekind rings**.

And the decomposition subfield $K^{\mathfrak{P}}$ (=fixed field of decomposition group $G_{\mathfrak{P}}$) is the smallest subfield of K such that $\mathfrak{P}$ is the only prime lying over $K^{\mathfrak{P}} \cap \mathfrak{P}$.

[11.5] Claim: The inclusion $\mathfrak{o}/\mathfrak{p} \to \mathfrak{O}^{\mathfrak{P}}/\mathfrak{q}$ to the residue field attached to the decomposition field of $\mathfrak{P}$ is an *isomorphism.*

Proof: The induced map is indeed an *inclusion*, because

$$\mathfrak{p} \;=\; k \cap \mathfrak{P} \;=\; k \cap K^{\mathfrak{P}} \cap \mathfrak{P}$$

For surjectivity: for $\sigma \in G$ but not in $G_{\mathfrak{P}}$, $\sigma\mathfrak{P} \neq \mathfrak{P}$, and the prime ideal

$$\mathfrak{q}_\sigma \;=\; K^{\mathfrak{P}} \cap \sigma\mathfrak{P}$$

is not $\mathfrak{q}$, since $\mathfrak{P}$ is the only prime lying over $\mathfrak{q}$.

Thus, given $x \in \mathfrak{O}^{\mathfrak{P}}$, Sun-Ze's theorem gives $y \in \mathfrak{O}^{\mathfrak{P}}$ such that

$$\begin{cases} y \;=\; x \quad \bmod \mathfrak{q} \\ y \;=\; 1 \quad \bmod \mathfrak{q}_\sigma \quad (\text{for all } \sigma \text{ not in } G_{\mathfrak{P}}) \end{cases}$$

Thus, certainly in the larger ring $\mathfrak{O}$

$$\begin{cases} y \;=\; x \quad \bmod \mathfrak{P} \\ y \;=\; 1 \quad \bmod \sigma\mathfrak{P} \quad (\text{for all } \sigma \text{ not in } G_{\mathfrak{P}}) \end{cases}$$

That is, $\sigma y = 1 \bmod \mathfrak{P}$ for $\sigma \notin G^{\mathfrak{P}}$. The Galois norm of y from $K^{\mathfrak{P}}$ to k is a product of y with images σy with $\sigma \notin G^{\mathfrak{P}}$. Therefore,

$$N_k^{K^{\mathfrak{P}}} y \;=\; x \bmod \mathfrak{P}$$

The norm is in $\mathfrak{o}$, and the congruence holds mod $\mathfrak{q}$ since $x \in \mathfrak{O}^{\mathfrak{P}}$. ///

[11.6] Claim: $\tilde\kappa = \mathfrak{O}/\mathfrak{P}$ is *normal* over $\kappa = \mathfrak{o}/\mathfrak{p}$, and $G_{\mathfrak{P}}$ *surjects* to $\text{Gal}(\tilde\kappa/\kappa)$.

Proof: Let $\alpha \in \mathfrak{O}$ generate a separable subextension (mod $\mathfrak{P}$) of $\tilde\kappa$ over κ. The minimal polynomial of α over k has coefficients in $\mathfrak{o}$ because α is integral over $\mathfrak{o}$. Since K/k is Galois, f splits into linear factors $x - \alpha_i$ in $K[x]$. Then f mod $\mathfrak{P}$ factors into linear factors $x - \bar\alpha_i$ where $\bar\alpha_i$ is α_i mod $\mathfrak{P}$.

Thus, whatever the minimal polynomial of $\bar\alpha$ over κ, it factors into linear factors in $\tilde\kappa[x]$. That is, $\tilde\kappa/\kappa$ is normal, and

$$[\kappa(\bar\alpha) : \kappa] \;\le\; [k(\alpha) : k] \;\le\; [K : k]$$

By the theorem of the primitive element, the maximal separable subextension is of finite degree, bounded by $[K : k]$.

To prove surjectivity of the Galois group map, it suffices to consider the situation that $\mathfrak{P}$ is the only prime over $\mathfrak{p}$, from the discussion of the decomposition group and field above. Thus, $G = G_{\mathfrak{P}}$ and $K = K^{\mathfrak{P}}$.

By the theorem of the primitive element, there is α in $\mathfrak{O}$ with image $\bar\alpha$ mod $\mathfrak{P}$ generating the (maximal separable subextension of the) residue field extension $\tilde\kappa/\kappa$. Let f be the minimal polynomial of α over k, and $\overline{f}$ the reduction of f mod $\mathfrak{p}$.

Normality of K/k gives the factorization of $f(x)$ into linear factors $x - \alpha_i$ in $\mathfrak{O}[x]$, and this factorization reduces mod $\mathfrak{P}$ to a factorization into linear factors $x - \bar\alpha_i$ in $\tilde\kappa[x]$.

Automorphisms of $\tilde\kappa/\kappa$ are determined by their effect on $\bar\alpha$, and map $\bar\alpha$ to other zeros $\bar\alpha_i$ of $\overline{f}$. Gal(K/k) is *transitive* on the α_i, so is transitive on the $\bar\alpha_i$. This proves surjectivity. ///

The **inertia subgroup** is the kernel $I_{\mathfrak{P}}$ of $G_{\mathfrak{P}} \to \text{Gal}(\tilde\kappa/\kappa)$, and the **inertia subfield** is the fixed field of $I_{\mathfrak{P}}$. (This is better called the 0^{th} **ramification** group...) For typical K/k, we'll see later that $I_{\mathfrak{P}}$ is *trivial* for most $\mathfrak{P}$.

[11.7] Remark: For us, $\tilde{\kappa}/\kappa$ will almost always be *separable.*

A prime $\mathfrak{p}$ is **inert** in K/k (or in $\mathfrak{O}/\mathfrak{o}$) the degree of the residue field extension (for any prime lying over $\mathfrak{p}$) is equal to the global field extension degree: $[\tilde{\kappa} : \kappa] = [K : k]$.

[11.8] Corollary: For *finite* residue field κ, existence of inert primes in K/k implies $\mathrm{Gal}(K/k)$ is *cyclic.*

Proof: Galois groups of finite extensions of finite fields are (separable and) cyclic. The degree equality requires that the map $G_{\mathfrak{P}} \to \mathrm{Gal}(\tilde{\kappa}/\kappa)$ be an *isomorphism*, and that $G = G_{\mathfrak{P}}$. ///

[11.9] Examples: In quadratic Galois extensions K/k, there is no obvious *obstacle* to primes being *inert*, since a group with 2 elements could easily surject to a group with 2 elements.

[11.10] Remark: Lack of an obstacle does not prove *existence...* Indeed, in extensions of $\mathbb{C}(x)$ no prime stays prime, since the residue fields are all $\mathbb{C}$, which is already algebraically closed.

In non-abelian Galois extensions such as $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$, with ω a cube root of unity, *no* prime $p \in \mathfrak{o} = \mathbb{Z}$ can stay prime.

The Galois group of a cyclotomic extension $\mathbb{Q}(\omega)/\mathbb{Q}$ with ω an n^{th} root of unity is $(\mathbb{Z}/n)^\times$, which is *cyclic* only for n of the form $n = p^\ell$, $n = 2p^\ell$, for p an odd prime, and for $n = 4$ (from elementary number theory).

[11.11] Examples: *(cont'd)* We had already seen that $p \in \mathbb{Z}$ stays prime in $\mathbb{Q}(\omega)/\mathbb{Q}$ if and only if the n^{th} cyclotomic polynomial Φ_n is irreducible in $\mathbb{F}_p[x]$. This irreducibility is equivalent to n *not* dividing $p^d - 1$ for any $d < \deg \Phi_n$. This is equivalent to p being a *primitive root* (=generator) for $(\mathbb{Z}/n)^\times$.

Again, a *necessary* condition for cyclic-ness of $(\mathbb{Z}/n)^\times$ is that n be of the special forms $p^\ell, 2p^\ell, 4$.

But *Dirichlet's theorem* on primes in arithmetic progression is necessary to prove existence of *primes* equal mod n to a primitive root.

Quadratic reciprocity gives a congruence condition for quadratic extensions of $\mathbb{Q}$, and Dirichlet's theorem again gives *existence.*

$\mathfrak{p}$ **splits completely** in K when there are $[K : k]$ distinct primes lying over $\mathfrak{p}$ in $\mathfrak{O}$.

[11.12] Examples: In $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$ with square-free $D \in \mathbb{Z}$, odd p not dividing D with D a square mod p *split completely*: with $D = 2, 3 \bmod 4$, for simplicity, so that the ring of integers is really $\mathbb{Z}[\sqrt{D}]$, as earlier,

$$\mathfrak{O}/p\mathfrak{O} \;=\; \mathbb{Z}[x]/\langle p,\, x^2 - D\rangle \;=\; \mathbb{F}_p[x]/\langle x^2 - D\rangle$$

In $\mathbb{Q}(\omega)/\mathbb{Q}$ with ω an n^{th} root of unity, primes $p = 1 \bmod n$ *split completely.* As we will see, the integral closure $\mathfrak{O}$ of $\mathbb{Z}$ in $\mathbb{Q}(\omega)$ really is $\mathbb{Z}[\omega]$, and then, with Φ_n the n^{th} cyclotomic polynomial,

$$\mathfrak{O}/p\mathfrak{O} \;=\; \mathbb{Z}[x]/\langle p,\, \Phi_n\rangle \;=\; \mathbb{F}_p[x]/\langle \Phi_n\rangle$$

The n^{th} cyclotomic polynomial splits into linear factors over $\mathbb{F}_p$ exactly when $p = 1 \bmod n$, because $\mathbb{F}_p^\times$ is *cyclic.*

Proof that there are infinitely-many primes $p = 1 \bmod n$ is much easier than the general case of Dirichlet's theorem:

Given a list $p_1, \ldots, p_\ell$ of primes, consider $N = \Phi_n(tp_1 \ldots p_\ell)$ for integers t at our disposal. The cyclotomic Φ_n has integer coefficients and constant coefficient ± 1, so N is not divisible by any p_j. For sufficiently large t, N cannot be ± 1, either. Thus, N has prime factors p other than p_j.

At the same time, $p|\Phi_n(j)$ for an integer j says that j is a primitive n^{th} root of unity mod p, so $p = 1 \bmod n$. ///

[11.13] Corollary: For *abelian* K/k, the decomposition subfield $K^{\mathfrak{P}}$ is the maximal subfield of K (containing k) in which $\mathfrak{p}$ splits completely.

Proof: With $\sigma_1, \ldots, \sigma_n$ representatives for $G/G_{\mathfrak{P}}$, by transitivity, $\sigma_j\mathfrak{P}$ are distinct, and are all the primes over $\mathfrak{p}$. The abelian-ness implies that the decomposition subfields $K^{\mathfrak{P}}$ for the $\sigma_j\mathfrak{P}$ are all the same.

Let $\mathfrak{q} = \mathfrak{P} \cap K^{\mathfrak{P}}$. From above, $\mathfrak{P}$ is the only prime over $\mathfrak{q}$, and $\sigma_j\mathfrak{P}$ is the only prime over $\sigma_j\mathfrak{q}$, and the latter must be *distinct.* Since $[K : k] = |G| = |G_{\mathfrak{P}}| \cdot n$, necessarily $\mathfrak{p}$ splits completely in $K^{\mathfrak{P}}$.

Conversely, with E an intermediate field in which $\mathfrak{p}$ splits completely, $G_{\mathfrak{P}}$ fixes $\mathfrak{P} \cap E$. The hypothesis that $\mathfrak{p}$ splits completely in E implies that the decomposition subgroup of $\mathfrak{P} \cap E$ in $\text{Gal}(E/k)$ is *trivial.* That is, the restriction of $G_{\mathfrak{P}}$ to E is trivial, so $G_{\mathfrak{P}} \subset \text{Gal}(K/E)$. ///

The distinguishing feature of **number fields** (finite extensions of $\mathbb{Q}$) and **function fields** (finite extensions of $\mathbb{F}_p(x)$), and their completions, is that their *residue fields are finite.*

All finite extensions of finite fields are *cyclic* (Galois). There is a canonical generator, the **Frobenius automorphism** $x \to x^q$ of the Galois group of *any* extension of $\mathbb{F}_q$.

Given a prime $\mathfrak{p}$ and $\mathfrak{P}$ lying over it in a Galois extension K/k of number fields or functions fields, with residue field extension $\tilde{\kappa}/\kappa$, with $\kappa \approx \mathbb{F}_q$, the **Frobenius map/automorphism** in $G_{\mathfrak{P}}$ is anything that maps to $x \to x^q$.

Artin map/automorphism is Frobenius for *abelian* extensions.

The point is that, by transitivity of Galois on primes $\mathfrak{P}$ lying over $\mathfrak{p}$, in an *abelian* extension all decomposition groups $G_{\mathfrak{P}}$ are the same subgroup, so the Frobenius element of $\text{Gal}(K/k)$ does not depend on the choice of $\mathfrak{P}$ over $\mathfrak{p}$.

A **fractional ideal** $\mathfrak{a}$ of $\mathfrak{o}$ in its fraction field k is an $\mathfrak{o}$-submodule of k such that there is $0 \neq c \in \mathfrak{o}$ such that $c\mathfrak{a} \subset \mathfrak{o}$.

[11.14] Examples: Fractional ideals of $\mathbb{Z}$ are $\mathbb{Z} \cdot r$ for $r \in \mathbb{Q}$.

$\mathbb{Z}$-submodules of $\mathbb{Q}$ requiring infinitely-many generators are *not* fractional ideals. E.g., neither the localization $\mathbb{Z}_{(p)}$, nor the localization

$$\bigcup_{\ell \geq 1} \frac{1}{p^\ell} \cdot \mathbb{Z} \qquad\qquad (\textbf{not} \text{ a fractional ideal})$$

[11.15] Theorem: In a Noetherian, integrally closed integral domain $\mathfrak{o}$ in which every non-zero prime ideal is *maximal*, every non-zero ideal is *uniquely a product of prime ideals*, and the non-zero fractional ideals form a *group* under multiplication. [Below]

Dedekind domains are Noetherian, integrally-closed integral domains in which every non-zero prime ideal is maximal. The **ideal class group** $I_k = I_{\mathfrak{o}}$ is the group of non-zero fractional ideals modulo *principal* fractional ideals.

Also: Dedekind domains are characterized by the fact that their ideals are finitely-generated *projective* modules. [Proof later.]

An R-module P is *projective* when any diagram

$$\begin{tikzcd} B \arrow[r] & C \arrow[r] & 0 \\ & P \arrow[u] & \end{tikzcd} \qquad\qquad (\text{with } B \to C \to 0 \text{ exact})$$

admits at least one extension to a commutative diagram

$$\begin{tikzcd}
B \arrow[r] & C \arrow[r] & 0 \\
& P \arrow[u] \arrow[ul, dashed] &
\end{tikzcd}$$

Free modules are projective, but over non-PIDs there are more.

While we're here: an R-module I is *injective* when any diagram

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] \arrow[d] & B \\
& I &
\end{tikzcd} \qquad \text{(with } 0 \to A \to B \text{ exact)}$$

admits at least one extension to a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] \arrow[d] & B \arrow[dl, dashed] \\
& I &
\end{tikzcd} \qquad \text{(with } 0 \to A \to B \text{ exact)}$$

Baer showed that, for example, *divisible* $\mathbb{Z}$-modules are injective.

The **structure theorem for finitely-generated modules** over Dedekind domains, is **Steinitz' theorem:**

A finitely-generated module M over a Dedekind domain $\mathfrak{o}$ is

$$M \approx \mathfrak{o}/\mathfrak{a}_1 \oplus \ldots \oplus \mathfrak{o}/\mathfrak{a}_n \oplus \mathfrak{o}^r \oplus \mathfrak{a}$$

where $\mathfrak{a}_1 | \ldots | \mathfrak{a}_n$ are uniquely-determined non-zero ideals, the rank r of the free part $\mathfrak{o}^r$ is uniquely determined, and the isomorphism class of the ideal $\mathfrak{a}$ is uniquely determined.

[This is often omitted from algebraic number theory books. See Milnor's *Algebraic K-theory*, or Cartan-Eilenberg.]

That is, the ideal class group is the torsion part of the K-group $K_0(\mathfrak{o})$ = projective finitely-generated $\mathfrak{o}$-modules, with tensor product, modulo free.

12. *Unique factorization of ideals in Dedekind domains*

Now we prove the factorization theorem for Dedekind domains:

[12.1] Theorem: In a Noetherian, integrally closed integral domain $\mathfrak{o}$ in which every non-zero prime ideal is *maximal*, every non-zero ideal is *uniquely a product of prime ideals*, and the non-zero fractional ideals form a *group* under multiplication.

Again, **Dedekind domains** are Noetherian, integrally-closed integral domains in which every non-zero prime ideal is maximal. The **ideal class group** $I_k = I_\mathfrak{o}$ is the group of non-zero fractional ideals modulo *principal* fractional ideals.

Proof: [Noether/van der Waerden, Lang] Let $\mathfrak{o}$ be a Noetherian integral domain, integrally closed in its field of fractions, and every non-zero prime ideal is maximal.

First: given non-zero ideal $\mathfrak{a}$, there is a product of non-zero prime ideals *contained in* $\mathfrak{a}$. If not, by Noetherian-ness there is a *maximal* ideal $\mathfrak{a}$ failing to contain a product of primes, and $\mathfrak{a}$ is not prime. Thus, there are $b, c \in \mathfrak{o}$ neither in $\mathfrak{a}$ such that $bc \in \mathfrak{a}$. Thus, $\mathfrak{b} = \mathfrak{a} + \mathfrak{o}b$ and $\mathfrak{c} = \mathfrak{a} + \mathfrak{o}c$ are strictly larger than $\mathfrak{a}$, and $\mathfrak{bc} \subset \mathfrak{a}$.

Since $\mathfrak{a}$ was maximal among ideals not containing a product of primes, both $\mathfrak{b}, \mathfrak{c}$ contain such products. But then their product $\mathfrak{bc} \subset \mathfrak{a}$ does, contradiction.

Second: for maximal $\mathfrak{m}$, the $\mathfrak{o}$-module $\mathfrak{m}^{-1} = \{x \in k : x\mathfrak{m} \subset \mathfrak{o}\}$ is strictly larger than $\mathfrak{o}$. Certainly $\mathfrak{m}^{-1} \supset \mathfrak{o}$, since $\mathfrak{m}$ is an ideal. We claim that $\mathfrak{m}^{-1}$ is strictly larger than $\mathfrak{o}$. Indeed, for $m \in \mathfrak{m}$ and a (smallest possible) product of primes $\mathfrak{p}_j$ such that

$$\mathfrak{p}_1 \ldots \mathfrak{p}_n \subset m\mathfrak{o}$$

Since $m\mathfrak{o} \subset \mathfrak{m}$ and $\mathfrak{m}$ is prime, $\mathfrak{p}_j \subset \mathfrak{m}$ for at least one $\mathfrak{p}_j$, say $\mathfrak{p}_1$. Since every (non-zero) prime is maximal, $\mathfrak{p}_1 = \mathfrak{m}$.

By minimality, $\mathfrak{p}_2 \ldots \mathfrak{p}_n \not\subset m\mathfrak{o}$. That is, there is $y \in \mathfrak{p}_2 \ldots \mathfrak{p}_n$ but $y \notin m\mathfrak{o}$, or $m^{-1}y \notin \mathfrak{o}$. But $y\mathfrak{m} = y\mathfrak{p}_1 \subset m\mathfrak{o}$, so $m^{-1}y\mathfrak{m} \subset \mathfrak{o}$, and $m^{-1}y \in \mathfrak{m}^{-1}$ but not in $\mathfrak{o}$.

Third: maximal $\mathfrak{m}$ in $\mathfrak{o}$ is invertible. By this point, $\mathfrak{m} \subset \mathfrak{m}^{-1}\mathfrak{m} \subset \mathfrak{o}$. By maximality of $\mathfrak{m}$, either $\mathfrak{m}^{-1}\mathfrak{m} = \mathfrak{m}$ or $\mathfrak{m}^{-1}\mathfrak{m} = \mathfrak{o}$.

The Noetherian-ness of $\mathfrak{o}$ implies that $\mathfrak{m}$ is finitely-generated. A relation $\mathfrak{m}^{-1}\mathfrak{m} = \mathfrak{m}$ would show that $\mathfrak{m}^{-1}$ stabilizes a non-zero, finitely-generated $\mathfrak{o}$-module. Since $\mathfrak{o}$ is integrally closed in k, this would give $\mathfrak{m}^{-1} \subset \mathfrak{o}$, but we have seen otherwise. Thus, we have the inversion relation $\mathfrak{m}^{-1}\mathfrak{m} = \mathfrak{o}$ for maximal $\mathfrak{m}$.

Fourth: every non-zero ideal $\mathfrak{a}$ has inverse $\mathfrak{a}^{-1} = \{y \in k : y\mathfrak{a} \subset \mathfrak{o}\}$. If not, there is maximal $\mathfrak{a}$ *failing* this, and $\mathfrak{a}$ cannot be a maximal ideal, by the previous step. Thus, $\mathfrak{a}$ is *properly* contained in some maximal ideal $\mathfrak{m}$. Certainly $\mathfrak{a} \subset \mathfrak{m}^{-1}\mathfrak{a} \subset \mathfrak{a}^{-1}\mathfrak{a} \subset \mathfrak{o}$. Integral-closedness of $\mathfrak{o}$ and $\mathfrak{m}^{-1} \neq \mathfrak{o}$, $\mathfrak{m} \supset \mathfrak{o}$ show that $\mathfrak{m}^{-1}\mathfrak{a} \not\subset \mathfrak{a}$.

Thus, $\mathfrak{m}^{-1}\mathfrak{a}$ is strictly larger than $\mathfrak{a}$, so has an inverse $\mathfrak{f}$. Thus, $(\mathfrak{f}\mathfrak{m}^{-1}) \cdot \mathfrak{a} = \mathfrak{f} \cdot (\mathfrak{m}^{-1}\mathfrak{a}) = \mathfrak{o}$. That is, $\mathfrak{f}\mathfrak{m}^{-1}$ is an inverse for $\mathfrak{a}$, contradiction.

Fifth: ideals $\mathfrak{a}$ have *unique* inverses. For fractional ideal $\mathfrak{f}$ such that $\mathfrak{fa} = \mathfrak{o}$, certainly $\mathfrak{f} \subset \{y \in k : y\mathfrak{a} \subset \mathfrak{o}\}$. On the other hand, for $y\mathfrak{a} \subset \mathfrak{o}$, multiply by $\mathfrak{f}$ to obtain $y\mathfrak{af} \subset \mathfrak{f}$. Since $\mathfrak{af} = \mathfrak{o} \ni 1$, $y \in \mathfrak{f}$.

Sixth: every *fractional* ideal $\mathfrak{f}$ is uniquely *invertible*, and $\mathfrak{a} \subset \mathfrak{b}$ implies $\mathfrak{a}^{-1} \supset \mathfrak{b}^{-1}$. Let $0 \neq c \in \mathfrak{o}$ such that $c\mathfrak{f} \subset \mathfrak{o}$. Then $c\mathfrak{f}$ has unique inverse $\mathfrak{k}$, and $\mathfrak{f}$ has unique inverse $c^{-1}\mathfrak{k}$. For $\mathfrak{a} \subset \mathfrak{b}$, visibly $\{x \in k : x\mathfrak{a} \subset \mathfrak{o}\} \supset \{x \in k : x\mathfrak{b} \subset \mathfrak{o}\}$, so inversion is inclusion-reversing.

Seventh: every ideal $\mathfrak{a}$ is a product of prime ideals. If not, let $\mathfrak{a}$ be maximal among failures. It is not prime, so is properly contained in maximal $\mathfrak{m}$. Then $\mathfrak{a} \subset \mathfrak{m}$ gives $\mathfrak{m}^{-1}\mathfrak{a} \subset \mathfrak{o}$. Invertibility of fractional ideals gives $\mathfrak{m}^{-1}\mathfrak{a} \neq \mathfrak{o}$ and $\mathfrak{m}^{-1}\mathfrak{a} \neq \mathfrak{a}$. Thus, $\mathfrak{m}^{-1}\mathfrak{a}$ is a proper ideal strictly larger than $\mathfrak{a}$, and is a product of primes. Multiplication by $\mathfrak{m}$ expresses $\mathfrak{a}$ as a product, contradiction.

Eighth: for *fractional* ideals $\mathfrak{a}, \mathfrak{b}$, the **divisibility** property $\mathfrak{a}|\mathfrak{b}$, meaning there is an *ideal* $\mathfrak{c}$ such that $\mathfrak{c} \cdot \mathfrak{a} = \mathfrak{b}$, is equivalent to $\mathfrak{a} \supset \mathfrak{b}$. Indeed, on one hand, $\mathfrak{c} \subset \mathfrak{o}$ gives $\mathfrak{b} = \mathfrak{ca} \subset \mathfrak{oa} = \mathfrak{a}$. On the other hand, for $\mathfrak{a} \supset \mathfrak{b}$, since inversion is inclusion-reversing, $\mathfrak{a}^{-1} \subset \mathfrak{b}^{-1}$, so $\mathfrak{c} \subset \mathfrak{a}^{-1}\mathfrak{b} \subset \mathfrak{o}$.

Ninth: unique factorization of ideals into primes. The definition of prime ideal $\mathfrak{p}$ gives $\mathfrak{ab} \subset \mathfrak{p}$ only when $\mathfrak{a} \subset \mathfrak{p}$ or $\mathfrak{b} \subset \mathfrak{p}$, for ideals $\mathfrak{a}, \mathfrak{b}$. That is, $\mathfrak{p}|\mathfrak{ab}$ implies $\mathfrak{p}|\mathfrak{a}$ or $\mathfrak{p}|\mathfrak{b}$. Given two factorizations

$$\mathfrak{p}_1 \ldots \mathfrak{p}_m = \mathfrak{a} = \mathfrak{q}_1 \ldots \mathfrak{q}_n$$

$\mathfrak{p}_1$ must divide some $\mathfrak{q}_j$, thus, $\mathfrak{p}_1 = \mathfrak{q}_j$. Renumber so $\mathfrak{p}_1 = \mathfrak{q}_1$. Using *invertibility*, multiply by $\mathfrak{p}_1^{-1}$, obtaining $\mathfrak{p}_2 \ldots \mathfrak{p}_m = \mathfrak{q}_2 \ldots \mathfrak{q}_n$ and use induction.

Tenth: unique factorization of *fractional ideals*. Given fractional $\mathfrak{a}$, take $0 \neq c \in \mathfrak{o}$ such that $c\mathfrak{a} \subset \mathfrak{o} = \mathfrak{p}_1 \ldots \mathfrak{p}_m$. Let $c\mathfrak{o} = \mathfrak{q}_1 \ldots \mathfrak{q}_n$. Then

$$\mathfrak{a} = (\mathfrak{p}_1 \ldots \mathfrak{p}_m) \cdot (\mathfrak{q}_1 \ldots \mathfrak{q}_n)^{-1} = \frac{\mathfrak{p}_1 \ldots \mathfrak{p}_m}{\mathfrak{q}_1 \ldots \mathfrak{q}_n}$$

Cancel any common factors. ///

The **order** $\mathrm{ord}_{\mathfrak{p}}\mathfrak{a}$ at prime $\mathfrak{p}$ of a (non-zero) fractional ideal $\mathfrak{a}$ is the integer exponent of $\mathfrak{p}$ appearing in a factorization of $\mathfrak{a}$:

$$\mathfrak{a} \;=\; \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}\mathfrak{a}} \cdot (\text{primes distinct from } \mathfrak{p})$$

Similarly for $\alpha \in k^\times$, $\mathrm{ord}_{\mathfrak{p}}\alpha = \mathrm{ord}_{\mathfrak{p}}\alpha\mathfrak{o}$.

Elements or fractional ideals are **(locally) integral at $\mathfrak{p}$**, when their $\mathfrak{p}$-orders are non-negative. An element is a **$\mathfrak{p}$-unit** when its $\mathfrak{p}$-ord is 0.

[12.2] Corollary: For Dedekind $\mathfrak{o}$, an element $\alpha \in k$ is in $\mathfrak{o}$ if and only if it is $\mathfrak{p}$-integral everywhere locally. A fractional ideal $\mathfrak{f}$ is a genuine ideal if and only if it is $\mathfrak{p}$-integral everywhere locally.

Proof: Unique factorization: if $\mathfrak{f} = (\mathfrak{p}_1 \ldots \mathfrak{p}_m) \cdot (\mathfrak{q}_1 \ldots \mathfrak{q}_n)^{-1}$ is inside $\mathfrak{o}$, then $\mathfrak{p}_1 \ldots \mathfrak{p}_m \subset \mathfrak{q}_1 \ldots \mathfrak{q}_n$. ///

[12.3] Lemma: Localization $S^{-1}\mathfrak{o}$ is Dedekind. The primes of $S^{-1}\mathfrak{o}$ are $S^{-1}\mathfrak{p}$ for primes $\mathfrak{p}$ of $\mathfrak{o}$ not meeting S. Factorization of fractional ideals behaves like

$$S^{-1}\Big(\prod_{\mathfrak{p}} \mathfrak{p}^{e(\mathfrak{p})}\Big) \;=\; \prod_{\mathfrak{p}:\, \mathfrak{p}\cap S=\phi} (S^{-1}\mathfrak{p})^{e(\mathfrak{p})}$$

Proof: The integral domain property is preserved, because $S^{-1}\mathfrak{o}$ sits inside the field of fractions. Noetherianness is preserved: there are fewer ideals in $S^{-1}\mathfrak{o}$ than in $\mathfrak{o}$. Integral closedness: for $\alpha \in k$ integral over $S^{-1}\mathfrak{o}$, multiply out the denominators (from S) of the coefficients, obtaining an equation of the form

$$s\cdot\alpha^n + c_{n-1}\alpha^{n-1} + \ldots + c_1\alpha + c_o \;=\; 0 \qquad\qquad (\text{with } s \in S)$$

Thus,

$$(s\alpha)^n + (c_{n-1}s)\cdot(s\alpha)^{n-1} + \ldots + (c_1 s^{n-1})(s\alpha) + (s^n c_o) \;=\; 0$$

By integral closedness, $s\alpha \in \mathfrak{o}$, and $\alpha \in S^{-1}\mathfrak{o}$.

A prime $\mathfrak{p}$ meeting S becomes the whole ring $S^{-1}\mathfrak{o}$. For $\mathfrak{p}$ not meeting S, if $(x/s)(y/t) = z/u$ with $x, y \in \mathfrak{o}$, $z \in \mathfrak{p}$, and $s, t, u \in S$, then $u \cdot xy = st \cdot z$. Since $z \in \mathfrak{p}$ and $u \notin \mathfrak{p}$, $xy \in \mathfrak{p}$. Thus, $S^{-1}\mathfrak{p}$ is prime. Likewise, non-zero primes are *maximal*.

If $S^{-1}\mathfrak{p} = S^{-1}\mathfrak{q}$ for primes $\mathfrak{p}, \mathfrak{q}$, then $s\mathfrak{p} = \mathfrak{q}$ for some $s \in S \subset \mathfrak{o}$. Unique factorization of $s \cdot \mathfrak{o}$ shows $s \in \mathfrak{o}^\times$ and $\mathfrak{p} = \mathfrak{q}$.

Finally, with S containing 1 and closed under multiplication, $S^{-1}(\mathfrak{a}\mathfrak{b}) = (S^{-1}\mathfrak{a}) \cdot (S^{-1}\mathfrak{b})$ for all fractional ideals $\mathfrak{a}, \mathfrak{b}$, from the definition of the multiplication $\mathfrak{a} \cdot \mathfrak{b}$. This gives the factorization in the localization. ///

When we only care about finitely-many primes...:

[12.4] Proposition: Dedekind domains with finitely-many primes are PIDs.

Proof: Let the primes be $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$. Since $\mathfrak{p}_j^2 \neq \mathfrak{p}_j$, there is $\varpi_j \in \mathfrak{p}_j - \mathfrak{p}_j^2$. Given $\mathfrak{a} = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_n^{e_n}$, Sun-Ze's theorem gives a solution in $\mathfrak{o}$ of

$$x \;=\; \varpi_j^{e_j} \bmod \mathfrak{p}_j^{e_j+1} \qquad\qquad (\text{for } j = 1, \ldots, n)$$

The principal ideal $x\mathfrak{o}$ has a prime factorization, with the same exponents as $\mathfrak{a}$. ///

[12.5] Corollary: The localization of Dedekind $\mathfrak{o}$ at a prime $\mathfrak{p}$ is a PID, with unique prime $(\mathfrak{o} - \mathfrak{p})^{-1} \cdot \mathfrak{p}$. ///

[12.6] Corollary: For Dedekind $\mathfrak{o}$ in field of fractions k, the integral closure $\mathfrak{O}$ in a finite separable extension K/k is Dedekind.

Proof: Use the theorem characterizing Dedekind domains. $\mathfrak{O}$ is an integral domain and is integrally closed. By the Lying-Over theorem, primes $\mathfrak{P}$ in $\mathfrak{O}$ over non-zero, hence maximal, primes $\mathfrak{p}$ in $\mathfrak{o}$ are maximal.

Conversely, any prime $\mathfrak{P}$ of $\mathfrak{O}$ meets $\mathfrak{o}$ in a prime ideal $\mathfrak{p}$. As observed earlier, $\mathfrak{p}$ cannot be 0, because Galois norms from $\mathfrak{P}$ are in $\mathfrak{o} \cap \mathfrak{P}$ and are non-zero. Thus, $\mathfrak{p}$ is maximal, and by Lying-Over $\mathfrak{P}$ is maximal.

Noetherian-ness follows from the earlier result that $\mathfrak{O}$ is finitely-generated over $\mathfrak{o}$, using the non-degeneracy of the *trace pairing* corresponding to the finite separable extension K/k. ///

13. *Ramification, residue field extension degrees, e, f, g*

Prime $\mathfrak{p}$ in $\mathfrak{o}$ factors in an integral extension as $\mathfrak{p}\mathfrak{O} = \prod_{\mathfrak{P}} \mathfrak{P}^{e(\mathfrak{P}/\mathfrak{p})}$. The exponents $e(\mathfrak{P}/\mathfrak{p})$ are **ramification indices**.

The residue field extensions $\tilde{\kappa} = \mathfrak{O}/\mathfrak{P}$ over $\kappa = \mathfrak{o}/\mathfrak{p}$ have degrees $f(\mathfrak{P}/\mathfrak{p}) = [\tilde{\kappa} : \kappa]$.

[13.1] Theorem: For fixed $\mathfrak{p}$ in $\mathfrak{o}$,

$$\sum_{\mathfrak{P}|\mathfrak{p}} e(\mathfrak{P}/\mathfrak{p}) \cdot f(\mathfrak{P}/\mathfrak{p}) \quad = \quad [K : k]$$

For K/k Galois, the ramification indices e and residue field extension degrees f depend only on $\mathfrak{p}$ (and K/k), and in that case

$$e \cdot f \cdot (\text{number of primes } \mathfrak{P}|\mathfrak{p}) \quad = \quad [K : k]$$

Proof: We first treat the case that $\mathfrak{o}$ and $\mathfrak{O}$ are PIDs, and then reduce to this case by localizing. As usual, Sun-Ze's theorem gives

$$\mathfrak{O}/\mathfrak{p}\mathfrak{O} \quad \approx \quad \bigoplus_{\mathfrak{P}|\mathfrak{p}} \mathfrak{O}/\mathfrak{P}^{e(\mathfrak{P}/\mathfrak{p})}$$

For $\mathfrak{o}$ a PID, $\mathfrak{O}$ is a free $\mathfrak{o}$-module of rank $[K : k]$. Then $\mathfrak{O}/\mathfrak{p}\mathfrak{O}$ is a $\kappa = \mathfrak{o}/\mathfrak{p}$-vectorspace of dimension $[K : k]$. Each $\mathfrak{O}/\mathfrak{P}^e$ is a κ-vectorspace, and the sum of their dimensions is $[K : k]$. The κ-dimension of $\mathfrak{O}/\mathfrak{P}$ is $f(\mathfrak{P}/\mathfrak{p})$. The slightly more complicated $\mathfrak{O}/\mathfrak{P}^e$ require slightly more effort.

The chain of κ-vectorspaces

$$\{0\} = \mathfrak{P}^e/\mathfrak{P}^e \ \subset\ \mathfrak{P}^{e-1}/\mathfrak{P}^e \ \subset\ \ldots \ \subset\ \mathfrak{P}^2/\mathfrak{P}^e \ \subset\ \mathfrak{P}/\mathfrak{P}^e \ \subset\ \mathfrak{O}/\mathfrak{P}^e$$

has consecutive quotients

$$\big(\mathfrak{P}^i/\mathfrak{P}^e\big)/\big(\mathfrak{P}^{i+1}/\mathfrak{P}^e\big) \quad \approx \quad \mathfrak{P}^i/\mathfrak{P}^{i+1}$$

Using the fact that $\mathfrak{O}$ is a PID, let ϖ generate $\mathfrak{P}$. Visibly, $\mathfrak{P}^{i+1}/\mathfrak{P}^i \approx \mathfrak{O}/\mathfrak{P}$ by the map

$$x + \mathfrak{O}\varpi \quad \longrightarrow \quad \varpi^i x + \mathfrak{O}\varpi^{i+1} \qquad\qquad (\text{multiplication by } \varpi^i)$$

In general, for a chain $\{0\} = V_o \subset V_1 \subset \ldots \subset V_{e-1} \subset V_e$ of finite-dimensional vectorspaces, we have

$$\dim V_e \ = \ \dim(V_1/V_o) + \dim(V_2/V_1) + \ldots + \dim(V_e/V_{e-1})$$

In the case at hand, the dimensions of the consecutive quotients are all $f(\mathfrak{P}/\mathfrak{p})$, so

$$\dim_\kappa \mathfrak{O}/\mathfrak{P}^e \quad = \quad e(\mathfrak{P}/\mathfrak{p}) \cdot f(\mathfrak{P}/\mathfrak{p})$$

and $[K:k] = \sum_{\mathfrak{P}|\mathfrak{p}} e(\mathfrak{P}/\mathfrak{p}) \cdot f(\mathfrak{P}/\mathfrak{p})$. The transitivity of Galois on $\mathfrak{P}|\mathfrak{p}$ gives equality among the e, fs in the Galois case.

Now reduce to the case that $\mathfrak{o}$ is a PID, by *localizing* at $\mathfrak{p}$, thus leaving a single prime. We must show that localizing at $S = \mathfrak{o} - \mathfrak{p}$ does not change the e, fs.

A factorization $\mathfrak{p}\mathfrak{O} = \prod_{\mathfrak{P}} \mathfrak{P}^{e(\mathfrak{P}/\mathfrak{p})}$ gives a corresponding

$$(S^{-1}\mathfrak{p})(S^{-1}\mathfrak{O}) = \prod_{\mathfrak{P}} (S^{-1}\mathfrak{P})^{e(\mathfrak{P}/\mathfrak{p})}$$

The primes of $\mathfrak{O}$ surviving to $S^{-1}\mathfrak{O}$ are exactly those lying over $\mathfrak{p}$, seen as follows. For $\mathfrak{P}$ to lie over $\mathfrak{p}$ means that $\mathfrak{P} \cap \mathfrak{o} = \mathfrak{p}$. Since $S \subset \mathfrak{o}$, and $\mathfrak{p} \cap S = \phi$, $\mathfrak{P} \cap S = \phi$ for $\mathfrak{P}$ lying over $\mathfrak{p}$. For all other $\mathfrak{P}$, $\mathfrak{P} \cap \mathfrak{o}$ is a prime ideal $\mathfrak{q} \neq \mathfrak{p}$ of $\mathfrak{o}$. Taking Galois norms shows that $\mathfrak{q} \neq \{0\}$, so $S \cap \mathfrak{q} \neq \phi$, and $S^{-1}\mathfrak{P} = \mathfrak{O}$.

Thus, the ramification indices $e(\mathfrak{P}/\mathfrak{p})$ are unchanged by localizing. Next, show that the residue field extension degrees are unchanged by localization. First, *claim/recall* that $\mathfrak{o}/\mathfrak{p} \approx S^{-1}\mathfrak{o}/S^{-1}\mathfrak{p}$. Indeed, $\mathfrak{o} \to S^{-1}\mathfrak{o} \to S^{-1}\mathfrak{o}/S^{-1}\mathfrak{p}$ has kernel $\mathfrak{o} \cap S^{-1}\mathfrak{p}$. For $sx \in \mathfrak{p}$ with $s \in S$ and $x \in \mathfrak{o}$, then $x \in \mathfrak{p}$ by primality of $\mathfrak{p}$ and $S \cap \mathfrak{p} = \phi$. This gives injectivity.

For surjectivity, given $\frac{x}{s} + S^{-1}\mathfrak{p}$, find $y \in \mathfrak{o}$ such that $y - \frac{x}{s} \in S^{-1}\mathfrak{p}$. It suffices to have $sy - x \in \mathfrak{p}$. Since $\mathfrak{p}$ is maximal, $s\mathfrak{o} + \mathfrak{p} = \mathfrak{o}$, so there is $z \in \mathfrak{o}$ such that $sz - 1 \in \mathfrak{p}$. Multiplying through by x gives $(xz)s - x \in x\mathfrak{p} \subset \mathfrak{p}$, proving surjectivity.

Similarly, *claim* that $\mathfrak{O}/\mathfrak{P} \approx S^{-1}\mathfrak{O}/S^{-1}\mathfrak{P}$ for $\mathfrak{P}|\mathfrak{p}$. The kernel of

$$\mathfrak{O} \longrightarrow S^{-1}\mathfrak{O} \longrightarrow S^{-1}\mathfrak{O}/S^{-1}\mathfrak{P}$$

is $\mathfrak{O} \cap S^{-1}\mathfrak{P}$. For $sx \in \mathfrak{P}$ with $x \in \mathfrak{O}$ and $s \in S$, then either $s \in \mathfrak{P}$ or $x \in \mathfrak{P}$. Since $\mathfrak{P} \cap \mathfrak{o} = \mathfrak{p}$ and $S \subset \mathfrak{o}$, $\mathfrak{P} \cap S = \phi$. Thus, $x \in \mathfrak{P}$, and $\mathfrak{O}/\mathfrak{P} \to S^{-1}\mathfrak{O}/S^{-1}\mathfrak{P}$ is *injective.*

For surjectivity, given $\frac{x}{s} + S^{-1}\mathfrak{P}$, find $y \in \mathfrak{O}$ such that $y - \frac{x}{s} \in S^{-1}\mathfrak{P}$. It suffices to have $sy - x \in \mathfrak{P}$. Since $\mathfrak{p}$ is maximal, $s\mathfrak{o} + \mathfrak{p} = \mathfrak{o}$, so there is $z \in \mathfrak{o}$ such that $sz - 1 \in \mathfrak{p} \subset \mathfrak{P}$. Multiplying through by x gives $(xz)s - x \in x\mathfrak{P} \subset \mathfrak{P}$, proving surjectivity.

Thus, we can localize at $S = \mathfrak{o} - \mathfrak{p}$ without changing the e, fs, thereby assuming without loss of generality that $\mathfrak{o}$ and $\mathfrak{O}$ are PIDs, being Dedekind with finitely-many primes. ///

Proposition: The e, f's are *multiplicative in towers*, that is, for separable extensions $k \subset E \subset K$ and corresponding primes $\mathfrak{p} \subset \mathfrak{q} \subset \mathfrak{P}$,

$$e(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{q}/\mathfrak{p}) \cdot e(\mathfrak{P}/\mathfrak{q}) \qquad f(\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{q}/\mathfrak{p}) \cdot f(\mathfrak{P}/\mathfrak{q})$$

Proof: This follows from the ideas of the previous proof, together with the fact from field theory that for fields $\kappa \subset \kappa' \subset \tilde{\kappa}$, $\dim_\kappa \tilde{\kappa} = \dim_\kappa \kappa' \cdot \dim_{\kappa'} \tilde{\kappa}$ ///

[13.2] Remark: The incidental fact that localization at $\mathfrak{p}$ does not alter the $e(\mathfrak{P}/\mathfrak{p})$s and $f(\mathfrak{P}/\mathfrak{p})$'s for $\mathfrak{P}|\mathfrak{p}$ will be re-used on several later occasions. For example:

Proposition: For $\alpha \neq 0$ in the integral closure $\mathfrak{O}$ of $\mathbb{Z}$ in a number field K, the Galois norm and ideal norm are essentially the same:

$$|N_{\mathbb{Q}}^K(\alpha)| = N(\alpha\mathfrak{O})$$

with *ideal* norm $N(\mathfrak{A}) = \#\mathfrak{O}/\mathfrak{A}$ for ideals $\mathfrak{A}$ in $\mathfrak{O}$.

A stronger assertion has a simpler proof. To set it up, define a variant notion of *ideal* norm N_k^K from fractional ideals of $\mathfrak{O}$ to fractional ideals of $\mathfrak{o}$, first on primes $\mathfrak{P}$ of $\mathfrak{O}$, by

$$\text{(ideal-norm)}\, N_k^K \mathfrak{P} = \mathfrak{p}^{f(\mathfrak{P}/\mathfrak{p})} \qquad \text{(for } \mathfrak{P}|\mathfrak{p})$$

and extend this to the group of fractional ideals by multiplicativity:

$$\text{(ideal-norm)}\, N_k^K\Big(\prod_{\mathfrak{P}} \mathfrak{P}^{\ell_{\mathfrak{P}}}\Big) \;=\; \prod_{\mathfrak{P}} (N_k^K \mathfrak{P})^{\ell_{\mathfrak{P}}}$$

Proposition: With $\mathfrak{o} \subset k$ and $\mathfrak{O} \subset K$ as usual, for $0 \neq \alpha \in \mathfrak{O}$,

$$\text{(ideal-norm)}\, N_k^K(\alpha\mathfrak{O}) \;=\; \mathfrak{o} \cdot \text{(Galois norm)}\, N_k^K(\alpha)$$

Proof: Without loss of generality, we can take K/k Galois, since extending to the Galois closure E of K over k has the effect of raising everything to the $[E:K]$ power. With $G = \mathrm{Gal}(K/k)$,

$$\prod_{\sigma \in G} \sigma\mathfrak{P} \;=\; \prod_{\sigma \in G/G_{\mathfrak{P}}} (\sigma\mathfrak{P})^{ef} \;=\; \Big(\prod_{\mathfrak{P}_i | \mathfrak{p}} \mathfrak{P}_i^e\Big)^f \;=\; \mathfrak{p}^f \cdot \mathfrak{O}$$

Thus, for an ideal $\mathfrak{A}$ of $\mathfrak{O}$, $\prod_{\sigma\in G}\; \sigma\mathfrak{A} \;=\; \text{(ideal-norm)}\, N_k^K \mathfrak{A} \cdot \mathfrak{O}$

On the other hand,

$$\prod_{\sigma \in G} \sigma(\alpha\mathfrak{O}) \;=\; \Big(\prod_{\sigma \in G} \sigma(\alpha)\Big) \cdot \mathfrak{O} \;=\; \text{(Galois-norm)}\, N_k^K(\alpha) \cdot \mathfrak{O}$$

Combining these,

$$\text{(ideal-norm)}\; N_k^K(\alpha\mathfrak{O}) \cdot \mathfrak{O} \;=\; \text{(Galois-norm)}\; N_k^K(\alpha) \cdot \mathfrak{O}$$

The ideal norm $N_k^K(\alpha\mathfrak{O})$ is in $\mathfrak{o}$, by definition, and $N_k^K(\alpha)$ is in $\mathfrak{o}$. Unique factorization into prime ideals in $\mathfrak{O}$ proves

$$\text{(ideal-norm)}\; N_k^K(\alpha\mathfrak{O}) \cdot \mathfrak{o} \;=\; \text{(Galois-norm)}\; N_k^K(\alpha) \cdot \mathfrak{o}$$

as claimed. ///

Equality of ideal and Galois norms eliminates ambiguities in comparing the following general definition to simpler instances.

Now $\mathfrak{o}$ must have *finite residue fields*. It suffices that its field of fractions k is either a finite extension of $\mathbb{Q}$ or of $\mathbb{F}_q(x)$.

And revert to using the *ideal norm* unadorned N to refer to the ideal norm $N\mathfrak{a} = \#\mathfrak{o}/\mathfrak{a}$.

14. *Finiteness of ramification*

[14.1] Theorem: Only finitely many primes *ramify* in the integral closure $\mathfrak{O}$ of a Dedekind domain $\mathfrak{o}$ in a finite separable extension K/k of the field of fractions k of $\mathfrak{o}$.

In fact, we will prove more.

The *inverse different* $\mathfrak{d}^{-1} = \mathfrak{d}^{-1}_{\mathfrak{O}/\mathfrak{o}}$ of $\mathfrak{O}/\mathfrak{o}$ is

$$\mathfrak{d}^{-1} \;=\; \mathfrak{d}^{-1}_{\mathfrak{O}/\mathfrak{o}} \;=\; \{x \in K \;:\; \mathrm{tr}_k^K(x\mathfrak{O}) \subset \mathfrak{o}\}$$

[14.2] Proposition: The inverse different is a fractional ideal of $\mathfrak{O}$ containing $\mathfrak{O}$.

Proof: Since $\mathrm{tr}_k^K(\mathfrak{O}) \subset \mathfrak{o}$, certainly $\mathfrak{O} \subset \mathfrak{d}^{-1}$.

Given a k-basis x_i of K, we can adjust by a non-zero constant in k so that all x_i are in $\mathfrak{O}$. Let $\widehat{x}_i$ be the dual basis with respect to the trace pairing, which by separability is non-degenerate.

Since $\sum_i \mathfrak{o}x_i \subset \mathfrak{O}$, certainly $\mathfrak{d}^{-1} \subset \sum_i \mathfrak{o}\widehat{x}_i$, a finitely-generated $\mathfrak{o}$-module inside K. Since $\mathfrak{o}$ is *Noetherian*, every submodule of a finitely-generated $\mathfrak{o}$-module is finitely-generated, so $\mathfrak{d}^{-1}$ is finitely-generated as an $\mathfrak{o}$-module. Thus, it is certainly finitely-generated as an $\mathfrak{O}$-module, so is a fractional ideal. Since $\mathfrak{d}^{-1} \supset \mathfrak{O}$, its inverse is contained in $\mathfrak{O}$. ///

Given the proposition, it makes sense to define the *different* $\mathfrak{d}_{\mathfrak{O}/\mathfrak{o}}$ to be the fractional-ideal inverse of $\mathfrak{d}^{-1}_{\mathfrak{O}/\mathfrak{o}}$. When the Dedekind rings $\mathfrak{o} \subset k$ and $\mathfrak{O} \subset K$ are understood, write

$$\mathfrak{d}_{K/k} \;=\; \mathfrak{d}_{\mathfrak{O}/\mathfrak{o}}$$

[14.3] Proposition: In a finite separable extension K/k with respective rings of integers $\mathfrak{O}$ and $\mathfrak{o}$, for $\mathfrak{p} \cdot \mathfrak{O} = \mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_n^{e_n}$, each $\mathfrak{P}_i^{e_i - 1}$ divides $\mathfrak{d}_{K/k}$.

Proof: Compute directly

$$\mathrm{tr}_k^K(\mathfrak{P}_1^{1-e_1} \cdot \mathfrak{O}) \;=\; \mathrm{tr}_k^K(\mathfrak{P}_1^{1-e_1}) \;=\; \mathfrak{p}^{-1}\mathfrak{p} \cdot \mathrm{tr}_k^K(\mathfrak{P}_1^{1-e_1}) \;=\; \mathfrak{p}^{-1}\mathrm{tr}_k^K(\mathfrak{p}\mathfrak{P}_1^{1-e_1}) \;=\; \mathfrak{p}^{-1}\mathrm{tr}_k^K(\mathfrak{P}_1\mathfrak{P}_2^{e_2} \ldots \mathfrak{P}_n^{e_n})$$

$$\subset\; \mathfrak{p}^{-1}\mathrm{tr}_k^K(\mathfrak{P}_1\mathfrak{P}_2 \ldots \mathfrak{P}_n) \;\subset\; \mathfrak{p}^{-1} \cdot (\mathfrak{P}_1\mathfrak{P}_2 \ldots \mathfrak{P}_n \cap \mathfrak{o}_k) \;\subset\; \mathfrak{p}^{-1} \cdot \mathfrak{p} \;=\; \mathfrak{o}$$

Thus, $\mathfrak{P}_1^{1-e_1} \subset \mathfrak{d}^{-1}_{K/k}$, which is equivalent to $\mathfrak{d}_{K/k} \subset \mathfrak{P}_1^{e-1}$, so $\mathfrak{P}_1^{e-1}|\mathfrak{d}_{K/k}$. ///

As a corollary, we have the theorem: only finitely-many primes $\mathfrak{p}$ in $\mathfrak{o}$ ramify in $\mathfrak{O}/\mathfrak{o}$ for finite separable K/k.

15. *Dedekind zeta functions*

Even though the subscript should make a reference to the ring $\mathfrak{o}$ rather than k, the ring $\mathfrak{o}$ is essentially implied by specifying the field k. (This is not quite true for functions fields, but never mind.)

$$\zeta_k(s) \;=\; \sum_{0 \neq \mathfrak{a} \subset \mathfrak{o}} \frac{1}{N\mathfrak{a}^s}$$

The Dedekind property and the same analysis as for $\mathbb{Z}$ suggests (convergence?!) the Euler product

$$\zeta_k(s) \;=\; \sum_{0 \neq \mathfrak{a} \subset \mathfrak{o}} \frac{1}{N\mathfrak{a}^s} \;=\; \prod_{\mathfrak{p} \text{ prime in } \mathfrak{o}} \frac{1}{1 - N\mathfrak{p}^{-s}}$$

Understanding splitting/factorization of primes in extensions of $\mathbb{Z}$ or of $\mathbb{F}_q[x]$ gives

Proposition: The Euler product expression for $\zeta_k(s)$ is absolutely convergent for $\mathrm{Re}(s) > 1$.

Proof: Treat the number field case. Group the Euler factors according to the associated rational primes.

The picture:

$$\begin{tikzcd}
k \arrow[r, dash, "\supset"] \arrow[dd, dash] & \mathfrak{o} \arrow[r, dash, "\supset"] \arrow[dd, dash] \arrow[rrd] & \mathfrak{p} \arrow[dd, dash] & \\
& & & \mathfrak{o}/\mathfrak{p} = \tilde{\kappa} \arrow[dd, dash, "f(\mathfrak{p}/p)"] \\
\mathbb{Q} \arrow[r, dash, "\supset"] & \mathbb{Z} \arrow[r, dash, "\supset"] \arrow[rrd] & p & \\
& & & Z/p = \mathbb{F}_p
\end{tikzcd}$$

With $p\mathfrak{o} = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_g^{e_g}$ with residue field extension degrees f_i, and $\sum_i e_i f_i = [k:\mathbb{Q}]$, with $\sigma = \mathrm{Re}(s)$,

$$\Big|\frac{1}{1 - N\mathfrak{p}^{-s}}\Big| \;=\; \frac{1}{1-p^{-f\sigma}} \;\le\; \Big(\frac{1}{1-p^{-\sigma}}\Big)^f$$

Thus,

$$\Big|\prod_{\mathfrak{p}|p} \frac{1}{1 - N\mathfrak{p}^{-s}}\Big| \;\le\; \Big(\frac{1}{1-p^{-\sigma}}\Big)^{[k:\mathbb{Q}]}$$

and the Euler product for $\zeta_k(s)$ is dominated by the Euler product for $\zeta_{\mathbb{Q}}(\sigma)^{[k:\mathbb{Q}]}$, nicely convergent for $\mathrm{Re}(s) > 1$. ///

The estimate

$$|\zeta_k(s)| \;\le\; \zeta_{\mathbb{Q}}(\sigma)^{[k:\mathbb{Q}]} \qquad\qquad (\sigma = \mathrm{Re}(s) > 1)$$

is bad. It suggests that the meromorphically continued $\zeta_k(s)$ has a pole of order $[k:\mathbb{Q}]$ at $s = 1$. In reality, this pole is of order 1, but this is non-trivial to prove. It is related to *finiteness of class number* $h(\mathfrak{o})$ (order of ideal class group), and *Dirichlet's Units Theorem* (the units group $\mathfrak{o}^\times$ is as large as possible).

Thus, the expected sum over principal ideals

$$Z_{[\mathfrak{o}]}(s) \;=\; \sum_{0\neq\alpha\,\in\,\mathfrak{o}/\mathfrak{o}^\times} \frac{1}{N(\alpha\mathfrak{o})^s} \;=\; \sum_{0\neq\alpha\,\in\,\mathfrak{o}/\mathfrak{o}^\times} \frac{1}{|N^k_{\mathbb{Q}}(\alpha)|^s}$$

is only a *partial zeta function*, because it is only *part* of $\zeta_k(s)$. For any ideal class $[\mathfrak{b}]$, the corresponding partial zeta function is

$$Z_{[\mathfrak{b}]}(s) \;=\; \sum_{0\neq\mathfrak{a}\subset\mathfrak{o},\ \mathfrak{a}\in[\mathfrak{b}]} \frac{1}{N\mathfrak{a}^s}$$

and

$$\zeta_k(s) \;=\; \sum_{\text{classes }[\mathfrak{b}]} Z_{[\mathfrak{b}]}(s)$$

The partial zetas can be rewritten as sums over field elements, as follows. Given ideal class $[\mathfrak{b}]$, to say $\mathfrak{a} \in [\mathfrak{b}]$ is to say $\mathfrak{a} = \alpha\cdot\mathfrak{b}$ for some $\alpha \in k^\times$. That $\mathfrak{a} \subset \mathfrak{o}$ is $\alpha\mathfrak{b} \subset \mathfrak{o}$, or $\alpha \in \mathfrak{b}^{-1}$.

Also, $N(\alpha\mathfrak{b}) = |N^k_{\mathbb{Q}}(\alpha)| \cdot N\mathfrak{b}$, so the subsum over ideals $[\mathfrak{b}]$ is

$$Z_{[\mathfrak{b}]}(s) \;=\; \sum_{0\neq\alpha\,\in\,\mathfrak{b}^{-1}/\mathfrak{o}^\times} \frac{1}{(|N^k_{\mathbb{Q}}\alpha| \cdot N\mathfrak{b})^s} \;=\; \frac{1}{N\mathfrak{b}^s} \sum_{0\neq\alpha\,\in\,\mathfrak{b}^{-1}/\mathfrak{o}^\times} \frac{1}{|N^k_{\mathbb{Q}}\alpha|^s}$$

The units group $\mathfrak{o}^\times$ is finite for *complex quadratic fields* $k = \mathbb{Q}(\sqrt{-D})$ for $D > 0$ [and *only* in that case and for $k = \mathbb{Q}$ itself, by Dirichlet's Units Theorem, below...]. With $|\mathfrak{o}^\times| < \infty$,

$$Z_{[\mathfrak{b}]}(s) \;=\; \frac{1}{N\mathfrak{b}^s}\frac{1}{|\mathfrak{o}^\times|}\sum_{0\neq\alpha\,\in\,\mathfrak{b}^{-1}} \frac{1}{|N^k_{\mathbb{Q}}\alpha|^s}$$

We will obtain a formula for the class number $h(\mathfrak{o})$ of $\mathfrak{o}$ for complex quadratic fields. In particular, this proves finiteness in that case.

For $k = \mathbb{Q}(\sqrt{-D})$ for $D > 0$, the ring of algebraic integers $\mathfrak{o}$ is either $\mathbb{Z}[\sqrt{-D}]$ or $\mathbb{Z}[\frac{1+\sqrt{-D}}{2}]$, depending whether $-D = 2, 3 \bmod 4$, or $-D = 1 \bmod 4$.

More to the point, *qualitatively* $\mathfrak{o}$ is a free $\mathbb{Z}$-module of rank 2, and is a *lattice* in $\mathbb{C}$, in the sense that $\mathfrak{o}$ is a *discrete* subgroup of $\mathbb{C}$, and $\mathbb{C}/\mathfrak{o}$ is *compact*.

For *any* complex quadratic field, the *Galois* norm is the *complex* norm squared, because the non-trivial Galois automorphism is the restriction of complex conjugation:

$$N^k_{\mathbb{Q}}(\alpha) \;=\; \alpha\cdot\bar{\alpha} \;=\; |\alpha|^2 \qquad\qquad \text{(for complex quadratic } k\text{)}$$

Thus, in particular, as we know well, in this situation $N^k_{\mathbb{Q}}(\alpha)$ is the square of the distance of α from 0.

[15.1] Lemma: For a lattice Λ in $\mathbb{C}$, the associated Epstein zeta function

$$Z_\Lambda(s) \;=\; \sum_{0\neq\lambda\in\Lambda} \frac{1}{|\lambda|^{2s}}$$

has a meromorphic continuation to $\mathrm{Re}(s) > 1-\varepsilon$ for small $\varepsilon > 0$, and

$$Z_\Lambda(s) \;=\; \frac{\pi}{\text{co-area}\,\Lambda}\cdot\frac{1}{s-1} \;+\; \text{(holomorphic near } s=1)$$

where *co-area* is intended to be the natural area of the quotient $\mathbb{C}/\Lambda$, or the inverse of the *density* of Λ. Formulaically,

$$\text{(co-area) }\Lambda \;=\; |\det\begin{pmatrix} x_1 & y_1 \\ x_2 & y_2\end{pmatrix}|$$

for $\mathbb{Z}$-basis $\lambda_1 = x_1 + iy_1$, $\lambda_2 = x_2 + iy_2$ of Λ. Equivalently,

$$\begin{aligned}\text{(co-area) }\Lambda \;&=\; \text{area of fundamental parallelogram for }\Lambda\\ &=\; \text{area of parallelogram with vertices } 0,\,\lambda_1,\,\lambda_2,\,\lambda_1+\lambda_2\end{aligned}$$

Proof: This is a slight sharpening of a higher-dimensional *integral test* applied to this situation. Part of the idea is that for some (or *any*) r_o

$$\sum_{0\neq\lambda\in\Lambda}\frac{1}{|\lambda|^{2s}} \;\sim\; \int_{|z|\geq r_o}\frac{(\text{density of }\Lambda)}{|z|^{2s}}\,dx\,dy \;=\; 2\pi\int_{r_o}^\infty \frac{(\text{density of }\Lambda)}{r^{2s}}\,r\,dr \;=\; \frac{2\pi(\text{density of }\Lambda)}{2(s-1)}\cdot r_o^{2-2s}$$

$$=\; \frac{\pi}{\text{co-area }\Lambda}\cdot\frac{1}{s-1}\cdot r_o^{2-2s} \;=\; \frac{\pi}{\text{co-area }\Lambda}\cdot\frac{1}{s-1} \;+\; \text{(holo near } s=1)$$

This correctly suggests the blow-up at $s = 1$ and the dependence on the co-area of Λ.

A small amount of care clarifies this, as a very easy example of a line of reasoning brought to classical perfection by Minkowski *circa* 1900.

Let $\nu(r) = \#\{0 \neq \lambda \in \Lambda : |\lambda| \le r\}$ be the number of lattice points inside a circle of radius r.

[15.2] Claim:

$$\nu(r) \;=\; \frac{\pi r^2}{\text{co-area } \Lambda} + O(r)$$

where $O(r)$ denotes a function bounded by some constant multiple of r as $r \to \infty$.

Proof: Let F be any fundamental parallelogram for Λ with one vertex at 0. Let d be the diameter of F. Let B_r be the ball in $\mathbb{C}$ of radius r centered at 0.

For $|\lambda| \le r$, $\lambda + F \subset B_{r+d}$, so the number of lattice points inside B_r is bounded by the number of (disjoint!) copies of F inside B_{r+d}. Comparing areas,

$$\nu(r) \;\le\; \frac{\text{area } B_{r+d}}{\text{area } F} \;=\; \frac{\pi(r+d)^2}{\text{area } F} \;=\; \frac{\pi(r+d)^2}{\text{co-area } \Lambda}$$

On the other hand, for $\lambda + F \subset B_r$, certainly $\lambda \in B_r$. The smaller B_{r-d} is entirely covered by $\lambda + F$'s fitting inside B_r, so

$$\nu(r) \;\ge\; \frac{\text{area } B_{r-d}}{\text{area } F} \;=\; \frac{\pi(r-d)^2}{\text{co-area } \Lambda}$$

Together,

$$\frac{\pi(r-d)^2}{\text{co-area } \Lambda} \;\le\; \nu(r) \;\le\; \frac{\pi(r+d)^2}{\text{co-area } \Lambda}$$

which proves the claim that $\nu(r) = \pi r^2/\text{co-area}(\Lambda) + O(r)$. ///

Using Riemann-Stieljes integrals and integration by parts,

$$\sum_{0 \neq \lambda \in \Lambda} \frac{1}{|\lambda|^{2s}} \;=\; \int_{r_o}^{\infty} \frac{1}{r^{2s}}\, d\nu(r) \;=\; 2s \int_{r_o}^{\infty} \nu(r)\, \frac{dr}{r^{2s+1}}$$

And

$$2s \int_{r_o}^{\infty} \nu(r)\, \frac{dr}{r^{2s+1}} \;=\; 2s \int_{r_o}^{\infty} \frac{\pi r^2}{\text{co-area } \Lambda}\, \frac{dr}{r^{2s+1}} + 2s \int_{r_o}^{\infty} O(r)\, \frac{dr}{r^{2s+1}}$$

The second summand is holomorphic for $\text{Re}(2s) > 1$, and the first is

$$2s \frac{\pi}{\text{co-area } \Lambda} \cdot \int_{r_o}^{\infty} \frac{dr}{r^{2s-1}} \;=\; \frac{s\pi}{\text{co-area } \Lambda} \cdot \frac{1}{s-1}$$

The residue at $s = 1$ is $\pi/\text{co-area}(\Lambda)$. ///

That is, again, the Epstein zeta function $Z_\Lambda(s)$ attached to a lattice Λ is meromorphic on $\text{Re}(s) > \frac{1}{2}$, with simple pole at $s = 1$ with residue $\pi/\text{co-area}(\Lambda)$.

[15.3] Corollary:

For complex quadratic k, assuming $h(\mathfrak{o}) < \infty$,

$$\zeta_k(s) \;=\; \sum_{[\mathfrak{b}]} \sum_{\mathfrak{a} \sim \mathfrak{b}} \frac{1}{N\mathfrak{a}^s} \;\sim\; \frac{\pi \cdot h(\mathfrak{o})}{|\mathfrak{o}^\times| \cdot \text{co-area}(\mathfrak{o})} + (\text{holo at } s = 1)$$

Proof: As observed earlier,

$$\zeta_k(s) \;=\; \sum_{[\mathfrak{b}]} \frac{1}{N\mathfrak{b}^s} \frac{1}{|\mathfrak{o}^\times|} \sum_{0 \neq \alpha \in \mathfrak{b}^{-1}} \frac{1}{N\alpha^s} \;=\; \sum_{[\mathfrak{b}]} \frac{1}{N\mathfrak{b}^s} \cdot Z_{\mathfrak{b}^{-1}}(s)$$

By the lemma, this will have residue

$$\mathrm{Res}_{s=1}\zeta_k(s) \;=\; \sum_{[\mathfrak{b}]} \frac{1}{N\mathfrak{b}} \cdot \frac{\pi}{|\mathfrak{o}^\times| \cdot \text{co-area } \mathfrak{b}^{-1}}$$

The co-area of $\mathfrak{b}^{-1}$ is determined as follows. Observe that for an ideal $\mathfrak{a}$

$$N\mathfrak{a} \;=\; [\mathfrak{o} : \mathfrak{a}] \;=\; \frac{\text{area } \mathbb{C}/\mathfrak{a}}{\text{area } \mathbb{C}/\mathfrak{o}} \;=\; \frac{\text{co-area } \mathfrak{a}}{\text{co-area } \mathfrak{o}}$$

By multiplicativity, the co-area of $\mathfrak{b}^{-1}$ is $N(\mathfrak{b}^{-1}) = (N\mathfrak{b})^{-1}$. That is, the $\mathfrak{b}^{th}$ summand in the residue does not depend on $\mathfrak{b}$, and we have the assertion. ///

[15.4] Corollary: With $\chi(p) = (-D/p)_2$,

$$\frac{\pi \cdot h(\mathfrak{o})}{|\mathfrak{o}^\times| \cdot \text{co-area } \mathfrak{o}} \;=\; L(1,\chi)$$

Proof: Recall (!?!) the *factorization*

$$\zeta_k(s) \;=\; \zeta_{\mathbb{Q}}(s) \cdot L(s,\chi)$$

Since $\zeta(s) = \zeta_{\mathbb{Q}}(s)$ has residue 1 at $s = 1$, the value $L(1,\chi)$ is the residue of $\zeta_k(s)$ at $s = 1$. ///

[15.5] Remark: For complex quadratic k, all the units are roots of unity, and the number of roots of unity is often denoted w. Thus, rewriting,

$$\frac{\pi \cdot h}{w \cdot \text{coarea}(\mathfrak{o})} \;=\; L(1,\chi)$$

In particular, not only is $L(1,\chi) \neq 0$, it is *positive*. Further, for complex quadratic k, the special value $L(1,\chi)$ has a finite, closed-form expression. Let N be the conductor of χ. From the Fourier expansion of the sawtooth function

$$x - \tfrac{1}{2} \;=\; \frac{-1}{2\pi i} \sum_{n\neq 0} \frac{e^{2\pi i n x}}{n}$$

$$\sum_{a \bmod N} \big(\frac{a}{N} - \tfrac{1}{2}\big) \cdot \chi(a) \;=\; \frac{-1}{2\pi i} \sum_{n\neq 0} \frac{1}{n} \sum_a \chi(a) e^{2\pi i n a/N} \;=\; \frac{-1}{2\pi i} \sum_{n\neq 0} \frac{\chi(n)}{n} \cdot \sum_a \chi(a) e^{2\pi i a/N}$$

by replacing a by an^{-1} mod N. Since $\chi(-1) = -1$ (!!!)

$$\sum_{a \bmod N} \big(\frac{a}{N} - \tfrac{1}{2}\big) \cdot \chi(a) \;=\; \frac{-1}{\pi i} \cdot L(1,\chi) \cdot \sum_a \chi(a) e^{2\pi i a/N}$$

Thus,

$$L(1,\chi) \;=\; \frac{-\pi i}{\sum_a \chi(a) e^{2\pi i a/N}} \sum_{a \bmod N} \big(\frac{a}{N} - \tfrac{1}{2}\big) \cdot \chi(a)$$

Thus,

$$\frac{\pi \cdot h(\mathfrak{o})}{w \cdot \text{coarea}(\mathfrak{o})} \;=\; \frac{-\pi i}{\sum_a \chi(a) e^{2\pi i a/N}} \sum_{a \bmod N} \big(\frac{a}{N} - \tfrac{1}{2}\big) \cdot \chi(a)$$

and

$$h(\mathfrak{o}) \;=\; \frac{-iw \cdot \text{coarea}(\mathfrak{o})}{\sum_a \chi(a) e^{2\pi i a/N}} \sum_{a \bmod N} \big(\frac{a}{N} - \tfrac{1}{2}\big) \cdot \chi(a)$$

Again, this is for *complex quadratic* fields. ///

The simplest family of rings of algebraic integers that are typically *not* PIDs, but with the simple feature of *finitely-many units*, is *complex quadratic* $k = \mathbb{Q}(\sqrt{-D})$ for $D > 0$. Let the ring of algebraic integers be $\mathfrak{o}$, quadratic symbol $\chi(p)$=$(-D/p)_2$, N the conductor of χ, $h(\mathfrak{o})$ the *class number*. Then

$$h(\mathfrak{o}) \;=\; \frac{-i\cdot|\mathfrak{o}^\times|\cdot \mathrm{coarea}(\mathfrak{o})}{\sum_a \chi(a)e^{2\pi i a/N}} \sum_{a \bmod N} \big(\frac{a}{N}-\tfrac{1}{2}\big)\cdot\chi(a)$$

Again, ...

$$\mathfrak{o} \;=\; \begin{cases} \mathbb{Z}[\sqrt{-D}] & = \;\; \mathbb{Z}\oplus\mathbb{Z}\sqrt{-D} \quad (\text{for } -D = 2,3 \bmod 4) \\ \mathbb{Z}[\frac{1+\sqrt{-D}}{2}] & = \;\; \mathbb{Z}\oplus\mathbb{Z}\frac{1+\sqrt{-D}}{2} \quad (\text{for } -D = 1 \bmod 4)\end{cases}$$

$\mathfrak{o}$ is a free $\mathbb{Z}$-module of rank 2, and is a *lattice* in $\mathbb{C}$: $\mathfrak{o}$ is a *discrete* subgroup of $\mathbb{C}$, and $\mathbb{C}/\mathfrak{o}$ is *compact*.

Galois norm is the *complex* norm-squared: $N^k_{\mathbb{Q}}(\alpha) = \alpha\cdot\bar{\alpha} = |\alpha|^2$.

For complex quadratic k, the special value $L(1,\chi)$ has a finite, closed-form expression. Recall that the *conductor* N of χ is a positive integer such that $\chi(p)$ depends only on p mod N.

[15.6] Claim: The *conductor* N of $\chi(p) = (-D/p)_2$ is

$$N \;=\; \begin{cases} D & (\text{for } -D = 1 \bmod 4) \\ 4D & (\text{for } -D = 2,3 \bmod 4)\end{cases}$$

Proof: Use quadratic reciprocity. For D an odd *prime*,

$$\Big(\frac{-D}{p}\Big)_2 \;=\; \Big(\frac{-1}{p}\Big)_2\Big(\frac{D}{p}\Big)_2 \;=\; (-1)^{\frac{p-1}{2}}\cdot(-1)^{\frac{p-1}{2}\frac{D-1}{2}}\Big(\frac{p}{D}\Big)_2$$

$$=\; (-1)^{\frac{p-1}{2}\frac{D+1}{2}}\Big(\frac{p}{D}\Big)_2 \;=\; \begin{cases} (\frac{p}{D})_2 & (\text{for } D = 3 \bmod 4) \\ (-1)^{\frac{p-1}{2}}\cdot(\frac{p}{D})_2 & (\text{for } D = 1 \bmod 4)\end{cases}$$

For $D = 2q$ with odd prime q,

$$\Big(\frac{-D}{p}\Big)_2 = \Big(\frac{-1}{p}\Big)_2\Big(\frac{2}{p}\Big)_2\Big(\frac{q}{p}\Big)_2 = \; (-1)^{\frac{p-1}{2}}(-1)^{\frac{p^2-1}{8}}(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\Big(\frac{p}{q}\Big)_2$$

Here, as $(-1)^{(p^2-1)/8}$ is a slightly un-transparent interpolation of the quadratic symbol for 2, we must check the cases $p = 1,3,5,7 \bmod 8$ to see that, no matter the congruence class of q, the aggregate is only defined mod $8q = 4(2q)$.

For $D = q_1 \ldots q_\ell$ with odd primes q_j,

$$\Big(\frac{-D}{p}\Big)_2 \;=\; (-1)^{\frac{p-1}{2}[1+\frac{q_1-1}{2}+\ldots+\frac{q_\ell-1}{2}]}\Big(\frac{p}{q_1}\Big)_2\cdots\Big(\frac{p}{q_\ell}\Big)_2$$

With ν the number of $q_j = 3 \bmod 4$, the power of -1 is $(-1)^{\frac{p-1}{2}(1+\nu)}$. For $\nu = 1 \bmod 4$, this depends on $p \bmod 4$, and $q_1 \ldots q_\ell = 3 \bmod 4$, while for $\nu = 3 \bmod 4$ this is $+1$, and $q_1\ldots q_\ell = 1 \bmod 4$. A similar consideration applies to $D = 2q_1\ldots q_\ell$. ///

[15.7] Remark: The precise determination of the conductor of χ for quadratic characters χ accounts for a classical usage: for square-free integer d,

$$\text{discriminant } \mathbb{Q}(\sqrt{d}) \;=\; \begin{cases} |d| & (\text{for } d = 1 \bmod 4) \\ \\ 4|d| & (\text{for } d = 2, 3 \bmod 4) \end{cases} \;=\; \text{conductor of } \begin{pmatrix} d \\ * \end{pmatrix}_2$$

This appears to differ from the *square* of *co-area* of $\mathfrak{o}$ by a factor of 4: for example,

$$\text{co-area } \mathbb{Z}[\sqrt{-5}] \;=\; \text{area of rectangle spanned by } 1, \sqrt{-5} \;=\; \sqrt{5}$$

while the discriminant/conductor is 20. Later, we will find that the best normalization of measure on $\mathbb{C}$ rectifies this!

The Fourier expansion of the sawtooth function is

$$s(x) \;=\; x - \tfrac{1}{2} \;=\; \frac{-1}{2\pi i}\sum_{n\neq 0} \frac{e^{2\pi i n x}}{n} \qquad\qquad (\text{for } 0 < x < 1)$$

The standard discussion of the Dirichlet kernel shows that Fourier series of piecewise differentiable functions f with left and right limits at discontinuities *do* converge, and to f, at points where f is differentiable. Thus,

$$\sum_{a \bmod N} \chi(a)\cdot\Big(\frac{a}{N} - \tfrac{1}{2}\Big) \;=\; \sum_{a \bmod N} \chi(a)\cdot s\Big(\frac{a}{N}\Big) \;=\; \frac{-1}{2\pi i}\sum_a \chi(a) \sum_{n\neq 0} \frac{e^{2\pi i n a/N}}{n} \;=\; \frac{-1}{2\pi i}\sum_{n\neq 0}\frac{\chi(n)}{n}\cdot\sum_a \chi(a) e^{2\pi i a/N}$$

by replacing a by an^{-1} mod N. Since $\chi(-1) = -1$ (!!!)...

In fact, for quadratic characters, $\chi(-1)$ does tell whether the field is *real* or *complex*:

[15.8] Lemma: For quadratic characters χ,

$$\chi(-1) \;=\; \begin{cases} -1 & (\text{for } \chi(p) = (-D/p)_2) \\ \\ +1 & (\text{for } \chi(p) = (D/p)_2) \end{cases} \qquad\qquad (\text{squarefree } D > 0)$$

Proof: As a simple case, take D odd *prime*. The conductor is either D or $4D$. For a *prime* $p = -1 \bmod 4D$,

$$\chi(-1) \;=\; \begin{pmatrix} -D \\ p \end{pmatrix}_2 \;=\; (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{D-1}{2}}\begin{pmatrix} p \\ D \end{pmatrix}_2$$

$$=\; (-1)^{\frac{p-1}{2}\frac{D+1}{2}}\begin{pmatrix} -1 \\ D \end{pmatrix}_2 = \; (-1)^{\frac{p-1}{2}\frac{D+1}{2}}(-1)^{\frac{D-1}{2}} \;=\; (-1)^{\frac{p-1}{2}\cdot D} \;=\; -1$$

since $p = 3 \bmod 4$. For $(D/p)_2$ with *prime* $p = -1 \bmod 4D$,

$$\chi(-1) \;=\; \begin{pmatrix} D \\ p \end{pmatrix}_2 \;=\; (-1)^{\frac{p-1}{2}\frac{D-1}{2}}\begin{pmatrix} p \\ D \end{pmatrix}_2 \;=\; (-1)^{\frac{p-1}{2}\frac{D-1}{2}}\begin{pmatrix} -1 \\ D \end{pmatrix}_2 = \; (-1)^{\frac{p-1}{2}\frac{D-1}{2}}(-1)^{\frac{D-1}{2}} \;=\; +1$$

Dirichlet's theorem on primes in arithmetic progressions gives infinitely-many primes $p = -1 \bmod 4D$, but this is excessive. Instead, with $n = -1 \bmod 4D$, factor $n = q_1 \ldots q_\ell$, apply quadratic reciprocity, and track parities, as we did in the determination of the conductor of quadratic characters. And factor D... ///

Thus, indeed, $\chi(-1) = -1$ for complex quadratic fields. Back to the class number formula computation...

So far,

$$\sum_{a \bmod N} \chi(a) \cdot \left(\frac{a}{N} - \tfrac{1}{2}\right) \;=\; \frac{-1}{2\pi i} \sum_{n \neq 0} \frac{\chi(n)}{n} \cdot \sum_a \chi(a) e^{2\pi i a/N}$$

Since $\chi(-1) = -1$, the summands $\chi(n)/n$ for $\pm n$ are *identical*, rather than *cancelling*, so

$$\sum_{a \bmod N} \chi(a) \cdot \left(\frac{a}{N} - \tfrac{1}{2}\right) \;=\; \frac{-1}{\pi i} \cdot L(1,\chi) \cdot \sum_a \chi(a) e^{2\pi i a/N}$$

and

$$L(1,\chi) \;=\; \frac{-\pi i}{\sum_a \chi(a) e^{2\pi i a/N}} \sum_{a \bmod N} \chi(a) \cdot \left(\frac{a}{N} - \tfrac{1}{2}\right)$$

Thus,

$$\frac{\pi \cdot h(\mathfrak{o})}{|\mathfrak{o}^\times| \cdot \text{co-area}(\mathfrak{o})} \;=\; \frac{-\pi i}{\sum_a \chi(a) e^{2\pi i a/N}} \sum_{a \bmod N} \left(\frac{a}{N} - \tfrac{1}{2}\right) \cdot \chi(a)$$

and, for *complex* quadratic fields,

$$h(\mathfrak{o}) \;=\; \frac{-i \cdot |\mathfrak{o}^\times| \cdot \text{co-area}(\mathfrak{o})}{\sum_a \chi(a) e^{2\pi i a/N}} \sum_{a \bmod N} \left(\frac{a}{N} - \tfrac{1}{2}\right) \cdot \chi(a)$$

[15.9] Claim:

$$\left| \frac{\text{co-area}(\mathfrak{o})}{\sum_a \chi(a) e^{2\pi i a/N}} \right| \;=\; \frac{1}{2}$$

Proof: For $-D = 1 \bmod 4$, $\mathfrak{o} = \mathbb{Z}[\frac{1+\sqrt{-D}}{2}]$, and the co-area of $\mathfrak{o}$ is

$$\det \begin{pmatrix} \mathrm{Re}(1) & \mathrm{im}(1) \\ \mathrm{Re}(\frac{1+\sqrt{-D}}{2}) & \mathrm{im}(\frac{1+\sqrt{-D}}{2}) \end{pmatrix} \;=\; \det \begin{pmatrix} 1 & 0 \\ \frac{1}{2} & \frac{\sqrt{D}}{2} \end{pmatrix} \;=\; \frac{\sqrt{D}}{2}$$

For $-D = 2, 3 \bmod 4$, $\mathfrak{o} = \mathbb{Z}[\sqrt{-D}]$, and the co-area of $\mathfrak{o}$ is

$$\det \begin{pmatrix} \mathrm{Re}(1) & \mathrm{im}(1) \\ \mathrm{Re}(\sqrt{-D}) & \mathrm{im}(\sqrt{-D}) \end{pmatrix} \;=\; \det \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{D} \end{pmatrix} \;=\; \sqrt{D}$$

These conditions mod 4 also determine whether the conductor N is D, or $4D$, and in all cases

$$\text{co-area}(\mathfrak{o})^2 \;=\; \frac{1}{4} \cdot N \qquad\qquad \text{(in a naive normalization)}$$

(Recall the)

[15.10] Claim: The Gauss sum for a character of conductor N has absolute value $\sqrt{N}$.

Proof: Starting the computation in the obvious fashion, writing $\psi(a) = e^{2\pi i a/N}$. Let Σ' denote sum over $(\mathbb{Z}/N)^\times$, and Σ'' denote sum over $\mathbb{Z}/N - (\mathbb{Z}/N)^\times$.

$$\Big| \sum_{a \bmod N} \chi(a)\, \psi(a) \Big|^2 \;=\; {\sum_{a,b}}' \; \chi(a)\, \psi(a)\, \overline{\chi}(b)\, \psi(-b)$$

Replacing a by ab, this becomes

$$\sum_{a,b}{}' \chi(a)\,\psi\big((a-1)\cdot b\big)$$

We claim that, because χ has conductor N (and not smaller!)

$$\sum_{a}{}' \chi(a)\,\psi((a-1)\cdot b) \;=\; 0 \qquad\qquad (\text{for } \gcd(b,N)>1)$$

To see this, let p be a prime dividing $\gcd(b,N)$. That N is the conductor of χ is to say that χ is *primitive* mod N, meaning that χ does not factor through *any* quotient $\mathbb{Z}/(N/p)$. That is, there is some $\eta = 1 \bmod N/p$ such that $\chi(\eta)\neq 1$.

Since $p|b$, and $\eta = 1 \bmod N/p$,

$$(a\eta-1)\cdot b \;=\; (a-1)b + a(\eta-1)b \;=\; (a-1)b \bmod N$$

Thus, replacing a by ηa,

$$\sum_{a}{}' \chi(a)\,\psi((a-1)\cdot b) \;=\; \sum_{a}{}' \chi(a\eta)\,\psi((a\eta-1)\cdot b)$$

$$=\; \chi(\eta)\sum_{a}{}' \chi(a)\,\psi((a-1)\cdot b)$$

Thus, the sum over a is 0. Thus, we can drop the coprimality constraint:

$$\sum_{a,b}{}' \chi(a)\,\psi\big((a-1)\cdot b\big) \;=\; \sum_{a,b} \chi(a)\,\psi\big((a-1)\cdot b\big)$$

For $a\neq 1$, the inner sum over b is 0, because the sum of a non-trivial character over a finite group is 0. For $a=1$ the sum over b gives N. ///

Thus, the absolute value of the Gauss sum for *any* character with conductor exactly N is $\sqrt{N}$.

Returning to the class number formula for complex quadratic fields,

$$h(\mathfrak{o}) \;=\; \frac{\varepsilon\cdot|\mathfrak{o}^\times|}{2}\sum_{a \bmod N}\big(\frac{a}{N}-\tfrac{1}{2}\big)\cdot\chi(a) \qquad (\text{for some } |\varepsilon|=1)$$

The number of summands can be reduced by a factor of 2, as follows. Since $\chi(-1)=-1$, $\chi(N-a) = \chi(-a) = -\chi(a)$. Likewise,

$$\frac{N-a}{N}-\tfrac{1}{2} \;=\; 1-\frac{a}{N}-\tfrac{1}{2} \;=\; -\big(\frac{a}{N}-\tfrac{1}{2}\big)$$

Thus, we need only sum up over $a<N/2$. When $N/2$ is an integer, N was even, so divisible by 4, so $\chi(N/2)=0$. Thus,

$$h(\mathfrak{o}) \;=\; \varepsilon\cdot|\mathfrak{o}^\times|\sum_{1\le a<N/2}\big(\frac{a}{N}-\tfrac{1}{2}\big)\cdot\chi(a) \qquad (\text{for some } |\varepsilon|=1)$$

[15.11] Example: $D=3$ gives the Eisenstein integers $\mathfrak{o}$, which we know to have class number 1, since the ring is a PID. Here $|\mathfrak{o}^\times|=6$.

$$|\mathfrak{o}^\times|\sum_{1\le a<N/2}\big(\frac{a}{N}-\tfrac{1}{2}\big)\cdot\chi(a) \;=\; 6(\tfrac{1}{3}-\tfrac{1}{2})\cdot(+1) \;=\; -1$$

Adjust by $\varepsilon = -1$ to obtain $h(\mathfrak{o}) = 1$, indeed.

[15.12] Example: For $D = 5$, the conductor is $N = 20$ and $|\mathfrak{o}^\times| = 2$.

$$|\mathfrak{o}^\times| \sum_{1\le a<N/2} \big(\frac{a}{N} - \tfrac{1}{2}\big) \cdot \chi(a)$$

$$= 2\Big((\tfrac{1}{20} - \tfrac{1}{2})(+1) + (\tfrac{3}{20} - \tfrac{1}{2})\big(\tfrac{-5}{3}\big)_2 + (\tfrac{7}{20} - \tfrac{1}{2})\big(\tfrac{-5}{7}\big)_2 + (\tfrac{9}{20} - \tfrac{1}{2})\big(\tfrac{-5}{9}\big)_2\Big)$$

$$= 2\Big((\tfrac{1}{20} - \tfrac{1}{2})(+1) + (\tfrac{3}{20} - \tfrac{1}{2})(+1) + (\tfrac{7}{20} - \tfrac{1}{2})(+1) + (\tfrac{9}{20} - \tfrac{1}{2})(+1)\Big)$$

$$= 2\Big(\tfrac{1}{20} + \tfrac{3}{20} + \tfrac{7}{20} + \tfrac{9}{20} - 2\Big) = -2$$

Adjust by $\varepsilon = -1$ to obtain $h(\mathfrak{o}) = 2$. This is not surprising, given

$$2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$$

---

16. *Topologies, completions/limits*

An **absolute value** or *norm* $x \to |x|$ on a field k is a non-negative real-valued function on k such that

$$\begin{cases} |x| = 0 \text{ only for } x = 0 & \text{(positivity)} \\ |xy| = |x| \cdot |y| & \text{(multiplicativity)} \\ |x+y| \le |x| + |y| & \text{(triangle inequality)} \end{cases}$$

When $|x + y| \le \max(|x|, |y|)$, the norm is *non-archimedean*, or a *valuation.*

A norm gives k has a metric *topology* by $d(x, y) = |x - y|$. Since $|x| = |x \cdot 1| = |x| \cdot |1|$ we have $|1| = 1$. Also, $|\omega|^n = |\omega^n| = |1|$ for an n^{th} root of unity, so $|\omega| = 1$. Then *reflexivity, symmetry*, and the triangle inequality follow for the metric.

[16.1] Theorem: Two norms $| * |_1$ and $| * |_2$ on k give the same *non-discrete* topology on a field k if and only if $| * |_1 = | * |_2^t$ for some $0 < t \in \mathbb{R}$.

Proof: If the two norms are related this way, they certainly give the same topology. Conversely, assume they give the same non-discrete topology. Then $|x|_1 < 1$ implies $x^n \to 0$ in the $| * |_1$ topology. Thus, $x^n \to 0$ in the $| * |_2$ topology, so $|x|_2 < 1$. Similarly, if $|x|_1 > 1$, then $|x^{-1}|_1 < 1$, so $|x|_2 > 1$.

Fix y with $|y|_1 > 1$. Given $|x|_1 \ge 1$, there is $t \in \mathbb{R}$ such that $|x|_1 = |y|_1^t$. For rational $a/b > t$, $|x|_1 < |y|_1^{a/b}$, so $|x^b/y^a|_1 < 1$. Then $|x^b/y^a|_2 < 1$, and $|x|_2 < |y|_2^{a/b}$.

Similarly, $|x|_2 > |y|_2^{a/b}$ for $a/b < t$. Thus, $|x|_2 = |y|_2^t$, and

$$|x|_2 = |y|_2^t = \big(|y|_1^{\frac{\log|y|_2}{\log|y|_1}}\big)^t = \big(|y|_1^t\big)^{\frac{\log|y|_2}{\log|y|_1}} = |x|_2^{\frac{\log|y|_2}{\log|y|_1}} \qquad ///$$

The *completion* of k with respect to a metric given by a norm is the usual metric completion, and the norm and metric extend by continuity. Assume k is not *discrete.*

It is reasonable to think of $k = \mathbb{R}, \mathbb{C}, \mathbb{Q}_p$ or finite extensions of $\mathbb{Q}_p$, and also $\mathbb{F}_q((x))$ and its finite extensions.

[16.2] Theorem: Over a complete, non-discrete normed field k,

- A *finite-dimensional* k-vectorspace V has just one Hausdorff topology so that vector addition and scalar multiplication are continuous (a *topological vectorspace* topology). All linear endomorphisms are *continuous.*
- A finite-dimensional k-subspace V of a topological k-vectorspace W is necessarily a *closed* subspace of W.
- A k-linear map $\phi : X \to V$ to a finite-dimensional space V is continuous if and only if the kernel is closed.

[16.3] Remark: The main application of this is to finite field extensions V of $k = \mathbb{Q}_p$ or of $k = \mathbb{F}_q((x))$. The argument also succeeds over complete non-discrete *division algebras.*

A subset E of V is **balanced** when $xE \subset E$ for every $x \in k$ with $|x| \leq 1$.

[16.4] Lemma: Let U be a neighborhood of 0 in V. Then U contains a *balanced* neighborhood N of 0.

Proof: By continuity of scalar multiplication, there is $\varepsilon > 0$ and a neighborhood U' of $0 \in V$ so that when $|x| < \varepsilon$ and $v \in U'$ then $xv \in U$. Since k is non-discrete, there is $x_o \in k$ with $0 < |x_o| < \varepsilon$. Since scalar multiplication by a non-zero element is a *homeomorphism*, x_oU' is a neighborhood of 0 and $x_oU' \subset U$. Put

$$N \;=\; \bigcup_{|y|\leq 1} y(x_oU')$$

$|xy| \leq |y| \leq 1$ for $|x| \leq 1$, so

$$xN \;=\; \bigcup_{|y|\leq 1} x(yx_oU') \subset \bigcup_{|y|\leq 1} yx_oU' = N \qquad ///$$

[16.5] Proposition: For a one-dimensional topological vectorspace V, that is, a free module on one generator e, the map $k \to V$ by $x \to xe$ is a *homeomorphism.*

Proof: Scalar multiplication is continuous, so we need only show that the map is *open.* Given $\varepsilon > 0$, by non-discreteness there is x_o in k so that $0 < |x_o| < \varepsilon$. Since V is Hausdorff, there is a neighborhood U of 0 so that $x_oe \notin U$. Shrink U so it is *balanced.* Take $x \in k$ so that $xe \in U$. If $|x| \geq |x_o|$ then $|x_ox^{-1}| \leq 1$, so that

$$x_oe \;=\; (x_ox^{-1})(xe) \in U$$

by the balanced-ness of U, contradiction. Thus,

$$xe \in U \implies |x| < |x_o| < \varepsilon \qquad ///$$

[16.6] Corollary: Fix $x_o \in k$. A not-identically-zero k-linear k-valued function f on V is *continuous* if and only if the affine hyperplane

$$H = \{v \in V : f(v) = x_o\}$$

is *closed* in V.

Proof: For f is continuous, H is closed, being the complement of the open $f^{-1}(\{x \neq x_o\})$. For the converse, take $x_o = 0$, since vector additions are homeomorphisms of V to itself.

For $v_o, v \in V$ with $f(v_o) \neq 0$,

$$f\big(v - f(v)f(v_o)^{-1}v_o\big) \;=\; f(v) - f(v)f(v_o)^{-1}f(v_o) = 0$$

Thus, V/H is one-dimensional. Let $\bar{f} : V/H \to k$ be the induced k-linear map on V/H so that $f = \bar{f} \circ q$:

$$\bar{f}(v + H) = f(v)$$

By the previous proposition, $\bar{f}$ is a homeomorphism to k. so f is continuous. ///

Proof: *(of theorem)* To prove the uniqueness of the topology, prove that for any k-basis $e_1, \ldots, e_n$ for V, the map $k \times \ldots \times k \to V$ by

$$(x_1, \ldots, x_n) \to x_1 e_1 + \ldots + x_n e_n$$

is a homeomorphism. Prove this by induction on the dimension n. $n = 1$ was treated already. Granting this, since k is complete, the lemma asserting the closed-ness of complete subspaces shows that any one-dimensional subspace is closed. Take $n > 1$, and let $H = ke_1 + \ldots + ke_{n-1}$. By induction, H is closed in V, so V/H is a topological vector space. Let q be the quotient map. V/H is a one-dimensional topological vectorspace over k, with basis $q(e_n)$. By induction,

$$\varphi : xq(e_n) = q(xe_n) \to x$$

is a homeomorphism to k.

Likewise, ke_n is a closed subspace and we have the quotient map

$$q' : V \to V/ke_n$$

We have a basis $q'(e_1), \ldots, q'(e_{n-1})$ for the image, and by induction

$$\phi' : x_1 q'(e_1) + \ldots + x_{n-1} q'(e_{n-1}) \to (x_1, \ldots, x_{n-1})$$

is a homeomorphism.

By induction,

$$v \to (\phi \circ q)(v) \times (\phi' \circ q')(v)$$

is continuous to

$$k^{n-1} \times k \approx k^n$$

On the other hand, by the continuity of scalar multiplication and vector addition, the map

$$k^n \to V \quad \text{by} \quad x_1 \times \ldots \times x_n \to x_1 e_1 + \ldots + x_n e_n$$

is continuous.

The two maps are mutual inverses, proving that we have a homeomorphism.

Thus, a n-dimensional subspace is homeomorphic to k^n, so is complete, since a finite product of complete spaces is complete.

Thus, by the lemma asserting the closed-ness of complete subspaces, an n-dimensional subspace is always closed.

Continuity of a linear map $f : X \to k^n$ implies that the kernel $N = \ker f$ is closed. On the other hand, if N is closed, then X/N is a topological vectorspace of dimension at most n. Therefore, the induced map $\bar{f} : X/N \to V$ is unavoidably continuous. But then $f = \bar{f} \circ q$ is continuous, where q is the quotient map.

In particular, any k-linear map $V \to V$ has finite-dimensional kernel, so the kernel is closed, and the map is continuous.

This completes the induction. ///

[16.7] Corollary: Finite field extensions K of complete, non-discrete k have unique Hausdorff topologies making addition and multiplication continuous.

Proof: K is a finite-dimensional k-vectorspace. The only ingredient perhaps not literally supplied by the theorem is the continuity of the multiplication by elements of K. Such multiplications are k-linear endomorphisms of the vector space K, so are continuous, by the theorem. ///

[16.8] Remark: This discussion still did *not* use *local compactness* of the field k, so is not specifically number theoretic.

[16.9] Constructions/existence For any Dedekind domain $\mathfrak{o}$, and for a non-zero prime $\mathfrak{p}$ in $\mathfrak{o}$, the $\mathfrak{p}$-adic norm is

$$|x|_{\mathfrak{p}} \;=\; C^{-\mathrm{ord}_{\mathfrak{p}} x} \qquad\qquad (\text{where } x\cdot\mathfrak{o} = \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}} x}\cdot\text{prime-to-}\mathfrak{p})$$

and $C > 1$ is a constant. Since this norm is ultrametric/non-archimedean, the choice of C does not immediately matter, but it *can* matter in interactions of norms for varying $\mathfrak{p}$, as in the **product formula** for number fields and function fields. Recall the product formula for $\mathbb{Q}$:

[16.10] Theorem:

$$\prod_{v\le\infty} |x|_v \;=\; 1 \qquad\qquad (\text{for } x\in\mathbb{Q}^\times)$$

That is, with $|*|_\infty$ the 'usual' absolute value on $\mathbb{R}$,

$$|x|_\infty\cdot\prod_{p\text{ prime}} |x|_p \;=\; 1 \qquad\qquad (\text{for } x\in\mathbb{Q}^\times)$$

Proof: Both sides are *multiplicative* in x, so it suffices to consider $x=\pm1$ and $x=q$ prime. For units ±1, both sides are 1. For $x=q$ prime, $|q|_\infty = q$, while $|q|_q = 1/q$, and $|q|_p = 1$ for $p\neq q$, so again both sides are 1. ///

One normalization to have the product formula hold for *number fields k*: for $\mathfrak{p}$ lying over p, letting $k_{\mathfrak{p}}$ be the $\mathfrak{p}$-adic completion of k and Q_p the usual p-adic completion of $\mathbb{Q}$,

$$|x|_{\mathfrak{p}} \;=\; |N^{k_{\mathfrak{p}}}_{\mathbb{Q}_p} x|_p$$

For *archimedean* completion k_v of k, define (or renormalize)

$$|x|_v \;=\; |N^{k_v}_{\mathbb{R}} x|_\infty$$

The latter entails a normalization which (harmlessly) fails to satisfy the triangle inequality:

$$|x|_{\mathbb{C}} \;=\; |N^{\mathbb{C}}_{\mathbb{R}} x|_\infty \;=\; x\cdot\overline{x} \;=\; \textit{square}\text{ of usual complex abs value}$$

This normalization is used only in a multiplicative context, so failure of the triangle inequality is harmless. The metric topology is given by the *usual* norm.

In other words, for primes $\mathfrak{p}$ in $\mathfrak{o}$, in the formula above take $C = N\mathfrak{p} = |\mathfrak{o}/\mathfrak{p}|$, so

$$|x|_{\mathfrak{p}} \;=\; N\mathfrak{p}^{-\mathrm{ord}_{\mathfrak{p}} x}$$

[16.11] Theorem: *(Product formula for number fields)*

$$\prod_{\text{places } w \text{ of } k} |x|_w \;=\; \prod_{\text{places } v \text{ of } \mathbb{Q}}\;\prod_{w|v} |N^{k_w}_{Q_v}(x)|_v \;=\; 1 \qquad\qquad (\text{for } x\in k^\times)$$

Reduce to the product formula for $\mathbb{Q}$ by showing

$$\prod_{w|v} N^{k_w}_{\mathbb{Q}_v}(x) \;=\; N^k_{\mathbb{Q}}(x) \qquad\qquad (\text{for } x \in k, \text{ abs value } v \text{ of } \mathbb{Q})$$

Proof: Recall that one way to define Galois norm is, for an algebraically closed field Ω containing $\mathbb{Q}$,

$$N^k_{\mathbb{Q}}(x) \;=\; \prod_{\mathbb{Q}-algebra\ maps\ \sigma:k\to\Omega} \sigma(x)$$

[16.12] Claim: Let Ω be an algebraic closure of $\mathbb{Q}_v$. There is a natural isomorphism of sets

$$\mathrm{Hom}_{\mathbb{Q}-alg}(k,\Omega) \;\approx\; \mathrm{Hom}_{\mathbb{Q}_v-alg}(\mathbb{Q}_v \otimes_{\mathbb{Q}} k, \Omega)$$

by

$$\Big(x \to \sigma(x)\Big) \;\longrightarrow\; \Big(\alpha\otimes x \to \alpha\cdot\sigma(x)\Big)$$

Proof: Recall that a map from the tensor product is specified by its values on monomials $\alpha\otimes x$, and that these values can indeed be arbitrary, as long as the image of $\alpha a\otimes x$ is the same as that of $\alpha\otimes ax$, for $a \in \mathbb{Q}$.

Then the inverse set-map is

$$\Big(\alpha\otimes x \to \tau(\alpha\otimes x)\Big) \;\longrightarrow\; \Big(x \to \tau(1\otimes x)\Big) \qquad\qquad ///$$

[16.13] Remark: This is an example of *extension of scalars*, an example of a *left adjoint* to a forgetful functor. Then the isomorphism is an example of an *adjunction*.

Next, for finite *separable* $k/\mathbb{Q}$, invoke the theorem of the primitive element to choose α such that $k = \mathbb{Q}(\alpha)$, and let $P \in \mathbb{Q}[x]$ be the minimal polynomial of α over $\mathbb{Q}$. Since $k/\mathbb{Q}$ is separable, P has no repeated roots in an algebraic closure, etc. Then

$$\mathbb{Q}_v \otimes_{\mathbb{Q}} k \;\approx\; \mathbb{Q}_v\otimes_{\mathbb{Q}} \mathbb{Q}[x]/P \;\approx\; \mathbb{Q}_v[x]/P \;\approx\; \coprod_j \mathbb{Q}_v[x]/P_j \;\approx\; \text{coproduct of finite field extensions of } \mathbb{Q}_v$$

by Sun-Ze's theorem, where the P_j are the irreducible factors of P in $\mathbb{Q}_v[x]$, and we use the separability of $k/\mathbb{Q}$ to know that no repeated factors appear. By the defining property of coproducts

$$\mathrm{Hom}_{\mathbb{Q}_v-alg}(\coprod_j \mathbb{Q}_v[x]/P_j,\, \Omega) \;\approx\; \prod_j \mathrm{Hom}_{\mathbb{Q}_v-alg}(\mathbb{Q}_v[x]/P_j,\, \Omega)$$

Because Ω is a field, the $\mathbb{Q}_v$-algebra homs $\mathbb{Q}_v\otimes_{\mathbb{Q}} k \to \Omega$ biject with the maximal ideals of the $\mathbb{Q}_v\otimes_{\mathbb{Q}} k$. The maximal ideals in a product $K_1\times\ldots\times K_n$ of fields K_j are $M_j = K_1\times\ldots\times\widehat{K_j}\times\ldots\times K_n$. Thus, the homs to Ω, with kernel M_j, are identified with homs $K_j \to \Omega$. That is, the set of $\mathbb{Q}$-homs $k\to\Omega$ is *partitioned* by the $\mathbb{Q}_v$-homs of the direct summands $\mathbb{Q}_v[x]/P_j$ to Ω.

It remains to show that the direct summands $\mathbb{Q}_v[x]/P_j$ are exactly the completions k_w of k extending the completion $\mathbb{Q}_v$ of $\mathbb{Q}$, *distinct* in the sense that there is *no* topological isomorphism φ fitting into a diagram

$$\begin{tikzcd} k_w \arrow[rr, "(\text{non}-\text{existent})\ \varphi"] & & k_{w'} \\ & k \arrow[ul, "\text{inc}"] \arrow[ur, "\text{inc}"'] & \end{tikzcd}$$

(for $w \neq w'$)

First, Ω has a unique topological $\mathbb{Q}_v$-vectorspace topology, because it is an ascending union ((filtered) *colimit*!) of finite-dimensional $\mathbb{Q}_v$-vectorspaces, which have unique topological vector space topologies. Colimits are unique, up to unique isomorphism.

On one hand, $\sigma : k \to \Omega$ (over $\mathbb{Q}$) gives k a Hausdorff topology with continuous addition, multiplication, and non-zero inversion. The compositum $\mathbb{Q}_v \cdot \sigma(k)$ is finite-dimensional over $\mathbb{Q}_v$, so the closure of $\sigma(k)$ in Ω is a *complete* $\mathbb{Q}_v$ topological vector space. Thus, $\sigma : k \to \Omega$ gives a completion of k extending $\mathbb{Q}_v$.

On the other hand, a completion k_w is really an inclusion $k \to k_w$ with k_w complete. Again, there is the adjunction

$$\mathrm{Hom}_{\mathbb{Q}-alg}(k, k_w) \;\approx\; \mathrm{Hom}_{\mathbb{Q}_v-alg}(\mathbb{Q}_v \otimes_{\mathbb{Q}} k, k_w)$$

Thus, in fact, $\mathbb{Q}_v[x]/P_j \approx k_w$ for some P_j.

By the separability of $k/\mathbb{Q}$, the P_j's have no common factors, so the inclusions $k \to \mathbb{Q}_v[x]/P_j$ by $\alpha \to x \bmod P_j$ are incompatible with every non-zero $\mathbb{Q}_v$-hom $\mathbb{Q}_v[x]/P_i \to \mathbb{Q}_v[x]/P_j$ for $i \neq j$. Indeed, the requirement $\alpha \to x \bmod P_j$ limits the candidates to situations

$$\begin{tikzcd} \mathbb{Q}_v[x] \arrow[r, "\text{quot}"] \arrow[rr, bend left, "\Phi"] & \mathbb{Q}_v[x]/P_i \arrow[r, "???"] & \mathbb{Q}_v[x]/P_j \\ & k \arrow[ul, "\alpha\to x"] \arrow[u, "\alpha\to x"] \arrow[ur, "\alpha\to x"'] & \end{tikzcd}$$

which forces $\ker \Phi = \langle P_j \rangle$. This cannot factor through the quotient. Thus, there are no isomorphisms among the $\mathbb{Q}_v[x]/P_j$ compatible with the inclusions of k.

In summary, we have proven that the *global* (Galois) norm $N^k_{\mathbb{Q}}$ is the product of the *local* norms, reducing the product formula for number fields to that for $\mathbb{Q}$. ///

[16.14] Remark: The argument did not depend on the specifics, so applies to extensions K/k and completions k_v of the base field. In the course of the proof, some useful auxiliary points were demonstrated, stated now in general:

[16.15] Corollary: Let k be a field with completion k_v. Let K be a finite separable extension of k. Let w index the topological isomorphism classes of completions of K extending k_v. The sum of the *local* degrees is the *global* degree:

$$\sum_{w|v} [K_w : k_v] = [K : k]$$

[16.16] Corollary: For K/k finite separable, the topological isomorphism classes of completions K_w of K extending k_v arise from inclusions of K to the algebraic closure of k_v. (This does not address automorphisms.)

[16.17] Corollary: The global trace $K \to k$ is the sum of the local traces $K_w \to k_v$.

The following generalizes to number fields and functions fields over finite fields. Traditionally, this result (and its generalizations) are called *Ostrowski's theorem*, but there are some issues surrounding this attribution.

Classification of completions: The topologically (via the associated metrics) inequivalent (non-discrete) norms on $\mathbb{Q}$ are the usual $\mathbb{R}$ norm and the p-adic $\mathbb{Q}_p$'s.

Proof: Let $|*|$ be a norm on $\mathbb{Q}$. It turns out (intelligibly, if we guess the answer) that the watershed is whether $|*|$ is *bounded* or *unbounded* on $\mathbb{Z}$. That is, the statement of the theorem could be sharpened to say: norms on $\mathbb{Q}$ bounded on $\mathbb{Z}$ are topologically equivalent to p-adic norms, and norms unbounded on $\mathbb{Z}$ are topologically equivalent to the norm from $\mathbb{R}$.

To say that $|*|$ is *bounded* on $\mathbb{Z}$, but *not discrete*, implies that $|p| < 1$ for some prime number p, by unique factorization. Suppose that there were a second prime q with $|q| < 1$. Then...

... with $a, b \in \mathbb{Z}$ such that $ap^m + bq^n = 1$ for positive integers m, n,

$$1 \;=\; |1| \;=\; |ap^m + bq^n| \;\le\; |a| \cdot |p|^m + |b| \cdot |q|^n \;\le\; |p|^m + |q|^n$$

This is impossible if *both* $|p| < 1$ and $|q| < 1$, by taking m, n large. Thus, for $|*|$ bounded on $\mathbb{Z}$, there is a unique prime p such that $|p| < 1$. Up to normalization, such a norm is the p-adic norm.

Next, claim that if $|a| \le 1$ for some $1 < a \in \mathbb{Z}$, then $|*|$ is *bounded* on $\mathbb{Z}$. Given $1 < b \in \mathbb{Z}$, write b^n in an a-ary expansion

$$b^n \;=\; c_o + c_1 a + c_2 a^2 + \ldots + c_\ell a^\ell \qquad\qquad (\text{with } 0 \le c_i < a)$$

and apply the triangle inequality,

$$|b|^n \;\le\; (\ell + 1) \cdot \underbrace{(1 + \ldots + 1)}_{a} \;\le\; (n \log_a b + 1) \cdot a$$

Taking n^{th} roots and letting $n \to +\infty$ gives $|b| \le 1$, and $|*|$ is bounded on $\mathbb{Z}$.

The remaining scenario is $|a| \ge 1$ for $a \in \mathbb{Z}$. For $a > 1$, $b > 1$, the a-ary expansion

$$b^n \;=\; c_o + c_1 a + c_2 a^2 + \ldots + c_\ell a^\ell \qquad\qquad (\text{with } 0 \le c_i < a)$$

with $|a| \ge 1$ gives

$$|b|^n \;\le\; (\ell + 1) \cdot \underbrace{(1 + \ldots + 1)}_{a} \cdot |a|^\ell \;\le\; (n \log_a b + 1) \cdot a \cdot |a|^{n \log_a b + 1}$$

Taking n^{th} roots and letting $n \to +\infty$ gives $|b| \le |a|^{\log_a b}$. Similarly, $|a| \le |b|^{\log_b a}$. Since $|*|$ is not bounded on $\mathbb{Z}$, there is $C > 1$ such that $|a| = C^{\log |a|}$ for all $0 \ne a \in \mathbb{Z}$. Up to normalization, this is the usual absolute value for $\mathbb{R}$. ///

To have the product formula hold for *number fields k*: for $\mathfrak{p}$ lying over p, letting $k_\mathfrak{p}$ be the $\mathfrak{p}$-adic completion of k and Q_p the usual p-adic completion of $\mathbb{Q}$,

$$|x|_\mathfrak{p} \;=\; |N^{k_\mathfrak{p}}_{\mathbb{Q}_p} x|_p \;=\; N\mathfrak{p}^{-\mathrm{ord}_\mathfrak{p} x}$$

Similarly, for *archimedean k_v*, define (or renormalize)

$$|x|_v \;=\; |N^{k_v}_{\mathbb{R}} x|_\infty$$

This product-formula normalization of the norm on $\mathbb{C}$ (harmlessly) fails to satisfy the triangle inequality:

$$|x|_{\mathbb{C}} \;=\; |N_{\mathbb{R}}^{\mathbb{C}} x|_\infty \;=\; x \cdot \overline{x} \;=\; \textit{square} \text{ of usual complex abs value}$$

For example,

$$|2|_{\mathbb{C}} \;=\; |N_{\mathbb{R}}^{\mathbb{C}} 2|_{\mathbb{R}} \;=\; |4|_{\mathbb{R}} \;=\; 4 \;>\; 1+1 \;=\; |1|_{\mathbb{C}} + |1|_{\mathbb{C}}$$

For **function fields** $k = \mathbb{F}_q(x)$, for p-adic v associated to non-zero prime $\mathfrak{p} = \varpi \mathbb{F}_q[x]$, the same sort of definition of norm is appropriate:

$$|f|_v \;=\; N\mathfrak{p}^{-\mathrm{ord}_{\mathfrak{p}} f} \;=\; q^{-\deg \varpi \cdot \mathrm{ord}_{\mathfrak{p}} f}$$

The *infinite* norm $|*|_\infty$ corresponding to the prime ideal $\mathfrak{q}$ generated by $1/x$ in $\mathfrak{o}_\infty = \mathbb{F}_q[1/x]$, is

$$|f|_v \;=\; q^{+\deg f} \;=\; |\mathfrak{o}_\infty/\mathfrak{q}|^{-\mathrm{ord}_{\mathfrak{q}} f}$$

since $a_n x^n + \ldots + a_o = (\frac{1}{x})^{-n}(a_n + \ldots + a_o(\frac{1}{x})^n)$

[16.18] Corollary: *(of proof)* The sum of the *local* degrees is the *global* degree:

$$\sum_{w|v} [K_w : k_v] = [K : k]$$

The global trace is the sum of the local traces:

$$\mathrm{tr}_k^K(x) \;=\; \mathrm{tr}_{k_v}^{K_w}(x) \qquad\qquad (\text{for } x \in K)$$

Why do we care about formulas $\prod_v \mathit{symbol}_v(x) = 1$? The **idele group** $\mathbb{J} = \mathbb{J}_k$ of k is a colimit over finite sets S of places containing archimedean places:

$$\mathbb{J} \;=\; \mathbb{J}_k \;=\; \mathrm{colim}_S \Big(\prod_{v \in S} k_v^\times \times \prod_{v \notin S} \mathfrak{o}_v^\times \Big)$$

The idele group *surjects* to the group of fractional ideals of k, by

$$\alpha = \{\alpha_v\} \;\longrightarrow\; \prod_{v<\infty} \Big((\alpha_v \cdot \mathfrak{o}_v) \cap k \Big)$$

$k^\times$ maps to *principal* fractional ideals, so the **idele class group** $\mathbb{J}/k^\times$ surjects to the *ideal class group* C_k. It also parametrizes *generalized* class groups.

An **idele class character**, or **Hecke character**, or **grossencharacter**, is a continuous group hom $\mathbb{J}/k^\times \to \mathbb{C}^\times$. *Some* of these characters arise from composition with *ideal class group* characters χ, by

$$\begin{tikzcd} \mathbb{J}/k^\times \arrow[r] & C_k \arrow[r, "\chi"] & \mathbb{C}^\times \end{tikzcd}$$

The *product formula* asserts that the **idele norm**

$$x = \{x_v\} \;\longrightarrow\; |x| \;=\; \prod_{v \le \infty} |x_v|_v \qquad\qquad (\text{for } x \in \mathbb{J}_k)$$

factors through $\mathbb{J}/k^\times$. Thus, for $s \in \mathbb{C}$, we have an idele class character

$$x \longrightarrow |x|^s \qquad\qquad (\text{for } x \in \mathbb{J}/k^\times)$$

These characters enter the Iwasawa-Tate modern version of Riemann's argument for meromorphic continuation and functional equation of zeta functions and (abelian) L-functions.

Proving that an infinite product of almost-all 1's is equal to 1 should remind us of *reciprocity laws*, although reciprocity laws are subtler than the product formula. Recall

quadratic norm residue symbols $\subset$ idele class characters
$\Downarrow$
quadratic Hilbert symbol reciprocity
$\Downarrow$
quadratic reciprocity (general)

[16.19] Corollary: Up to topological equivalence, every norm on a number field is either $\mathfrak{p}$-adic or arises from $\mathbb{R}$ and $\mathbb{C}$. ///

[16.20] Remark: Note that the product-formula norms K_w on an extension K of k are *not* the *extensions* of the norm k_v with $w|v$. This is visible on the bottom completion k_v:

$$|x|_w \;=\; |N^{K_w}_{k_v}(x)|_v \;=\; |x^{[K:k]}|_v \;=\; |x|_v^{[K:k]} \qquad\qquad (\text{for } x \in k_v)$$

Indeed, on other occasions, the *extension* is the appropriate object, instead of composing with Galois norm.

Context should clarify what norm is appropriate. Typically, *multiplicative* computations/discussions use the product-formula norm, while genuine *metric* computations/discussions use the *extension.*

Additive (Weak) Approximation: *(Artin-Whaples, Lang)* Let $v_1, \ldots, v_n$ index pairwise topologically inequivalent norms on a field k. Given $x_1, \ldots, x_n \in k$ and $\varepsilon > 0$, there exists $x \in k$ such that

$$|x - x_j|_{v_j} \;<\; \varepsilon \qquad\qquad (\text{for } j = 1, \ldots, n)$$

[16.21] Remark: When the norms are p-adic, arising from prime ideals in a Dedekind ring $\mathfrak{o}$ inside k, this is Sun-Ze's theorem.

Proof: First, we need to refine the notion of topological inequivalence, to exclude the possibility that the $| * |_1$ topology τ_1 is strictly finer than the $| * |_2$-topology τ_2. This uses the same proof mechanism as the earlier result showing that with two norms giving the *same* topology, each is a power of the other.

Suppose that the identity $(k, \tau_1) \to (k, \tau_2)$ is continuous. Then $|x|_1 < 1$ implies $x^n \to 0$ in the $| * |_1$ topology. Thus, $x^n \to 0$ in the $| * |_2$ topology, so $|x|_2 < 1$. Similarly, if $|x|_1 > 1$, then $|x^{-1}|_1 < 1$, so $|x|_2 > 1$.

Fix y with $|y|_1 > 1$. Given $|x|_1 \geq 1$, there is $t \in \mathbb{R}$ such that $|x|_1 = |y|_1^t$. For rational $a/b > t$, $|x|_1 < |y|_1^{a/b}$, so $|x^b/y^a|_1 < 1$. Then $|x^b/y^a|_2 < 1$, and $|x|_2 < |y|_2^{a/b}$.

Similarly, $|x|_2 > |y|_2^{a/b}$ for $a/b < t$. Thus, $|x|_2 = |y|_2^t$, and

$$|x|_2 \;=\; |y|_2^t \;=\; \Big(|y|_1^{\frac{\log|y|_2}{\log|y|_1}}\Big)^t \;=\; \big(|y|_1^t\big)^{\frac{\log|y|_2}{\log|y|_1}} \;=\; |x|_1^{\frac{\log|y|_2}{\log|y|_1}} \qquad ///$$

Thus, as a corollary, for $|*|_1$ and $|*|_2$ topologically inequivalent, there exists $x \in k$ with $|x|_1 \geq 1$ and $|x|_2 < 1$.

Similarly, let $|y|_1 < 1$ and $|y|_2 \geq 1$. Then $z = y/x$ has $|z|_1 < 1$ and $|z|_2 > 1$.

Inductively, much as in Sun-Ze's theorem, suppose $|z|_1 > 1$ and $|z|_j < 1$ for $2 \leq j \leq n$, and find z' such that $|z'|_1 > 1$ and $|z'|_j < 1$ for $2 \leq j \leq n+1$. Let $|w|_1 > 1$ and $|w|_{n+1} < 1$. There are two cases: for $|z|_{n+1} \leq 1$, then $z' = w \cdot z^\ell$ is as desired, for large ℓ. For $|z|_{n+1} > 1$, $z' = w \cdot z^\ell/(1+z^\ell)$ is as desired, for large ℓ.

So there exist $z_1, \ldots, z_n$ with $|z_j| > 1$ while $|z_j|_{j'} \leq 1$ for $j' \neq j$. Then $z_j^\ell/(1+z_j^\ell)$ goes to 1 at $|*|_j$, and to 0 in the other topologies. Thus, for large-enough ℓ,

$$x_1 \cdot \frac{z_1^\ell}{1+z_1^\ell} + \ldots + x_n \cdot \frac{z_n^\ell}{1+z_n^\ell} \quad \longrightarrow \quad x_j \qquad \text{(in the } j^{th} \text{ topology)}$$

This proves the (weak) approximation theorem. ///

Recall that the ring of **adeles** $\mathbb{A} = \mathbb{A}_k$ of k is

$$\mathbb{A} \;=\; \mathbb{A}_k \;=\; \mathrm{colim}_S \Big(\prod_{v \in S} k_v \times \prod_{v \notin S} \mathfrak{o}_v \Big)$$

[16.22] Claim: Imbedding k diagonally in $\mathbb{A}_k$, by

$$\alpha \longrightarrow (\ldots, \alpha, \ldots) \;\in\; \mathbb{A}_k$$

the image of k is *discrete*, and the quotient $\mathbb{A}/k$ is *compact*.

Proof: Recall that a *topological group* is a group with a locally-compact Hausdorff topology in which the group operation and inverse are continuous. (Perhaps counter-intuitively, this disqualifies infinite-dimensional topological vectorspaces!) Usually a topological group will have a *countable basis*.

For *abelian* topological group G and (topologically) *closed* subgroup H, the quotient G/H is a topological group. If H were not closed, the quotient would fail to be Hausdorff.

In topological groups G (as in topological vector spaces), to describe a topology it suffices to give a local basis of neighborhoods at the identity $e \in G$: for all $g \in G$, the map $h \to gh$ is continuous (by definition), and has continuous inverse $h \to g^{-1}h$, so is a homeomorphism. Thus, for basis $\{N_j\}$ of neighborhoods of e, $\{gN_j\}$ is a basis of neighborhoods at g.

A sub*set* Y of a topological space X is *discrete* when every point $y \in Y$ has a neighborhood N in X such that $N \cap Y = \{y\}$.

[16.23] Claim: A sub*group* Γ of a topological group G is discrete as a sub*set* if and only if the identity e has a neighborhood N in G such that $N \cap \Gamma = \{e\}$.

Proof: Discreteness certainly implies that e has such a neighborhood. For any other $\gamma \in \Gamma$,

$$\gamma N \cap \Gamma \;=\; \gamma \cdot (N \cap \gamma^{-1}\Gamma) \;=\; \gamma \cdot (N \cap \Gamma) \;=\; \gamma \cdot \{e\} \;=\; \{\gamma\}$$

Thus, every point of Γ is isolated when e is. ///

[16.24] Claim: A discrete sub*group* Γ of G is *closed*. *Note:* A discrete sub*set* need not be closed: $\{\frac{1}{n} : 1 \leq n \in \mathbb{Z}\}$ is discrete in $\mathbb{R}$ but is not closed.

Proof: *(of claim)* Let N be a neighborhood of e in G meeting Γ just at e. By continuity of the group operation and inversion in G, there is a neighborhood U of e such that $U^{-1} \cdot U \subset N$. Suppose $g \notin \Gamma$ were in the closure of Γ in G. Then gU contains two distinct elements γ, δ of Γ. But

$$\gamma^{-1} \cdot \delta \;\in\; (gU)^{-1} \cdot (gU) \;=\; N^{-1} \cdot N \;\subset\; N$$

contradiction. Thus, Γ is closed in G. ///

Returning to proving k is discrete in $\mathbb{A} = \mathbb{A}_k$, it suffices to find a neighborhood N of $0 \in \mathbb{A}$ meeting k just at 0.

To begin, let

$$N_{\text{fin}} \;=\; \prod_{v|\infty} k_v \times \prod_{v<\infty} \mathfrak{o}_v \;=\; \text{open neighborhood of 0 in } \mathbb{A}$$

$N_{\text{fin}} \cap k = \mathfrak{o}$, since requiring local integrality everywhere implies global integrality ($\mathfrak{o}$ is Dedekind). Then it suffices to show that the projection of $\mathfrak{o}$ to $\prod_{v|\infty} k_v = k \otimes_{\mathbb{Q}} \mathbb{R}$ is discrete *there*.

We showed that $\mathfrak{o}$ is a free $\mathbb{Z}$-module of rank $[k:\mathbb{Q}]$, and that a $\mathbb{Z}$-basis $\{e_1, \ldots, e_n\}$ is a $\mathbb{Q}$-basis of k. Because extending scalars preserves free-ness, $\{e_1, \ldots, e_n\}$ is an $\mathbb{R}$-basis of $k \otimes_{\mathbb{Q}} \mathbb{R}$.

This reduces the question to a more classical one: given an $\mathbb{R}$-basis $\{e_1, \ldots, e_n\}$ of an $\mathbb{R}$ vector space V, show that the *lattice* $\Lambda = \bigoplus_j \mathbb{Z}e_j$ is *discrete* in V.

Conveniently, by now we know that a finite-dimensional $\mathbb{R}$-vectorspace has a unique (appropriate) topology, so, by changing coordinates, we can suppose the e_j are the *standard* basis of $\mathbb{R}^n$, so $\Lambda = \mathbb{Z}^n$, and $\mathbb{R}^n$ is given the usual metric topology. Any ball of radius < 1 at 0 meets $\mathbb{Z}^n$ just at 0, proving discreteness.

To show *compactness* of $\mathbb{A}/k$, in a similar fashion: first, show that, given $\alpha \in \mathbb{A}$, there is $x \in k$ such that $\alpha - x \in \prod_{v|\infty} k_v \times \prod_{v<\infty} \mathfrak{o}_v$. Let $0 \neq \ell \in \mathbb{Z}$ such that $\ell\alpha \in \mathfrak{o}_v$ at all $v < \infty$. With $\ell\mathfrak{o} = \prod_j \mathfrak{p}_j^{e_j}$ with $0 < e_j \in \mathbb{Z}$. By Sun-Ze, there is $y \in \mathfrak{o}$ such that $y - \ell\alpha_{\mathfrak{p}_j} \in \mathfrak{p}_j^{e_j} \cdot \mathfrak{o}_{\mathfrak{p}_j}$ for all j. Then $\ell^{-1}y - \alpha$ is locally integral at all finite places, so $x = \ell^{-1}y \in k$ is the desired element.

That is, $\mathbb{A}/k$ has representatives in $\prod_{v|\infty} k_v \times \prod_{v<\infty} \mathfrak{o}_v$. By Tychonoff, the latter is compact.

Again, a $\mathbb{Z}$-basis $\{e_1, \ldots, e_n\}$ of $\mathfrak{o}$ is an $\mathbb{R}$-basis of the real vector space $k_\infty = \prod_{v|\infty} k_v$. Every element of k_∞ has a representative $\sum_j c_j e_j$ with $0 \leq c_j \leq 1$. The collection of such elements is a continuous image (by scalar multiplication and vector addition) of the compact set $[0,1]^n$, so is compact. ///

[16.25] Remark: Recall that $\mathbb{A}_k/k$ is also the **solenoid** $\lim_{\mathfrak{a}} k_\infty/\mathfrak{a}$, the limit taken over non-zero ideals $\mathfrak{a}$ of $\mathfrak{o}$. This gives another proof of the compactness, again by Tychonoff.

17. *More on differents $\mathfrak{d}_{K/k}$ and complementary modules*

Again, for K/k a finite separable extension, with rings of integers $\mathfrak{O}, \mathfrak{o}$ respectively, an $\mathfrak{o}$-module Λ inside K has *complementary module* (over $\mathfrak{o}$)

$$\Lambda^* \;=\; \{\beta \in K \;:\; \text{tr}_{K/k}(\beta \cdot \mathfrak{O}) \subset \mathfrak{o}\}$$

We saw that the complementary lattice to $\mathfrak{O}$ (over $\mathfrak{o}$) is a fractional ideal $\mathfrak{d}_{K/k}^{-1}$. Its inverse is the *different* $\mathfrak{d}_{K/k}$.

[17.1] Remark: There is no general assertion that $(\Lambda^*)^* = \Lambda$.

[17.2] Proposition: The different is *multiplicative in towers*, that is, for finite separable extensions $k \subset K \subset L$, with k the field of fractions of Dedekind $\mathfrak{o}_k$, and for integral closures $\mathfrak{o}_K$ and $\mathfrak{o}_L$ of $\mathfrak{o}_k$ in K and L,

$$\mathfrak{d}_{L/k} \;=\; \mathfrak{d}_{L/K} \cdot \mathfrak{d}_{K/k} \qquad\qquad (\text{for } k \subset K \subset L)$$

Proof: On one hand, the natural step-wise computation

$$\mathrm{tr}_k^L(\mathfrak{d}_{L/K}^{-1}\,\mathfrak{d}_{K/k}^{-1}\,\mathfrak{o}_L) \;=\; (\mathrm{tr}_k^K \circ \mathrm{tr}_K^L)(\mathfrak{d}_{L/K}^{-1}\,\mathfrak{d}_{K/k}^{-1}\,\mathfrak{o}_L) \;=\; \mathrm{tr}_k^K(\mathfrak{d}_{K/k}^{-1} \cdot \mathrm{tr}_K^L(\mathfrak{d}_{L/K}^{-1}\,\mathfrak{o}_L)) \;\subset\; \mathrm{tr}_k^K(\mathfrak{d}_{K/k}^{-1}\,\mathfrak{o}_K) \;\subset\; \mathfrak{o}_k$$

gives $\mathfrak{d}_{L/K}^{-1} \cdot \mathfrak{d}_{K/k}^{-1} \subset \mathfrak{d}_{L/k}^{-1}$. Although $\mathfrak{d}_{K/k}^{-1}$ is not a fractional ideal of $\mathfrak{o}_L$, the containment shows that $\mathfrak{d}_{L/K}^{-1} \cdot \mathfrak{d}_{K/k}^{-1}$ is a sub-module of a finitely-generated module over the Noetherian ring $\mathfrak{o}_L$, so is finitely-generated, so $\mathfrak{d}_{L/K}^{-1} \cdot \mathfrak{d}_{K/k}^{-1}$ is a fractional ideal of $\mathfrak{o}_L$. Multiplying through by the $\mathfrak{o}_L$-ideals $\mathfrak{d}^{L/K}$ and $\mathfrak{d}_{L/k}$ gives

$$\mathfrak{d}_{L/k} \cdot \mathfrak{d}_{K/k}^{-1} \;\subset\; \mathfrak{d}_{L/K}$$

Both sides are $\mathfrak{o}_K$-modules, and multiplying through by the $\mathfrak{o}_K$-ideal $\mathfrak{d}_{K/k}$ gives

$$\mathfrak{d}_{L/k} \;\subset\; \mathfrak{d}_{L/K} \cdot \mathfrak{d}_{K/k}$$

On the other hand,

$$\mathrm{tr}_k^K((\mathrm{tr}_K^L \mathfrak{d}_{L/k}^{-1}) \cdot \mathfrak{o}_K) \;=\; \mathrm{tr}_k^K(\mathrm{tr}_K^L(\mathfrak{d}_{L/k}^{-1} \cdot \mathfrak{o}_K)) \;=\; \mathrm{tr}_k^K(\mathrm{tr}_K^L(\mathfrak{d}_{L/k}^{-1})) \;=\; \mathrm{tr}_k^L(\mathfrak{d}_{L/k}^{-1}) \;\subset\; \mathfrak{o}_k$$

Thus, $\mathrm{tr}_K^L \mathfrak{d}_{L/K}^{-1} \subset \mathfrak{d}_{K/k}^{-1}$. Further,

$$\mathrm{tr}_K^L(\mathfrak{d}_{K/k} \cdot \mathfrak{d}_{L/k}^{-1}) \;=\; \mathfrak{d}_{K/k} \cdot \mathrm{tr}_K^L(\mathfrak{d}_{L/k}^{-1}) \;\subset\; \mathfrak{d}_{K/k} \cdot \mathfrak{d}_{K/k}^{-1} \;=\; \mathfrak{o}_K$$

That is, $\mathfrak{d}_{K/k} \cdot \mathfrak{d}_{L/k}^{-1} \subset \mathfrak{d}_{L/K}^{-1}$. Although $\mathfrak{d}_{K/k}$ is not a fractional ideal in L, the product $\mathfrak{d}_{K/k} \cdot \mathfrak{d}_{L/k}^{-1}$ is contained in the finitely-generated $\mathfrak{o}_L$-module $\mathfrak{d}_{L/K}^{-1}$, and $\mathfrak{o}_L$ is Noetherian, so that product *is* a fractional ideal in L. Multiplying the containment through by the ideal $\mathfrak{d}_{L/k} \cdot \mathfrak{d}_{L/K}$ of $\mathfrak{o}_L$ gives $\mathfrak{d}_{L/K} \cdot \mathfrak{d}_{K/k} \subset \mathfrak{d}_{L/k}$. ///

[17.3] Proposition: The local differents $\mathfrak{d}_{K_\mathfrak{P}/k_\mathfrak{p}}$ for primes $\mathfrak{P}$ lying over primes $\mathfrak{p}$ are related to the global different $\mathfrak{d}_{K/k}$ by

$$\mathfrak{d}_{K/k} \cdot \mathfrak{O}_\mathfrak{P} \;=\; \mathfrak{d}_{K_\mathfrak{P}/k_\mathfrak{p}} \qquad\qquad (\text{for all } \mathfrak{P}/\mathfrak{p})$$

Proof: The global trace from K to k is the sum of all the local traces, in that $k_\mathfrak{p} \otimes_k K \approx \bigoplus_{\mathfrak{P}|\mathfrak{p}} K_\mathfrak{P}$ and with the diagonal copy of K inside that tensor product, for $\alpha \in K$

$$\mathrm{tr}_{K/k}(\alpha) \;=\; \bigoplus_{\mathfrak{P}|\mathfrak{p}} \mathrm{tr}_{K_\mathfrak{P}/k_\mathfrak{p}}(\alpha) \;\in\; K \;\subset\; \bigoplus_{\mathfrak{P}|\mathfrak{p}} K_\mathfrak{P}$$

Thus, on one hand, for $\alpha \in K$ locally integral except possibly at primes over $\mathfrak{p}$, the condition $\mathrm{tr}_{K/k}(\alpha \cdot \mathfrak{O}) \subset \mathfrak{o}$ implies $\mathrm{tr}_{K_\mathfrak{P}/k_\mathfrak{p}}(\alpha \cdot \mathfrak{O}) \subset \mathfrak{o}_\mathfrak{p}$ for all $\mathfrak{P}$ over $\mathfrak{p}$. Thus, $\mathfrak{d}_{K/k}^{-1} \subset \mathfrak{d}_{K_\mathfrak{P}/k_\mathfrak{p}}^{-1}$ with the natural projection of K to the $\mathfrak{P}^{th}$ summand. Letting the local different at $\mathfrak{P}$ be $\mathfrak{P}^m \cdot \mathfrak{O}_\mathfrak{P}$, this gives $\mathfrak{P}^m \subset \mathfrak{d}_{K/k}$ for each $\mathfrak{P}$ over $\mathfrak{p}$.

Conversely, using Sun-Ze, for $\alpha \in \mathfrak{P}^{-m}$ and $\alpha = 0 \bmod \mathfrak{Q}$ for $\mathfrak{Q} \neq \mathfrak{P}$ dividing $\mathfrak{p}$, writing $\mathrm{tr}_{K/k}(\alpha \cdot \mathfrak{O})$ as a direct sum of local traces, it has locally integral $\mathfrak{P}^{th}$-component by definition of the local different, has locally integral $\mathfrak{Q}^{th}$-component for all other primes over $\mathfrak{p}$, and is locally integral everywhere else. Thus, $\mathfrak{P}^{-m} \subset \mathfrak{d}_{K/k}^{-1}$, and $\mathfrak{d}_{K/k} \subset \mathfrak{P}^m$.

Density of K in $k_\mathfrak{p} \otimes_k K$, from the approximation theorem, finishes the argument that the global different's prime factors have exponents equal to the corresponding local differents' exponents. ///

[17.4] **Proposition:** Let $K = k(\alpha)$ be finite separable, with α integral over the integers $\mathfrak{o}$ of k with minimal polynomial $f(x)$ of degree n. With

$$\frac{f(x)}{x-\alpha} \;=\; b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \ldots + b_o$$

the complementary module $\mathfrak{o}[\alpha]^*$ is

$$\mathfrak{o}[\alpha]^* \;=\; \bigoplus_j \frac{b_j}{f'(\alpha)} \cdot \mathfrak{o}$$

Proof: We claim that

$$\sum_{\beta : f(\beta)=0} \frac{f(x)}{x-\beta} \cdot \frac{\beta^j}{f'(\beta)} \;=\; X^j \qquad\qquad (\text{for } 0 \le j \le n-1)$$

Indeed, both sides are of degree at most $n-1$, and agree on the n distinct zeros β of $f(x)$. The summands are coefficient-wise conjugate to each other, so

$$(\text{coefficient-wise})\,\mathrm{tr}_{K/k}\Big(\frac{f(x)}{x-\varpi} \cdot \frac{\backslash alf^j}{f'(\alpha)}\Big) \;=\; X^j$$

Equating i^{th} coefficients in the last polynomial identity,

$$\mathrm{tr}_{K/k}\Big(b_i \cdot \frac{\alpha^j}{f'(\alpha)}\Big) \;=\; \begin{cases} 1 & (\text{when } i=j) \\ 0 & (\text{when } i \ne j) \end{cases}$$

proving the lemma. ///

[17.5] **Corollary:** For $\mathfrak{P}/\mathfrak{p}$ *unramified* in a finite separable extension K/k, the different $\mathfrak{d}_{K/k}$ is *not* divisible by $\mathfrak{P}$.

Proof: By the comparison of local and global differents, it suffices to treat the case that k is *complete* with respect to the $\mathfrak{p}$-adic metric, and $\mathfrak{P} = \mathfrak{p} \cdot \mathfrak{O}$.

Let $\alpha \in \mathfrak{O}$ generating the residue class field extension $\mathfrak{O}/\mathfrak{P}$ of $\mathfrak{o}/\mathfrak{p}$, satisfying $f(\alpha) = 0$ for irreducible monic $f(x) \in \mathfrak{o}[x]$. We have seen that the separability of K/k implies that of the residue class field extension, so $f(x)$ mod $\mathfrak{p}$ is separable, so $\alpha - \beta \notin \mathfrak{P}$ for all pairs of distinct roots α, β of $f(x) = 0$. Thus, $f'(\alpha)$ is a *unit*. By the last proposition, $\mathfrak{o}[\alpha]^*$ is contained in $\mathfrak{o}[\alpha] \cdot \frac{1}{f'(\alpha)} = \mathfrak{o}[\alpha]$. Thus, $\mathfrak{o}[\alpha] \subset \mathfrak{O}$ gives

$$\mathfrak{O} \;\subset\; \mathfrak{d}_{K/k}^{-1} \;=\; \mathfrak{O}^* \;\subset\; \mathfrak{o}[\alpha]^* \;\subset\; \mathfrak{o}[\alpha] \cdot \frac{1}{f'(\alpha)} \;=\; \mathfrak{o}[\alpha] \;\subset\; \mathfrak{O}$$

proving that the different is trivial. ///

[17.6] **Corollary:** For $K = k(\alpha)$ with α integral over $\mathfrak{o}$ and irreducible monic $f(x) \in \mathfrak{o}[x]$, the only possible primes ramifying in K/k are those dividing $f'(\alpha)$.

Proof: From

$$\mathfrak{d}_{K/k}^{-1} \;=\; \mathfrak{O}^* \;\subset\; \mathfrak{o}[\alpha]^* \;\subset\; \mathfrak{o}[\alpha] \cdot \frac{1}{f'(\alpha)} \;\subset\; \mathfrak{O} \cdot \frac{1}{f'(\alpha)}$$

we find $\mathfrak{O} \cdot f'(\alpha) \subset \mathfrak{d}_{K/k}$, that is, $\mathfrak{d}_{K/k}$ divides $f'(\alpha)$. ///

[17.7] **Corollary:** For $\mathfrak{P}/p$ *totally* ramified in finite separable K/k, with $\mathfrak{P} = \varpi \cdot \mathfrak{O}$ *principal*, and with no other primes ramifying in K/k, we have $\mathfrak{O} = \mathfrak{o}[\varpi]$.

Proof: First consider k *complete* with respect to the $\mathfrak{p}$-adic metric. Since the residue class field extension is trivial, given $\alpha \in \mathfrak{O}$, there is $\alpha_1 \in \mathfrak{O}$ such that $\alpha - \alpha_1\varpi \in \mathfrak{o}$. That is, there is $a_o \in \mathfrak{o}$ such that $\alpha - a_o = \alpha_1\varpi \in \mathfrak{P}$. Continuing inductively, using the completeness, there are $a_i \in \mathfrak{o}$ such that α is a convergent infinite sum $\alpha = \sum_{i\geq 0} a_i\varpi^i$. Since ϖ is integral over $\mathfrak{o}$, the infinite sum can be rewritten as a polynomial with coefficients in $\mathfrak{o}$, so $\mathfrak{O} = \mathfrak{o}[\varpi]$.

The latter equality implies that $\mathfrak{O}^* = \mathfrak{o}[\varpi]^*$ and, by the proposition above, the different is generated by $f'(\varpi)$, where f is the irreducible monic in $\mathfrak{o}[x]$ of which ϖ is a zero.

Returning to the not-necessarily-complete situation: since no other primes ramify in K/k, no other primes divide the different, so $\mathfrak{d}_{K/k}$ is completely determined by its $\mathfrak{P}$-component, which has the same order at $\mathfrak{P}$ as the local different $\mathfrak{d}_{K_\mathfrak{P}/k_\mathfrak{p}}$. This order is the order of $f'(\varpi)$, since $\mathfrak{O}_\mathfrak{P} = \mathfrak{o}_\mathfrak{p}[\varpi]$. Thus, because no other primes interfere, $\mathfrak{d}_{K/k} = f'(\varpi)\cdot\mathfrak{O}$. From

$$\frac{1}{f'(\varpi)}\cdot\mathfrak{O} \;=\; \mathfrak{d}_{K/k}^{-1} \;=\; \mathfrak{O}^* \;\subset\; \mathfrak{o}[\varpi]^* \;\subset\; \frac{1}{f'(\varpi)}\cdot\mathfrak{O}$$

all these inclusions are equalities, and $\mathfrak{O} = \mathfrak{o}[x]$. ///

Recall that two algebraic field extensions K, E of a field k are *linearly disjoint* over k when $K \otimes_k E$ is a *field*. Equivalently, for any imbedded copies of K, E in an algebraic extension Ω of k, the compositum KE has degree over k equal to the product $[K : k]\cdot[E : k]$.

[17.8] Proposition: Let K, E be linearly disjoint finite separable extensions of k inside a larger field, with rings of algebraic integers $\mathfrak{o}_K, \mathfrak{o}_E$. Suppose that the ring of integers $\mathfrak{o}_k$ of k is a *principal ideal domain.* Suppose that the differents $\mathfrak{d}_{K/k}$ and $\mathfrak{d}_{E/k}$ are relatively prime. Then the ring of integers $\mathfrak{o}_{KE}$ of the compositum KE is $\mathfrak{o}_K \otimes_{\mathfrak{o}_k} \mathfrak{o}_E$.

Proof: By multiplicativity of differents in towers,

$$\mathfrak{d}_{KE/K}\cdot\mathfrak{d}_{K/k} \;=\; \mathfrak{d}_{KE/E}\cdot\mathfrak{d}_{E/k} \qquad\qquad \text{(as ideals in } \mathfrak{o}_{KE})$$

The relative primality assumption gives

$$\mathfrak{d}_{KE/K} \;=\; \mathfrak{d}_{E/k}\cdot\mathfrak{o}_{KE} \qquad \text{and} \qquad \mathfrak{d}_{KE/E} \;=\; \mathfrak{d}_{K/k}\cdot\mathfrak{o}_{KE}$$

and

$$\mathfrak{d}_{KE/K}^{-1} \;=\; \mathfrak{d}_{E/k}^{-1}\cdot\mathfrak{o}_{KE} \qquad \text{and} \qquad \mathfrak{d}_{KE/E}^{-1} \;=\; \mathfrak{d}_{K/k}^{-1}\cdot\mathfrak{o}_{KE}$$

Thus,

$$\mathfrak{d}_{E/k}^{-1}\otimes_{\mathfrak{o}_k}\mathfrak{o}_K \;\subset\; \mathfrak{d}_{E/k}^{-1}\cdot\mathfrak{o}_{KE} \;=\; \mathfrak{d}_{E/k}^{-1}\cdot\mathfrak{o}_{KE} \;=\; \mathfrak{d}_{KE/K}^{-1}$$

Taking complementary $\mathfrak{o}_K$-modules reverses the inclusion, and certainly $\mathfrak{o}_{KE} \subset ((\mathfrak{o}_{KE})^*)^* = (\mathfrak{d}_{KE/K}^{-1})^*$, whether or not we have equality, so

$$\mathfrak{o}_{KE} \;\subset\; (\mathfrak{d}_{KE/K}^{-1})^* \;\subset\; \big(\mathfrak{d}_{E/k}^{-1}\otimes_{\mathfrak{o}_k}\mathfrak{o}_K\big)^*$$

To compute the complementary module $(\mathfrak{d}_{E/k}^{-1}\otimes_{\mathfrak{o}_k}\mathfrak{o}_K)^*$ over $\mathfrak{o}_K$, let $\{\alpha_i\}$ be an $\mathfrak{o}_k$-basis for $\mathfrak{d}_{E/k}^{-1}$ and $\{\beta_j\}$ an $\mathfrak{o}_k$-basis for $\mathfrak{o}_K$, and $\{\alpha_i^*\}$ a dual $\mathfrak{o}_k$-basis with respect to $\mathrm{tr}_{E/k}$. For $\sum_{ij} A_{ij}\,\alpha_i\otimes\beta_j$ to be in $(\mathfrak{d}_{E/k}^{-1}\otimes_{\mathfrak{o}_k}\mathfrak{o}_K)^*$ for $A_{ij}\in k$ requires that for all ℓ,

$$\mathrm{tr}_{KE/K}\Big((\alpha_\ell^*\otimes 1)\cdot\sum_{ij} A_{ij}\alpha_i\otimes\beta_j\Big) \;\in\; \mathfrak{o}_K$$

Compute

$$\mathrm{tr}_{KE/K}\Big((\alpha_\ell^*\otimes 1)\cdot\sum_{ij} A_{ij}\alpha_i\otimes\beta_j\Big) \;=\; \mathrm{tr}_{KE/K}\Big(\sum_{ij} A_{ij}\alpha_\ell^*\alpha_i\otimes\beta_j\Big) \;=\; \sum_{ij} A_{ij}\mathrm{tr}_{KE/K}(\alpha_\ell^*\alpha_i)\otimes\beta_j$$

$$= \sum_{ij} A_{ij}\mathrm{tr}_{E/k}(\alpha_\ell^* \alpha_i) \otimes \beta_j \;=\; \sum_j A_{\ell,j}\, 1 \otimes \beta_j \;=\; \sum_j A_{\ell,j}\beta_j$$

Since $\{\beta_j\}$ is a $\mathfrak{o}_k$-basis for $\mathfrak{o}_K$, this requires that all $A_{\ell,j}$ are in $\mathfrak{o}_k$. That is,

$$\mathfrak{o}_{KE} \;\subset\; (\mathfrak{d}_{KE/K}^{-1})^* \;\subset\; \Big(\mathfrak{d}_{E/k}^{-1} \otimes_{\mathfrak{o}_k} \mathfrak{o}_K\Big)^* \;=\; \mathfrak{o}_E \otimes_{\mathfrak{o}_k} \mathfrak{o}_K$$

as claimed. ///

18. *Example: cyclotomic extensions of* $\mathbb{Q}$

[18.1] Theorem: The ring of algebraic integers $\mathfrak{o}$ in $k = \mathbb{Q}[\omega]$, where ω is a primitive n^{th} root of unity, is $\mathbb{Z}[\omega]$. The only primes ramified are those dividing n. For prime powers $n = p^m$, the prime p is *totally* ramified, that is, has ramification degree $(p-1)p^{m-1}$, the field extension degree.

Proof: First consider prime powers $n = p^m$ with $m > 1$ and $p > 2$. Let $\omega = \omega_{p^m}$ be a primitive p^{mth} root of unity. Recall the p^{mth} cyclotomic polynomial

$$\Phi_{p^m}(x) \;=\; \frac{x^{p^m} - 1}{x^{p^{m-1}} - 1} \;=\; \Phi_p(x^{p^{m-1}}) \;=\; (x^{p^{m-1}})^{p-1} + (x^{p^{m-1}})^{p-2} + \ldots + x^{p^{m-1}} + 1$$

Thus, it suffices to prove that $\Phi_p(x)$ is irreducible in $\mathbb{Q}[x]$ by Eisenstein's criterion. Replacing x by $x+1$,

$$\Phi_p(x+1) \;=\; \frac{(x+1)^p - 1}{x} \;=\; \frac{x^p + px^{p-1} + \ldots + \binom{p}{2}x^2 + px}{x} \;=\; x^{p-1} + px^{p-2} + \ldots + \binom{p}{2}x + p$$

Since the inner binomial coefficients $\binom{p}{i}$ are divisible by p, Eisenstein's criterion applies. And, then the Newton polygon criterion shows that the extension is *totally ramified* over p, with $\omega - 1$ generating the prime $\mathfrak{P}$ over p. From the discussion of *differents* and complementary modules in the previous section, only primes dividing $\Phi_n'(\omega)$ can ramify.

$$\Phi_{p^m}(x)' \;=\; \Phi_p(x^{p^{m-1}})' \;=\; p^{m-1} \cdot \Phi_p'(x^{p^{m-1}})$$

Since $\alpha = \omega^{p^{m-1}}$ is a primitive p^{th} root of unity,

$$\Phi_p'(\alpha) \;=\; \prod_{\beta^p=1,\, \beta\neq 1,\, \beta\neq\alpha} (\alpha - \beta) \;=\; \prod_{2\le j\le p-2} (\alpha - \alpha^j)$$

Thus, $\Phi_{p^m}'(\omega)$ is divisible by no other primes than $\mathfrak{P}$, so no primes other than $\mathfrak{P}/p$ ramify in $\mathbb{Q}(\omega)/\mathbb{Q}$. Since $\mathfrak{P}$ is *principal*, generated by $\omega - 1$, the corollary of the last section determines the ring of algebraic integers in $\mathbb{Q}(\omega)$:

$$\text{(algebraic integers in } \mathbb{Q}(\omega)) \;=\; \mathbb{Z}[\omega - 1] \;=\; \mathbb{Z}[\omega] \qquad\qquad \text{(at least for prime power orders)}$$

For composite n and n^{th} root of unity $\omega = \omega_n$, the multiplicativity of ramification in towers shows that the only primes ramified in $\mathbb{Q}(\omega)/\mathbb{Q}$ are those dividing n. Indeed, by induction on the number ℓ of distinct prime factors of $n = p_1^{m_1} \ldots p_\ell^{m_\ell}$, letting $n' = p_1^{m_1} \ldots p_{\ell-1}^{m_{\ell-1}}$, every prime lying over p_ℓ has ramification degree in $\mathbb{Q}(\omega_n)/\mathbb{Q}(\omega_{n'})$ equal to the ramification degree of p in $\mathbb{Q}(\omega_{p_\ell^{m_\ell}})/\mathbb{Q}$. Thus, the degree of $\mathbb{Q}(\omega_n)/\mathbb{Q}$ is the product of the degrees of the extensions $\mathbb{Q}(\omega_{p_i^{m_i}})/\mathbb{Q}$. Incidentally, this proves the *irreducibility* over $\mathbb{Q}$ of the n^{th} cyclotomic polynomial.

By induction on the number of prime factors, for coprime m, n, the *differents* of the two extensions $\mathbb{Q}(\omega_m)/\mathbb{Q}$ and $\mathbb{Q}(\omega_n)/\mathbb{Q}$ are relatively prime, so the last proposition of the previous section shows that the ring of algebraic integers in $\mathbb{Q}(\omega_{mn})$ is $\mathbb{Z}[\omega_m]\cdot\mathbb{Z}[\omega_n]$. Since ω_{mn} is a monomial in ω_m and ω_n, the ring of algebraic integers is $\mathbb{Z}[\omega_{mn}]$. ///

19. *Kummer, Eisenstein, Gauss sums, Lagrange resolvents*

Results of Kummer and Eisenstein allow computation of Lagrange resolvents for roots of unity. Everything here has been known for 160+ years.

Roots of unity are abelian over $\mathbb{Q}$, so by Galois theory are expressible in radicals. Expressions in radicals are obtained via *Lagrange resolvents*, in this case Gauss sums.

Evaluation of squares of quadratic Gauss sums shows that the quadratic subfield of the field $\mathbb{Q}(\zeta)$ obtained by adjoining a p^{th} root of unity ζ to $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{p\cdot(-1/p)_2})$, for p odd.

In fact, [Eisenstein 1850] evaluated cubes and fourth powers of Gauss sums attached to cubic and quartic characters to prove the corresponding reciprocity laws. One essential point is the p-adic approximation of Gauss sums by [Kummer 1847], generalized in [Stickelberger 1890]. Since the rings of algebraic integers generated by third or fourth roots of unity have class number one and finitely-many units, cubic (and sextic) and quartic subfields of cyclotomic fields are easily expressible in radicals, via Lagrange resolvents.

More generally, when a prime p splits into *principal* ideals in $\mathbb{Z}[\omega]$ with ω an m^{th} root of unity with $m|(p-1)$, this process systematically produces Lagrange resolvents for the unique degree m subfield of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$, with ζ a p^{th} root of unity. Ramification-theory suggests a qualitative conclusion of this sort, but falls short. Namely, by Kummer theory, a cyclic extension of degree m dividing $p-1$ over a groundfield with m^{th} roots of unity is obtained by adjoining m^{th} roots of an element ξ in the groundfield. Considering ramification, since the only primes ramifying in $\mathbb{Q}(\omega,\zeta_p)$ over $\mathbb{Q}(\omega)$ are primes lying over p, the prime factorization of ξ should not include any primes other than those lying over p. However, there is no indication about avoiding ramification at primes dividing m. Since p splits completely in an extension of $\mathbb{Q}$ by m^{th} roots of unity, there are many inequivalent choices of products of the primes lying over p. Even when the prime factors are determined, there is ambiguity by *units*.

The expressions for resolvents for degree-m subfields of $\mathbb{Q}(\zeta)$ inevitably involve auxiliary m^{th} roots of unity ρ, so are literal expressions in the larger field $\mathbb{Q}(\zeta,\rho)$. However, the resolvents do lie in the degree-m subfield of $\mathbb{Q}(\zeta)$. This is a more general instance of the minor scandal from the Renaissance, that the radical expression for roots of cubics involved complex numbers (cube roots of unity), even when the cubic had three real roots.

Our expression for the m^{th} power of a Gauss sum of an order m character contains a root of unity which we determine numerically in examples. The argument of Gauss sums is more serious: the quadratic case was a difficult result of Gauss, and the cubic case was treated relatively recently treated by [Heath-Brown Patterson 1979].

None of what is done here would have surprised Kummer, Eisenstein, nor Gauss circa 1850. It might not have surprised Lagrange in 1770, nor Vandermonde. Our principal advantage is the post-Dedekind, post-Noether conception of abstract algebra, which removes conceptual difficulties from the Kummer-Eisenstein computations, but otherwise adds little. [1]

[19.1] Solving cyclic equations by Lagrange resolvents

The introduction of resolvents in [Lagrange 1770] considerably predates Ruffini, Abel, and Galois.

Let k be a field and K a *cyclic* extension with Galois group G of order n prime to the characteristic. Assume

[1] [O'Connor-Robertson 2001] notes that Kronecker claimed in 1888 that modern algebra began with the first (1771) paper of Vandermonde, and that Cauchy states that Vandermonde had priority over Lagrange for the remarkable idea of permutations of roots.

that k contains n^{th} roots of unity. Given $\theta \in K$ and a character $\alpha : G \to k^\times$, the *Lagrange resolvent* is an average in K:

$$R \;=\; R(\alpha,\theta) \;=\; \sum_{g\in G} \alpha(g)\, g(\theta)$$

By design, $h(R) = \alpha(h^{-1}) \cdot R$ for $h \in G$. Since G is cyclic of order n, necessarily $\alpha^n = 1$, and for $h \in G$,

$$h(R^n) \;=\; \alpha(h^{-1})^n \cdot R^n \;=\; R^n$$

Thus, $R(\alpha,\theta)^n \in k$, since it is Galois-invariant. For α of order m, $R(\alpha,\theta)^m \in k$, for the same reason.

Since G is cyclic, the group of characters α is cyclic. Fix a generator χ, and fix a generator g for G. The element θ is expressible in terms of the collection of resolvents $R(\chi^\ell,\theta)$, using the invertibility of the Vandermonde matrix

$$V_\chi \;=\; \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ \chi(g^0) & \chi(g^1) & \chi(g^2) & \ldots & \chi(g^{n-1}) \\ \chi^2(g^0) & \chi^2(g^1) & \chi^2(g^2) & \ldots & \chi^2(g^{n-1}) \\ \vdots & & & & \vdots \\ \chi^{n-1}(g^0) & \chi^{n-1}(g^1) & \chi^{n-1}(g^2) & \ldots & \chi^{n-1}(g^{n-1}) \end{pmatrix}$$

The Vandermonde matrix V_χ is explicitly invertible:

$$V_\chi \cdot V_{\chi^{-1}}^\top \;=\; n \cdot 1_n$$

From

$$\begin{pmatrix} R(\chi^0,\theta) \\ R(\chi^1,\theta) \\ R(\chi^2,\theta) \\ \vdots \\ R(\chi^{n-1},\theta) \end{pmatrix} \;=\; V_\chi \cdot \begin{pmatrix} g^0(\theta) \\ g^1(\theta) \\ g^2(\theta) \\ \vdots \\ g^{n-1}(\theta) \end{pmatrix}$$

we have

$$\begin{pmatrix} g^0(\theta) \\ g^1(\theta) \\ g^2(\theta) \\ \vdots \\ g^{n-1}(\theta) \end{pmatrix} \;=\; \frac{1}{n} \cdot V_{\chi^{-1}}^\top \cdot \begin{pmatrix} R(\chi^0,\theta) \\ R(\chi^1,\theta) \\ R(\chi^2,\theta) \\ \vdots \\ R(\chi^{n-1},\theta) \end{pmatrix}$$

Then

$$\theta \;=\; g^0(\theta) \;=\; \frac{1}{n} \cdot \big(R(\chi^0,\theta) + R(\chi^1,\theta) + \ldots + R(\chi^{n-1},\theta)\big)$$

Expressing each $R(\chi^\ell,\theta)^n$ in terms of the coefficients of the irreducible for θ over k yields the expression for θ in radicals.

For cyclotomic extensions, *Lagrange resolvents are Gauss sums*: let $\theta = \zeta$ be a p^{th} root of unity, ω a $(p-1)^{th}$ root of unity, $k = \mathbb{Q}(\omega)$, $K = \mathbb{Q}(\zeta,\omega)$, $\psi(a) = \zeta^a$, identify $\mathrm{Gal}(K/k)$ with $(\mathbb{Z}/p)^\times$ by $\sigma_a(\zeta) = \zeta^a$. Then

$$R(\alpha,\zeta) \;=\; \sum_{a\in(\mathbb{Z}/p)^\times} \alpha(a)\,\sigma_a(\zeta) \;=\; \sum_{a\in(\mathbb{Z}/p)^\times} \alpha(a)\,\psi(a) \;=\; (\text{Gauss sum attached to } \alpha,\psi)$$

For $m|(p-1)$, for a multiplicative character α of order m, the Gauss sum $\gamma(\alpha)$ is a Lagrange resolvent for a generator for the unique degree m subfield of $\mathbb{Q}(\zeta,\omega)$ over $\mathbb{Q}(\omega)$. The values of α often generate a smaller field $\mathbb{Q}(\alpha)$ than $\mathbb{Q}(\omega)$, and then $0 \neq \gamma(\alpha)^m \in \mathbb{Q}(\alpha)$. When such an m^{th} power can be evaluated in useful terms, generators for subfields are expressible in terms of radicals.

[19.2] Kummer's approximation of Gauss sums

For a multiplicative character α on $(\mathbb{Z}/p)^\times$ and an additive character ψ on $\mathbb{Z}/p$, the corresponding Gauss sum is

$$\gamma(\alpha) \;=\; \sum_a \alpha(a)\,\psi(a)$$

We recall [Kummer 1847]'s (see [Cohen 2007] p. 155) and [Stickelberger 1890]'s by-now standard $\mathfrak{P}$-adic approximation. A key point is expression of the given character as a power of the *Kummer (-Teichmüller)* [2] *character*. This approximation determines the prime factorization of $\gamma(\alpha)$, as recalled just below.

Let p be a prime, $\zeta = \zeta_p$ a p^{th} root of unity in an extension of $\mathbb{Q}$. The prime lying over p in $\mathbb{Z}[\zeta]$ is generated by $\zeta - 1$. Specify an additive character ψ on $\mathbb{Z}/p$ by

$$\psi(a) \;=\; \zeta^a \qquad\qquad (\text{for } a \in \mathbb{Z}/p)$$

The choice of ζ and the corresponding character ψ will be fixed throughout, and will be suppressed from the notation. Let $\omega = \omega_{p-1}$ be a primitive $(p-1)^{th}$ root of unity. Let $\mathfrak{q}$ be one of the primes lying over p in $\mathbb{Z}[\omega]$, noting that p splits completely in $\mathbb{Z}[\omega]$. Let $\mathfrak{P}$ be the prime lying over $\mathfrak{q}$ in $\mathbb{Z}[\zeta,\omega]$: at all primes over p, the extension $\mathbb{Z}[\zeta,\omega]/\mathbb{Z}[\omega]$ is *totally ramified*. Since p splits completely in $\mathbb{Z}[\omega]$, the inclusion of residue class fields $\mathbb{Z}/p \longrightarrow \mathbb{Z}[\omega]/\mathfrak{q}$ is an *isomorphism*. This isomorphism identifies the images of the $(p-1)^{th}$ roots of unity in the quotient $\mathbb{Z}[\omega]/\mathfrak{q}$ with the cyclic group $(\mathbb{Z}/p)^\times$. For a choice of $\mathfrak{q}$ lying over p, the corresponding *Kummer (-Teichmüller) character* [3]

$$\chi \;=\; \chi_{\mathfrak{q}} \;:\; (\mathbb{Z}/p)^\times \;\longrightarrow\; \mathbb{Z}[\omega]^\times$$

is

$$\chi(a) \;=\; \chi_{\mathfrak{q}}(a) \;=\; a \bmod \mathfrak{q} \qquad\qquad (\text{for } a \in (\mathbb{Z}/p)^\times, \text{ fixed } \mathfrak{q} \text{ in } \mathbb{Z}[\omega] \text{ over } p)$$

Since $(\mathbb{Z}/p)^\times$ is cyclic, every character is a power of the Kummer (-Teichmüller) character. In any case, all Gauss sums $\gamma(\chi^{-n})$ lie in $\mathbb{Z}[\omega,\zeta]$.

[19.3] Proposition: *(Kummer)*

$$\frac{\gamma(\chi_{\mathfrak{q}}^{-n})}{(\zeta-1)^n} \;=\; \frac{-1}{n!} \bmod \mathfrak{P} \qquad\qquad (\text{with } \mathfrak{P} \text{ over } \mathfrak{q})$$

Proof: The first and clearest example of Kummer's approximation is that of the Gauss sum attached to the inverse of the Kummer (-Teichmüller) character χ itself,

$$\gamma(\chi^{-1}) \;=\; \sum_{a\in(\mathbb{Z}/p)^\times} \psi(a)\,\chi^{-1}(a)$$

First, recalling that $(\zeta-1)\mathbb{Z}[\zeta]$ lies under $\mathfrak{P}$,

$$\sum_{a\in(\mathbb{Z}/p)^\times} \chi^{-1}(a)\,\psi(a) \;=\; \sum_{a\in(\mathbb{Z}/p)^\times} \chi^{-1}(a)\,(1+\zeta-1)^a$$

$$=\; \sum_{a\in(\mathbb{Z}/p)^\times} \chi^{-1}(a)\,(1+a(\zeta-1)) \bmod \mathfrak{P}^2 \;=\; (\zeta-1)\sum_{a\in(\mathbb{Z}/p)^\times} a\,\chi^{-1}(a)$$

[2] The character nowadays named after Teichmüller was used by Kummer 80 years earlier.

[3] See below for *existence* of this character. Some sources normalize $\chi(a) = a^{-1} \bmod \mathfrak{q}$. The choice of a or a^{-1} is inessential.

since $\sum_a \chi^{-1}(a) = 0$. Thus,

$$\frac{\gamma(\chi^{-1})}{\zeta - 1} \;=\; \sum_{a \in (\mathbb{Z}/p)^\times} a\,\chi^{-1}(a) \bmod \mathfrak{P} \;=\; \sum_{a \in (\mathbb{Z}/p)^\times} a\,a^{-1} \bmod \mathfrak{P} \;=\; p - 1 \bmod \mathfrak{P} \;=\; -1 \bmod \mathfrak{P}$$

That is,

$$\frac{\gamma(\chi^{-1})}{\zeta - 1} \;=\; -1 \bmod \mathfrak{P}$$

The general case is obtained from this by induction, as follows. Start from the elementary relation among Gauss sums and Jacobi sums:

$$\gamma(\alpha)\,\gamma(\beta) \;=\; \gamma(\alpha\beta) \cdot \sum_{b \neq 0,1} \alpha(b)\,\beta(1-b) \qquad \text{(for } \alpha\beta \neq 1\text{)}$$

Expressing α, β in terms of the Kummer (-Teichmüller) character, $\alpha = \chi^{-m}$ and $\beta = \chi^{-n}$, the Jacobi sum $\sum \alpha(b)\,\beta(1-b)$ can be evaluated modulo $\mathfrak{P}$, producing a result resembling a beta function, as follows. With equalities modulo $\mathfrak{q}$,

$$\sum_{b \neq 0,1} \chi^{-m}(b)\,\chi^{-n}(1-b) \;=\; \sum_{b \neq 0,1} b^{-m}\,(1-b)^{-n} \;=\; \sum_{b \neq 0} b^{-m}\,(1-b)^{-n} \qquad \text{(all equalities mod } \mathfrak{q}\text{)}$$

The sum over b now *does* include 1. Modulo $\mathfrak{q}$,

$$= \sum_{b \neq 0} b^{-m}\,(1-b)^{(p-1)-n} \;=\; \sum_{j=0}^{p-1-n} \sum_{b \neq 0} b^{-m} \binom{p-1-n}{j} (-1)^j\, b^j \qquad \text{(all equalities mod } \mathfrak{q}\text{)}$$

$$= \sum_{j=0}^{p-1-n} \binom{p-1-n}{j} (-1)^j \sum_{b \neq 0} b^{j-m} \qquad \text{(mod } \mathfrak{q}\text{)}$$

The inner sum over b is 0 unless $j - m = 0$, in which case it is $p - 1$, since $b \to b^{j-m}$ is a character mod p. Thus, modulo $\mathfrak{q}$,

$$\sum_b \chi^{-m}(b)\,\chi^{-n}(1-b) \;=\; \binom{p-1-n}{m} (-1)^m (p-1) \;=\; \binom{p-1-n}{m} (-1)^{m+1} \bmod \mathfrak{q}$$

For $m = 1$ and replacing n by $n - 1$, the Jacobi sum is approximated $\mathfrak{q}$-adically by

$$\sum_b \chi^{-1}(b)\,\chi^{-(n-1)}(1-b) \;=\; \binom{p-1-(n-1)}{1} \bmod \mathfrak{q} \;=\; p-1-(n-1) \;=\; -n \bmod \mathfrak{q}$$

Going back to the elementary relation relating Gauss sums and Jacobi sums,

$$\gamma(\chi^{-1}) \cdot \gamma(\chi^{-(n-1)}) \;=\; -n \cdot \gamma(\chi^{-n}) \bmod \mathfrak{P}$$

or

$$\gamma(\chi^{-n}) \;=\; \frac{\gamma(\chi^{-1}) \cdot \gamma(\chi^{-(n-1)})}{-n} \bmod \mathfrak{P}$$

Induction gives Kummer's result

$$\frac{\gamma(\chi^{-n})}{(\zeta-1)^n} \;=\; \frac{\gamma(\chi^{-1})}{\zeta - 1} \cdot \frac{\gamma(\chi^{-(n-1)})}{(\zeta-1)^{n-1}} \cdot \frac{1}{\sum_b \chi^{-1}(b)\,\chi^{-(n-1)}(1-b)} \;=\; (-1) \cdot \frac{-1}{(n-1)!} \cdot \frac{1}{-n} \;=\; \frac{-1}{n!} \bmod \mathfrak{P}$$

[19.4] Galois equivariance and prime factorizations

Galois equivariance of Kummer's estimate is straightforward, and determines the prime ideal factorization of Gauss sums.

Rewrite Kummer's result as

$$\frac{\gamma(\chi_{\mathfrak{P}}^{-n})}{(\zeta-1)^n} + \frac{1}{n!} \;\in\; \mathfrak{P}$$

A Galois automorphism of $\mathbb{Q}(\omega,\zeta)$ over $\mathbb{Q}(\zeta)$ does not change ζ and does not change the character $\psi(a)=\zeta^a$, so the effect of σ on a Gauss sum $\gamma(\alpha)$ is only via α, namely,

$$\sigma\big(\gamma(\alpha)\big) \;=\; \sigma\big(\sum_a \alpha(a)\,\psi(a)\big) \;=\; \sum_a \sigma\big(\alpha(a)\big)\,\psi(a)\big) \;=\; \gamma(\sigma\alpha)$$

This gives the obvious Galois equivariance

$$\frac{\gamma(\sigma\chi_{\mathfrak{P}}^{-n})}{(\zeta-1)^n} + \frac{1}{n!} \;\in\; \sigma\mathfrak{P}$$

The Kummer (-Teichmüller) characters attached to primes $\mathfrak{q}$ or $\mathfrak{P}$ over p has a visible Galois equivariance: applying σ to the relation $\chi_{\mathfrak{P}}(a)-a\in\mathfrak{P}$ gives

$$\sigma\chi_{\mathfrak{P}}(a)-a \;\in\; \sigma\mathfrak{P} \qquad\qquad (\text{for } a\in(\mathbb{Z}/p)^\times)$$

For $b\in(\mathbb{Z}/(p-1))^\times$, let σ_b be the automorphism

$$\sigma_b\omega \;=\; \omega^b \qquad\quad \sigma_b\zeta \;=\; \zeta \qquad\qquad (\text{for } b\in(\mathbb{Z}/(p-1))^\times)$$

Then

$$\chi_{\mathfrak{P}}^b(a)-a \;=\; \sigma_b\chi_{\mathfrak{P}}(a)-a \;\in\; \sigma_b\mathfrak{P} \qquad\qquad (\text{for } a\in(\mathbb{Z}/p)^\times,\ b\in(\mathbb{Z}/(p-1))^\times)$$

That is,

$$\chi_{\sigma_b\mathfrak{P}} \;=\; \chi_{\mathfrak{P}}^b \qquad\qquad (\text{for } b\in(\mathbb{Z}/(p-1))^\times)$$

Since $\zeta-1$ splits completely in $\mathbb{Z}[\omega,\zeta]$ over $\mathbb{Z}[\zeta]$,

$$\mathrm{ord}_{\sigma_b\mathfrak{P}}(\zeta-1) \;=\; 1 \qquad\qquad (\text{for all } b \text{ prime to } p-1)$$

From Kummer's estimate,

$$\mathrm{ord}_{\mathfrak{P}}\,\gamma(\chi_{\sigma_b\mathfrak{P}}^{-1}) \;=\; \mathrm{ord}_{\mathfrak{P}}\,\gamma(\chi_{\mathfrak{P}}^{-b}) \;=\; b \qquad\qquad (\text{for } b\in(\mathbb{Z}/(p-1))^\times)$$

Likewise,

$$\mathrm{ord}_{\sigma_b\mathfrak{P}}\,\gamma(\chi_{\mathfrak{P}}^{-1}) \;=\; b^{-1} \mod p-1$$

For arbitrary n, the same argument gives

$$\mathrm{ord}_{\sigma_b\mathfrak{P}}\,\gamma(\chi_{\mathfrak{P}}^{-n}) \;=\; b^{-1}n \mod p-1 \qquad\qquad (\text{with } b^{-1}n \text{ in the range } 0,1,2,\ldots,p-2)$$

Scine $\gamma(\chi^{-n})\cdot\gamma(\chi^n)=\chi^n(-1)\cdot p$, no primes other than those lying above p divide these Gauss sums, so we have the prime ideal factorization in $\mathbb{Z}[\omega_{p-1},\zeta_p]$.

Galois equivariance shows that the $(p-1)^{th}$ power of $\gamma(\chi_{\mathfrak{P}}^{-1})$ lies in $\mathbb{Z}[\omega]$. The prime $\mathfrak{P}$ is totally ramified over the prime $\mathfrak{q}$ under it in $\mathbb{Z}[\omega]$, of degree $p-1$, so

$$\mathrm{ord}_{\sigma_b\mathfrak{q}}\,\gamma(\chi_{\mathfrak{P}}^{-n})^{p-1} \;=\; \frac{1}{p-1}\cdot\mathrm{ord}_{\sigma_b\mathfrak{P}}\,\gamma(\chi_{\mathfrak{P}}^{-n})^{p-1}$$

$$=\; \mathrm{ord}_{\sigma_b\mathfrak{P}}\,\gamma(\chi_{\mathfrak{P}}^{-n}) \;=\; b^{-1}n \mod p-1 \qquad\qquad (b^{-1}n \text{ in the range } 0,1,2,\ldots,p-2)$$

Generally, let the order of the character χ^{-n} be

$$m \;=\; \frac{p-1}{\gcd(n,p-1)}$$

The Gauss sum $\gamma(\chi^{-n})$ lies in the subfield $\mathbb{Q}(\omega_m,\zeta_p)$ of $\mathbb{Q}(\omega_{p-1},\zeta_p)$, and its m^{th} power $\gamma(\chi^{-n})^m$ lies in $\mathbb{Z}[\omega_m]$. The factorization of $\gamma(\chi^{-n})^m$ in $\mathbb{Z}[\omega_m]$ is completely determined, as follows. Let $\mathfrak{p}$ be the prime under $\mathfrak{P}$ in $\mathbb{Z}[\omega_m]$. The ramification degree of $\mathfrak{P}$ over $\mathfrak{p}$ is $p-1$. Then

$$\mathrm{ord}_{\sigma_b\mathfrak{p}}\,\gamma(\chi_{\mathfrak{P}}^{-n})^m \;=\; \frac{1}{p-1}\cdot \mathrm{ord}_{\sigma_b\mathfrak{P}}\,\gamma(\chi_{\mathfrak{P}}^{-n})^m \;=\; \frac{1}{p-1}\cdot m\cdot \mathrm{ord}_{\sigma_b\mathfrak{P}}\,\gamma(\chi_{\mathfrak{P}}^{-n})$$

$$=\; \frac{1}{p-1}\cdot m\cdot \big(b^{-1}n \bmod p-1\big) \;=\; \frac{1}{p-1}\cdot m\cdot \gcd(n,p-1)\cdot \big(\frac{b^{-1}n}{\gcd(n,p-1)} \bmod m\big)$$

$$=\; \frac{b^{-1}n}{\gcd(n,p-1)} \bmod m \qquad (\text{for } b\in(\mathbb{Z}/(p-1))^\times,\ b^{-1}n/\gcd(n,p-1) \text{ in the range } 0,1,\ldots,m-1\ )$$

[19.5] Ambiguity by units

When the ideals in $\mathbb{Z}[\omega_m]$ over p are *principal*, the Gauss sum can be determined up to a *root of unity*, rather than up to a more general unit.

Let $\omega=\omega_m$ and $\zeta=\zeta_p$. Let $\chi_{\mathfrak{P}}^{-n}$ be of order $m=(p-1)/\gcd(n,p-1)$, and put

$$\ell \;=\; \frac{n}{\gcd(n,p-1)}$$

Let q_o generate $\mathfrak{p}$, the ideal lying under $\mathfrak{P}$ in $\mathbb{Z}[\omega]$, where $\mathfrak{P}$ defines the Kummer (-Teichmüller) character. Identify $(\mathbb{Z}/m)^\times$ with the Galois group of $\mathbb{Q}(\omega)$ over $\mathbb{Q}$, which is transitive on primes over p in $\mathbb{Z}[\omega]$. Let τ_b be the Galois automorphism

$$\tau_b(\omega) \;=\; \omega^b \qquad (\text{for } b\in(\mathbb{Z}/m)^\times)$$

The factorization of $\gamma(\chi^{-n})^m$ gives

$$\gamma(\chi_{\mathfrak{P}}^{-n})^m \;=\; \eta\cdot \prod_{b\in(\mathbb{Z}/m)^\times} (\tau_b q_o)^{b^{-1}\ell \bmod m} \qquad (\text{exponents in the range } 0,1,2,\ldots,m-1)$$

with a unit η in $\mathbb{Z}[\omega]$. We will show that η is a *root of unity*, by applying Kronecker's theorem that an[4] algebraic integer with absolute value 1 at every archimedean place is a root of unity.

Observe that τ_{-1} acts as *complex conjugation* in the sense that, for every complex imbedding of $\mathbb{Q}(\omega)$, the automorphism τ_{-1} is the restriction of complex conjugation to the image. Since p splits completely in $\mathbb{Z}[\omega]$ over $\mathbb{Z}$,

$$\prod_b \tau_b q_o \;=\; \pm p$$

Since $\mathbb{Q}(\omega)$ has only complex archimedean places, none real, the factors $\tau_b q_o$ occur in complex conjugate pairs. This eliminates the ambiguity of sign:

$$\prod_b \tau_b q_o \;=\; p$$

[4] *Theorem (Kronecker):* An algebraic integer all whose complex imbeddings have absolute value 1 is a root of unity. To prove this, let α be an algebraic integer such that $|\sigma(\alpha)|=1$ for all complex (or real) imbeddings $\sigma:\mathbb{Q}(\alpha)\to\mathbb{C}$. Then the same is true of powers of α, and these are of degree over $\mathbb{Q}$ no more than that of α. Thus, the monic irreducibles of the powers of α over $\mathbb{Q}$ are of uniformly bounded degree and have uniformly bounded coefficients. The coefficients are in $\mathbb{Z}$, since α is an algebraic integer. There are only finitely-many polynomials of bounded degree with bounded integer coefficients. Thus, $\alpha^i=\alpha^j$ for some $i\neq j$.

Compute

$$\tau_{-1}\gamma(\chi_{\mathfrak{P}}^{-n})^m \;=\; \tau_{-1}\eta\cdot\prod_b \tau_{-1}\big((\tau_b q_o)^{b^{-1}\ell \bmod m}\big) \;=\; \prod_b (\tau_{-b}q_o)^{b^{-1}\ell \bmod m}$$

$$=\; \prod_b (\tau_b q_o)^{m-b^{-1}\ell \bmod m} \qquad \text{(exponents in the range } 0,1,\ldots,m-1)$$

by replacing b^{-1} by $m-b^{-1}$ in the product. Thus,

$$\prod_b (\tau_b q_o)^{b^{-1}\ell \bmod m}\cdot\prod_b \tau_{-1}\big((\tau_b q_o)^{b^{-1}\ell \bmod m}\big) \;=\; \prod_b (\tau_b q_o)^m \;=\; p^m$$

On the other hand, it is elementary that the product of a Gauss sum and its complex conjugate is p, so also

$$\gamma(\chi_{\mathfrak{P}}^{-n})^m\cdot\tau_{-1}\gamma(\chi_{\mathfrak{P}}^{-n})^m \;=\; p^m$$

Thus, $\eta\cdot\tau_{-1}\eta = 1$. Thus, for *any* complex imbedding $j:\mathbb{Q}(\omega)\to\mathbb{C}$, we have $|j(\eta)|=1$. Invoking Kronecker's theorem, η is a root of unity. ///

In summary, for $\chi_{\mathfrak{P}}^{-n}$ of order m, with $\ell = n/\gcd(n,p-1)$, when the prime ideals over p in $\mathbb{Z}[\omega_m]$ are *principal*, with generators $\tau_b q_o$, there is a *root of unity* η such that

$$\gamma(\chi_{\mathfrak{P}}^{-n})^m \;=\; \eta\cdot\prod_{b\in(\mathbb{Z}/m)^\times}(\tau_b q_o)^{b^{-1}\ell \bmod m} \qquad \text{(exponents in the range } 0,1,2,\ldots,m-1)$$

[19.6] Evaluating Gauss sums

We combine Kummer's estimate, the prime factorization, and the fact that the ambiguous unit η is a root of unity, for subsequent numerical computations, by obtaining a congruence completely determining η.

As above, let $\chi_{\mathfrak{P}}^{-n}$ be of order $m=(p-1)/\gcd(n,p-1)$, put $\ell = n/\gcd(n,p-1)$, and suppose that the primes lying over p in $\mathbb{Z}[\omega]$ are *principal*. We just saw that

$$\gamma(\chi_{\mathfrak{P}}^{-n})^m \;=\; \eta\cdot\prod_{b\in(\mathbb{Z}/m)^\times}(\tau_b q_o)^{b^{-1}\ell \bmod m} \qquad \text{(exponents in the range } 0,1,2,\ldots,m-1)$$

On the other hand, from Kummer's estimate,

$$\Big(\frac{\gamma(\chi_{\mathfrak{P}}^{-n})}{(\zeta-1)^n}\Big)^m \;=\; \Big(\frac{-1}{n!}\Big)^m \bmod \mathfrak{P}$$

or

$$\frac{\gamma(\chi_{\mathfrak{P}}^{-n})^m}{(\zeta-1)^{\ell\cdot(p-1)}} \;=\; \Big(\frac{-1}{n!}\Big)^m \bmod \mathfrak{P}$$

Combining these,

$$\frac{\eta\cdot\prod_{b\in(\mathbb{Z}/m)^\times}(\tau_b q_o)^{b^{-1}\ell \bmod m}}{(\zeta-1)^{\ell\cdot(p-1)}} \;=\; \Big(\frac{-1}{n!}\Big)^m \bmod \mathfrak{P}$$

This will determine η completely. The relation admits simplification, as follows. From

$$0 \;=\; \zeta^{p-1}+\ldots+\zeta+1 \;=\; \big((\zeta-1)+1\big)^{p-1}+\ldots+\big((\zeta-1)+1\big)+1 \;=\; (\zeta-1)^{p-1}+\ldots+p$$

we have

$$(\zeta-1)(\zeta^2-1)\ldots(\zeta^{p-1}-1) \;=\; p$$

Since $\zeta = 1 \bmod \zeta - 1$,

$$\frac{p}{(\zeta-1)^{p-1}} \;=\; \frac{(\zeta-1)(\zeta^2-1)\ldots(\zeta^{p-1}-1)}{(\zeta-1)^{p-1}}$$

$$=\; 1\cdot(\zeta+1)\cdot(\zeta^2+\zeta+1)\ldots(\zeta^{p-2}+\ldots+1) \;=\; (p-1)! \bmod \mathfrak{P} \;=\; -1 \bmod \mathfrak{P}$$

The relation determining η becomes

$$\frac{\eta\cdot\prod_{b\in(\mathbb{Z}/m)^\times}(\tau_b q_o)^{b^{-1}\ell \bmod m}}{(-p)^\ell} \;=\; \Big(\frac{-1}{n!}\Big)^m \bmod \mathfrak{P}$$

Everything is in $\mathbb{Z}[\omega]$, so

$$\frac{\eta\cdot\prod_{b\in(\mathbb{Z}/m)^\times}(\tau_b q_o)^{b^{-1}\ell \bmod m}}{(-p)^\ell} \;=\; \Big(\frac{-1}{n!}\Big)^m \bmod q_o$$

For simplicity, consider the case $n|(p-1)$, so $m = \frac{p-1}{n}$ and $\ell = 1$:

$$\frac{\eta\cdot\prod_{b\in(\mathbb{Z}/m)^\times}(\tau_b q_o)^{b^{-1} \bmod \frac{p-1}{n}}}{-p} \;=\; \Big(\frac{-1}{(\frac{p-1}{m})!}\Big)^m \bmod q_o$$

Since p is the product of the elements $\tau_b q_o$, in this case the left-hand side simplifies a little, to

$$-\eta\cdot\prod_{b\in(\mathbb{Z}/m)^\times}(\tau_b q_o)^{b^{-1} \bmod \frac{p-1}{n}-1} \;=\; \Big(\frac{-1}{(\frac{p-1}{m})!}\Big)^m \bmod q_o$$

with $b^{-1} \bmod \frac{p-1}{n}$ in the range $1,\ldots,\frac{p-1}{n}-1$. The fact that $\mathbb{Z}[\omega]$ modulo q_o has m^{th} roots of unity *almost* assures that η is completely determined by this congruence. However, for *m odd*, $\mathbb{Z}[\omega]$ also contains the $2m^{th}$ roots of unity. Luckily, p is odd, so $\mathbb{Z}[\omega]$ mod q_o *also* has $2m^{th}$ roots of unity. That is, the map from roots of unity in $\mathbb{Z}[\omega]$ to $\mathbb{Z}[\omega]$ modulo q_o is *injective*, so η is completely determined by this congruence, as claimed.

That is, since η is a root of unity, rather than a more general unit in $\mathbb{Z}[\omega]$, Kummer's estimate is sufficient to determine η completely.

[19.7] Numerical examples Several examples of primes p and Gauss sums attached to characters $\chi_{\mathfrak{P}}^{-n}$ of order m, with $n = \frac{p-1}{m}$ offer coincidences for less laborious computation.

Tiniest case $p = 5$ and order $m = 4$: The prime $p = 5$ has factors $q_o = 2+i$ and $\tau_3 q_o = 2-i$ in $\mathbb{Z}[i]$, and

$$\gamma(\chi_{\mathfrak{P}}^{-1})^4 \;=\; \eta\cdot(2+i)\cdot(2-i)^3$$

The congruence for the unit η is

$$-(2-i)^2\cdot\eta \;=\; \Big(\frac{-1}{(\frac{5-1}{4})!}\Big)^4 \bmod (2+i)$$

or simply

$$-(2-i)^2\cdot\eta \;=\; 1 \bmod (2+i)$$

Since $2-i = (2+i)-2i$, we have $-(-2i)^2\eta = 1 \bmod (2+i)$, or $\eta = 1 \bmod (2+i)$, so $\eta = 1$. That is,

$$\gamma(\chi_{\mathfrak{P}}^{-1})^4 \;=\; (2+i)\cdot(2-i)^3$$

and $\mathbb{Q}(\zeta_5,\omega)$ is generated by a fourth root of $(2+i)\cdot(2-i)^3$ over $\mathbb{Q}(\omega)$. Thus,

$$\mathbb{Q}(\zeta_5, i) \;=\; \mathbb{Q}(i)\big(\sqrt[4]{(2+i)\cdot(2-i)^3}\big)$$

[19.8] Example: $p = 13$ and order $m = 4$. With $q_o = 3 + 2i$ and $\tau_3 q_o = 3 - 2i$,

$$\gamma(\chi_{\mathfrak{P}}^{-1})^4 \;=\; \eta \cdot (3+2i) \cdot (3-2i)^3$$

The congruence for the unit η is

$$-(3-2i)^2 \cdot \eta \;=\; \Big(\frac{-1}{(\frac{13-1}{4})!}\Big)^4 \bmod (3+2i)$$

or simply

$$-(3-2i)^2 \cdot \eta \;=\; \frac{1}{6^4} \bmod (3+2i)$$

Since $3 - 2i = (3+2i) - 4i$ and $2 \cdot 6 = -1 \bmod 13$, this is

$$16 \cdot \eta \;=\; (-2)^4 \bmod (3+2i)$$

from which $\eta = 1$. Thus,

$$\gamma(\chi_{\mathfrak{P}}^{-3})^4 \;=\; q_o \cdot (\tau_3 q_o)^3 \cdot \eta \;=\; (3+2i) \cdot (3-2i)^3$$

and the quartic subfield $\mathbb{Q}(\zeta_{13}, \omega)$ over $\mathbb{Q}(\omega)$ is generated by a fourth root of $(3+2i) \cdot (3-2i)^3$. Thus, the quartic subfield of $\mathbb{Q}(\zeta_{13}, i)$ over $\mathbb{Q}(i)$ is

$$\Big(\text{quartic subfield of } \mathbb{Q}(\zeta_{13}, i) \text{ over } \mathbb{Q}(i)\Big) \;=\; \mathbb{Q}(i)\big(\sqrt[4]{(3+2i)\cdot(3-2i)^3}\big)$$

[19.9] Example: $p = 17$ and order $m = 4$. With $q_o = 4 + i$ and $\tau_3 q_o = 4 - i$,

$$\gamma(\chi_{\mathfrak{P}}^{-1})^4 \;=\; \eta \cdot (4+i) \cdot (4-i)^3$$

and the congruence for the unit η is

$$-(4-i)^2 \cdot \eta \;=\; \Big(\frac{-1}{(\frac{17-1}{4})!}\Big)^4 \bmod (4+i)$$

or

$$-(4-i)^2 \cdot \eta \;=\; \frac{1}{7^4} \bmod (4+i)$$

Since $4 - i = (4+i) - 2i$ and $5 \cdot 7 = 1 \bmod 17$, this is

$$4 \cdot \eta \;=\; 5^4 \bmod (4+i)$$

Since $-4 \cdot 4 = 1 \bmod 17$,

$$\eta \;=\; -4 \cdot 8^2 \;=\; -(2 \cdot 8)^2 \;=\; -(-1)^2 \;=\; -1 \bmod 4+i$$

Thus,

$$\gamma(\alpha)^4 \;=\; \eta \cdot (4+i)(4-i)^3 \;=\; -(4+i)(4-i)^3$$

Therefore, the quartic subfield of and $\mathbb{Q}(\zeta_{17}, \omega)$ over $\mathbb{Q}(\omega)$ is generated by a fourth root of $-(4+i)\cdot(4-i)^3$, and

$$\Big(\text{quartic subfield of } \mathbb{Q}(\zeta_{17}, i) \text{ over } \mathbb{Q}(i)\Big) \;=\; \mathbb{Q}(i)\big(\sqrt[4]{-(4+i)\cdot(4-i)^3}\big)$$

[19.10] Example: $p = 7$ and order $m = 3$. Let ρ be a cube root of unity, with Galois conjugate $\overline{\rho}$. Note that $\overline{\rho} = -1 - \rho$, and

$$(a + b\rho)(a + b\overline{\rho}) \;=\; a^2 - ab + b^2$$

For $p = 7$, take $q_o = 2 - \rho$ and $\tau_{-1} q_o = 2 - \overline{\rho} = 3 + \rho$.

$$\gamma(\chi_{\mathfrak{P}}^{-2})^3 \;=\; \eta \cdot (2-\rho) \cdot (3+\rho)^2$$

The congruence for the unit η is

$$-(3+\rho) \cdot \eta \;=\; \Big(\frac{-1}{(\frac{7-1}{3})!}\Big)^3 \bmod (2-\rho)$$

which becomes $(3+\rho) \cdot \eta = 1 \bmod (2-\rho)$. Since

$$3 + \rho \;=\; 3 + \rho + 2(2-\rho) \;=\; -\rho \bmod 2 - \rho$$

the congruence for η is

$$-\rho \cdot \eta \;=\; 1 \bmod (2-\rho)$$

so $\eta = -\rho^2$. That is,

$$\gamma(\chi_{\mathfrak{P}}^{-2})^3 \;=\; \eta \cdot (2-\rho) \cdot (3+\rho)^2 \;=\; -\rho^2 \cdot (2-\rho) \cdot (3+\rho)^2$$

and the cubic subfield of $\mathbb{Q}(\zeta_7, \rho)$ over $\mathbb{Q}(\omega)$ is generated by a cube root of $-\rho^2 \cdot (2-\rho) \cdot (3+\rho)^2$:

$$\big(\text{cubic subfield of } \mathbb{Q}(\rho, \zeta_7) \text{ over } \mathbb{Q}(\rho)\big) \;=\; \mathbb{Q}(\rho)\big(\sqrt[3]{-\rho^2 \cdot (2-\rho) \cdot (3+\rho)^2}\big)$$

[19.11] Example: $p = 7$ and order $m = 6$. Use $q_o = 2 - \rho$ and $\tau_{-1} q_o = 2 - \overline{\rho} = 3 + \rho$. We have

$$\gamma(\chi_{\mathfrak{P}}^{-1})^6 \;=\; \eta \cdot (2-\rho) \cdot (3+\rho)^5$$

and η satisfies

$$-(3+\rho)^4 \cdot \eta \;=\; \Big(\frac{-1}{(\frac{7-1}{6})!}\Big)^6 \bmod (2-\rho)$$

Using $\rho = 2 \bmod 2 - \rho$ and $5 = -2 \bmod 7$, this is

$$-(-2)^4 \cdot \eta \;=\; 1 \bmod (2-\rho)$$

or

$$2 \cdot \eta \;=\; -1 \bmod (2-\rho)$$

Thus,

$$\eta \;=\; -4 \;=\; -\rho^2 \bmod 2 - \rho$$

and

$$\gamma(\chi_{\mathfrak{P}}^{-1})^6 \;=\; -\rho^2 \cdot (2-\rho) \cdot (3+\rho)^5$$

Thus,

$$\mathbb{Q}(\rho, \zeta_7) \;=\; \mathbb{Q}(\rho)\big(\sqrt[6]{\rho^2 \cdot (2-\rho) \cdot (3+\rho)^5}\big)$$

[19.12] Example: $p = 11$ and order $m = 5$. Since $\omega = \omega_5$ satisfies $\omega^4 + \omega^3 + \ldots + \omega + 1 = 0$,

$$0 \;=\; \big((\omega+2) - 2\big)^4 + \big((\omega+2) - 2\big)^3 + \ldots + \big((\omega+2) - 2\big) + 1 \;=\; (\omega+2)^4 + \ldots + 11$$

The constant term $11 = (2^5 + 1)/(2+1)$ is the norm of $q_o = \omega + 2$, so

$$11 \;=\; (\omega+2)(\omega^2+2)(\omega^3+2)(\omega^4+2)$$

The fifth power of the quintic Gauss sum is

$$\gamma(\chi_{\mathfrak{P}}^{-2})^5 \;=\; \eta\cdot(\omega+2)\,(\omega^2+2)^3\,(\omega^3+2)^2\,(\omega^4+2)^4$$

and the congruence for η is

$$-\eta\,(\omega^2+2)^2\,(\omega^3+2)\,(\omega^4+2)^3 \;=\; \Big(\frac{-1}{(\frac{11-1}{5})!}\Big)^5 \bmod (\omega+2)$$

Using $\omega = -2 \bmod \omega+2$, this is

$$\eta\,((-2)^2+2)^2\,((-2)^3+2)\,((-2)^4+2)^3 \;=\; \frac{1}{2^5} \bmod (\omega+2)$$

or

$$\eta\cdot 6^2\cdot(5)\cdot(7)^3 \;=\; -1 \bmod (\omega+2)$$

which simplifies to $\eta\cdot 3\cdot 5\cdot 2 \;=\; -1 \bmod (\omega+2)$ and then $3\eta = 1 \bmod (\omega+2)$, so $\eta = 4 \bmod (\omega+2)$. Since $\omega = -2 \bmod (\omega+2)$, this gives $\eta = \omega^2$. Thus,

$$\gamma(\chi_{\mathfrak{P}}^{-2})^5 \;=\; \omega^2\cdot(\omega+2)\,(\omega^2+2)^3\,(\omega^3+2)^2\,(\omega^4+2)^4$$

and the quintic subfield of $\mathbb{Q}(\omega_5,\zeta_{11})$ is generated over $\mathbb{Q}(\omega_5)$ by the fifth root of this.

[19.13] Existence of Kummer (-Teichmüller) character

As above, let p be a prime, and ω a primitive $(p-1)^{th}$ root of unity. Fix a prime $\mathfrak{q}$ lying over p in $\mathbb{Z}[\omega]$. The complete splitting of p in $\mathbb{Z}[\omega]$ implies that the residue class field extension is trivial, so the inclusion $j:\mathbb{Z}/p \longrightarrow \mathbb{Z}[\omega]/\mathfrak{q}$ is an *isomorphism.* The units in $\mathbb{Z}[\omega]$ certainly map to units in $\mathbb{Z}[\omega]/\mathfrak{q}$. It would be perverse if the $(p-1)^{th}$ roots of unity in $\mathbb{Z}[\omega]$ did not surject to the units in $\mathbb{Z}[\omega]/\mathfrak{q}$, but this requires proof. Thus, we can use Hensel's lemma to specify a $\mathbb{Z}[\omega]_{\mathfrak{q}}^\times$-valued character on $(\mathbb{Z}/p)^\times$, beginning with $\chi_{\mathfrak{q}}(a) = j(a) \bmod \mathfrak{q}$. To solve the equation $x^{p-1}-1=0$ in $\mathbb{Z}[\omega]_{\mathfrak{q}}$, let $x_1 = a$. Since the derivative $(p-1)a^{p-2}$ is a $\mathfrak{q}$-adic unit, Hensel's lemma produces $x\in\mathbb{Z}[\omega]_{\mathfrak{q}}$ such that $x^{p-1}-1=0$ and $x = a \bmod \mathfrak{q}$, as desired. Of course, the $(p-1)^{th}$ roots of unity are in $\mathbb{Z}[\omega]$, without completing, but this discussion does prove that the $(p-1)]th$ roots of unity *surject* to the units in $(\mathbb{Z}/p)^\times \approx (\mathbb{Z}[\omega]/\mathfrak{q})^\times$. This proves existence of the Kummer (-Teichmüller) character.

[19.14] Properties of Gauss sums

Recall that, for a multiplicative character α and additive character ψ on $\mathbb{Z}/p$, the product $\gamma(\alpha)\cdot\gamma(\alpha^{-1})$ of Gauss sums is simply $p\cdot\alpha((-1)$, by a straightforward computation:

$$\gamma(\alpha)\cdot\gamma(\alpha^{-1}) \;=\; \big(\sum_a \alpha(a)\,\psi(a)\big)\cdot\big(\sum_b \alpha^{-1}(b)\,\psi(b)\big) \;=\; \sum_{a,b}\alpha(a)\,\alpha^{-1}(b)\,\psi(a+b)$$

Replace b by ab:

$$\gamma(\alpha)\cdot\gamma(\alpha^{-1}) \;=\; \sum_{a,b}\alpha^{-1}(b)\,\psi(a(1+b))$$

For fixed b, the sum over a is -1 unless $1+b=0$, in which case it is $p-1$. Thus,

$$\gamma(\alpha)\cdot\gamma(\alpha^{-1}) \;=\; -\sum_{b\neq -1}\alpha^{-1}(b) + \alpha^{-1}(-1)\cdot(p-1) \;=\; \alpha^{-1}(-1) + \alpha^{-1}(-1)\cdot(p-1) \;=\; \alpha(-1)\cdot p$$

since $\alpha(-1) = \alpha^{-1}(-1)$. That is,

$$\gamma(\alpha)\cdot\gamma(\alpha^{-1}) \;=\; \alpha(-1)\cdot p$$

On the other hand, for two multiplicative characters α,β with $\alpha\beta\neq 1$, an analogous computation has a different outcome, involving a *Jacobi sum*:

$$\gamma(\alpha)\cdot\gamma(\beta) \;=\; \sum_a \alpha(a)\,\psi(a)\cdot\sum_b \beta(b)\,\psi(b) \;=\; \sum_{a,b}\alpha(a)\,\beta(b)\,\psi(a+b)$$

$$= \sum_{a\neq 0}\sum_b \alpha(a-b)\,\beta(b)\,\psi(a) + \sum_b \alpha(-b)\,\beta(b) \;=\; \sum_{a\neq 0}\sum_b \alpha(a-b)\,\beta(b)\,\psi(a) + \alpha(-1)\sum_b \alpha(b)\,\beta(b)$$

For $\alpha\beta \neq 1$, the last sum vanishes. In the first sum, replace b by ab:

$$\gamma(\alpha)\cdot\gamma(\beta) \;=\; \sum_{a\neq 0}\sum_{b\neq 0,1} \alpha(a(1-b))\,\beta(ab)\,\psi(a)$$

$$= \sum_{a\neq 0}\sum_{b\neq 0,1} \alpha(a)\beta(a)\,\psi(a)\sum_b \alpha(1-b))\,\beta(b) \;=\; \gamma(\alpha\beta)\cdot\sum_{b\neq 0,1}\alpha(1-b))\,\beta(b)$$

That is,

$$\gamma(\alpha)\cdot\gamma(\beta) \;=\; \gamma(\alpha\beta)\cdot\sum_{b\neq 0,1}\alpha(1-b))\,\beta(b) \qquad\qquad (\text{with } \alpha\beta\neq 1)$$

The latter sum is a *Jacobi sum*.

20. *Fujisaki: units theorem, finiteness of class numbers*

In modern treatment, both Dirichlet's units theorem and the finiteness of class numbers are corollaries of *Fujisaki's compactness:*

[20.1] Theorem: $\mathbb{J}^1/k^\times$ is *compact.*

We state and prove two important corollaries first.

[20.2] Corollary: The class number of $\mathfrak{o}$ is finite. Let $k\otimes_{\mathbb{Q}}\mathbb{R} \approx \mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$. That is, k has r_1 *real* archimedean completions, and r_2 *complex* archimedean completions. These r_1, r_2 are *standard* references.

[20.3] Corollary: *(Dirichlet's Units Theorem)* The unit group $\mathfrak{o}^\times$, modulo torsion, is a free $\mathbb{Z}$-module of rank $r_1 + r_2 - 1$.

[20.4] Remark: It is striking that two big theorems of classical algebraic number theory, finiteness of class number, and the Units Theorem, follow from an innocuous *compactness* assertion.

Also, note the contrast to *additive* approximation, which is essentially a reformulation of elementary things akin to Sun-Ze's theorem, and has no breath-taking corollaries.

[20.5] Pell's equation Fermat considered the simplest non-trivial case of the Units Theorem, namely, *real quadratic* fields k, with $r_1 = 2$ and $r_2 = 0$. Note

$$N^k_{\mathbb{Q}}(x + y\sqrt{D}) \;=\; x^2 - Dy^2 \qquad\qquad (0 < D \in \mathbb{Z} \text{ squarefree})$$

To solve *Pell's equation* $x^2 - Dy^2 = 1$ with $x, y \in \mathbb{Z}$ is to find units in $\mathbb{Z}[\sqrt{D}]^\times$ with Galois norms 1. These are of index at most 2 in $\mathfrak{o}^\times$.

Multiplicativity of the Galois norm *also* shows that solutions of Pell's equation form a group. This can also be verified directly and cryptically: the secret multiplication

$$(x + y\sqrt{D})\cdot(z + w\sqrt{D}) \;=\; (xz - Dyw) + (xw + yz)\sqrt{D}$$

suggests showing by elementary algebra that with $x^2 - Dy^2 = 1$ and $z^2 - Dw^2 = 1$,

$$(xz - Dyw)^2 - D(xw + yz)^2 \;=\; \ldots \;=\; 1$$

Rational solutions $x, y \in \mathbb{Q}$ to $x^2 - Dy^2 = 1$ are elementary to find. Namely, because $x^2 - Dy^2 = 1$ is a quadratic curve with at least one rational point $(1, 0)$, the straight line $y = -t(x - 1)$ through $(1, 0)$ and $(0, t)$ meets the curve at a *rational* point for rational t: replacing y by $-t(x - 1)$ in the quadratic,

$$x^2(1 - Dt^2) + 2Dt^2x - (1 + Dt^2) \;=\; 0$$

By arrangement, $x = 1$ is a solution, and

$$x^2 + \frac{2Dt^2}{1 - Dt^2}x - \frac{1 + Dt^2}{1 - Dt^2} \;=\; (x - 1)\big(x - \frac{Dt^2 + 1}{Dt^2 - 1}\big)$$

Thus, $x = (Dt^2+1)/(Dt^2-1)$ and $y = t/(Dt^2-1)$ are *rational* solutions to Pell's equation. *Integer* solutions are harder to find.

An *upper* bound on *integer* solutions to $x^2 - Dy^2 = 1$ follows from *topological* considerations:

[20.6] Claim: The collection of positive-integer solutions x, y is a free group on either 1 or 0 generators.

Proof: Imbed $\mathbb{Z}[\sqrt{D}] \to \mathbb{R}^2$ by $x + y\sqrt{D} \to (x + y\sqrt{D}, x - y\sqrt{D})$. The image of $\mathfrak{o}$ is discrete. The units $x + y\sqrt{D}$ with $0 < x, y \in \mathbb{Z}$ lie on the hyperbola $u \cdot v = 1$, and are discrete there. Map the first-quadrant piece of that hyperbola to $\mathbb{R}$ by $(u, 1/u) \to \log u$. The units map to a discrete subgroup of $\mathbb{R}$.

The discrete subgroups Γ of $\mathbb{R}$ are the trivial $\{0\}$ and free groups on a single generator. This may be intuitively plausible, but also is readily provable, as follows.

[20.7] Claim: The discrete subgroups Γ of $\mathbb{R}$ are $\{0\}$ and free groups on a single generator.

Proof: For $\Gamma \neq \{0\}$, since it is closed under additive inverses, it contains *positive* elements. In the case that there is a *least* positive element γ_o, claim that $\Gamma = \mathbb{Z} \cdot \gamma_o$. Indeed, given $0 < \gamma \in \Gamma$, by the archimedean property of $\mathbb{R}$, there is an integer ℓ such that $\ell \cdot \gamma_o \leq \gamma < (\ell + 1) \cdot \gamma_o$. Either $\gamma = \ell \cdot \gamma_o$ and $\gamma \in \mathbb{Z} \cdot \gamma_o$, or else $0 < \gamma - \ell \cdot \gamma_o < \gamma_o$, contradiction.

Now suppose that there are $\gamma_1 > \gamma_2 > \ldots > 0$ in Γ, and show that $\Gamma = \mathbb{R}$. Since Γ is *closed* (!), the infimum γ_o of the γ_j is in Γ. Since Γ is a group, $0 < \gamma_j - \gamma_o \in \Gamma$. Replacing γ_j by $\gamma_j - \gamma_o$, we can suppose that $\gamma_j \to 0$. The collection of integer multiples of $\gamma_j > 0$ contains elements within distance γ_j of any real number, by the archimedean property of $\mathbb{R}$. Since $\gamma_j \to 0$, every real number is in the closure of Γ. Since Γ is closed (!), $\Gamma = \mathbb{R}$, which is not discrete. ///

There are two classical proof mechanisms for *existence* of solutions to Pell's equation, one by a pigeon-hole principle argument, the other by *continued fractions.* Neither obviously generalizes, although the measure-theory in the proof of Fujisaki's lemma should be construed as a vastly-more-powerful version of a pigeon-hole principle.

The proof of Fujisaki's lemma uses existence and essential uniqueness of *Haar measure* on $\mathbb{A}$, that is, a translation-invariant positive regular Borel measure. In fact, *we will not integrate anything*, but will only use some structural *properties* of Haar measure...

The simplicity and brevity of the proof, and the easy derivation of the two big corollaries, are powerful advertisements for the helpfulness of Haar measure. We discuss Haar measure afterward.

Proof: *(of Fujisaki's lemma)* Haar measure on $\mathbb{A} = \mathbb{A}_k$ and Haar measure on the (topological group) quotient $\mathbb{A}/k$ are inter-related by

$$\int_{\mathbb{A}} f(x)\,dx \;=\; \int_{\mathbb{A}/k} \sum_{\gamma \in k} f(\gamma + x)\,dx$$

Normalize the measure on $\mathbb{A}$ so that, mediated by this relation, $\mathbb{A}/k$ has measure 1.

We have the Minkowski-like claim, a measure-theory *pigeon-hole principle*, that a compact subset C of $\mathbb{A}$ with measure greater than 1 cannot *inject* to the quotient $\mathbb{A}/k$. Suppose, to the contrary, that C injects to the quotient. With f the characteristic function of C,

$$1 < \int_{\mathbb{A}} f(x)\,dx = \int_{\mathbb{A}/k} \sum_{\gamma\in k} f(\gamma+x)\,dx \le \int_{\mathbb{A}/k} 1\,dx = 1$$

with the last inequality by injectivity. Contradiction. For *idele* α, we will see later that the change-of-measure on $\mathbb{A}$ is given conveniently by

$$\frac{\text{meas}\,(\alpha E)}{\text{meas}\,(E)} = |\alpha| \qquad\qquad (\text{for measurable } E \subset \mathbb{A})$$

Given $\alpha \in \mathbb{J}^1$, we will adjust α by $k^\times$ to lie in a compact subset of $\mathbb{J}^1$. Fix compact $C \subset \mathbb{A}$ with measure > 1.

The topology on $\mathbb{J}$ is *strictly finer* than the subspace topology with $\mathbb{J} \subset \mathbb{A}$: the genuine topology is by imbedding $\mathbb{J} \to \mathbb{A}\times\mathbb{A}$ by $\alpha \to (\alpha, \alpha^{-1})$.

For $\alpha \in \mathbb{J}^1$, both αC and $\alpha^{-1}C$ have measure > 1, neither injects to the quotient $k\backslash\mathbb{A}$. So there are $x \ne y$ in k so that $x + \alpha C = y + \alpha C$. Subtracting,

$$0 \;\ne\; a \;=\; x-y \;\in\; \alpha(C-C)\cap k$$

That is,

$$a\cdot\alpha^{-1} \;\in\; C-C$$

Likewise, there is $0 \ne b \in \alpha^{-1}(C-C)\cap k$, and $b\cdot\alpha \in C-C$. There is an obvious constraint

$$ab = (a\cdot\alpha)(b\cdot\alpha^{-1}) \in (C-C)^2\cap k^\times = \text{compact} \cap \text{discrete} \;=\; \text{finite}$$

Let $\Xi = (C-C)^2 \cap k^\times$ be this finite set. Paraphrasing: given $\alpha \in \mathbb{J}^1$, there are $a \in k^\times$ and $\xi \in \Xi$ ($\xi = ab$ above) such that $(a\cdot\alpha^{-1},\ (a\cdot\alpha^{-1})^{-1}) \;\in\; (C-C)\times\xi^{-1}(C-C)$.

That is, α^{-1} can be adjusted by $a \in k^\times$ to be in the compact $C-C$, and, simultaneously, for one of the finitely-many $\xi \in \Xi$, $(a\cdot\alpha^{-1})^{-1} \in \xi\cdot(C-C)$.

In the topology on $\mathbb{J}$, for each $\xi \in \Xi$,

$$\Big((C-C)\times\xi^{-1}(C-C)\Big) \;\cap\; \mathbb{J} \;=\; \text{compact in } \mathbb{J}$$

The continuous image in $\mathbb{J}/k\times$ of each of these finitely-many compacts is compact. Their union covers the *closed* subset $\mathbb{J}^1/k^\times$, so the latter is compact. ///

Proof: (of finiteness of class number) Let i be the *ideal map* from ideles to non-zero fractional ideals of the integers $\mathfrak{o}$ of k. That is,

$$i(\alpha) \;=\; \prod_{v<\infty} \mathfrak{p}_v^{\text{ord}_v\alpha} \qquad\qquad (\text{for } \alpha \in \mathbb{J})$$

where $\mathfrak{p}_v$ is the prime ideal in $\mathfrak{o}$ attached to the place v. Certainly the subgroup $\mathbb{J}^1$ of $\mathbb{J}$ still surjects to the group of non-zero fractional ideals. The kernel in $\mathbb{J}$ of the ideal map is

$$G \;=\; \prod_{v|\infty} k_v^\times \;\times\; \prod_{v<\infty} \mathfrak{o}_v^\times$$

and the kernel on $\mathbb{J}^1$ is $G^1 = G \cap J^1$. The principal ideals are the image $i(k^\times)$. The map of $\mathbb{J}^1$ to the ideal class group factors through the idele class group $\mathbb{J}^1/k^\times$, noting as usual that the product formula implies that $k^\times \subset \mathbb{J}^1$.

G^1 is open in $\mathbb{J}^1$, so its image K in the quotient $\mathbb{J}^1/k^\times$ is open, since quotient maps are open. The cosets of K cover $\mathbb{J}^1/k^\times$, and by compactness there is a finite subcover. Thus, $\mathbb{J}^1/k^\times K$ is finite, and this finite group is the ideal class group. ///

A continuation proves the units theorem! Since K is open, its cosets are open. Thus, K is closed. Since $\mathbb{J}^1/k^\times$ is Hausdorff and compact, K is compact. That is, we have compactness of

$$K \;=\; (G^1 \cdot k^\times)/k^\times \;\approx\; G^1/(k^\times \cap G^1) \;=\; G^1/\mathfrak{o}^\times$$

with the global units $\mathfrak{o}^\times$ imbedded on the diagonal.

Since $\prod_{v<\infty} \mathfrak{o}_v^\times$ is compact, its image U under the continuous map to $G^1/\mathfrak{o}^\times$ is compact. By Hausdorff-ness, the image U is closed. Thus, we can take a further (Hausdorff) quotient by U,

$$G^1/(U \cdot \mathfrak{o}^\times) \;=\; \text{compact}$$

With $k^1_\infty = \{\alpha \in \prod_{v|\infty} k_v^\times \;:\; \prod_v |\alpha_v|_v = 1\}$,

$$k^1_\infty/\mathfrak{o}^\times \;\approx\; G^1/(U \cdot \mathfrak{o}^\times) \;=\; (\text{compact})$$

This compactness is essentially the units theorem! (See below...) ///

[20.8] Remark: To compare with the classical formulation, one wants the accompanying result that a *discrete* subgroup L of $\mathbb{R}^n$ with $\mathbb{R}^n/L$ is *compact* is a free $\mathbb{Z}$-module on n generators.

Measure-theory pigeon-hole principle: On $\mathbb{R}$ or $\mathbb{R}^n$, these ideas were highly developed by Minkowski 100 years ago. The adelic version should be viewed as the obvious modern extension of the following:

[20.9] Proposition: A set $E \subset \mathbb{R}$ with measure > 1 contains $x \neq y$ such that $x - y \in \mathbb{Z}$.

Proof: Let f be the characteristic function of E, and

$$F(x) \;=\; \sum_{n\in\mathbb{Z}} f(x+n)$$

If no two points of E differ by an integer, then $f(x+m) \neq 0$ and $f(x+n) \neq 0$ for integers m,n implies $m = n$. With this assumption, $0 \leq F(x) \leq 1$.

We claim that

$$\int_0^1 F(x)\,dx \;=\; \int_{-\infty}^{\infty} f(x)\,dx$$

The left-hand side is

$$\int_0^1 \sum_n f(x+n)\,dx \;=\; \sum_n \int_0^1 f(x+n)\,dx \;=\; \sum_n \int_n^{n+1} f(x)\,dx$$

by replacing x by $x - n$. And then this is indeed $\int_{-\infty}^{\infty} f(x)\,dx$.

Thus,

$$1 \;<\; \int_{-\infty}^{\infty} f(x)\,dx \;=\; \int_0^1 F(x)\,dx \;\leq\; 1$$

Impossible. Thus, there are $x \neq y \in E$ with $x - y \in \mathbb{Z}$. ///

[20.10] Remark: It might appear that we needed to find a subset $[0,1]$ of $\mathbb{R}$ whose translates by $\mathbb{Z}$ fill out $\mathbb{R}$ with overlaps of measure 0. Although the argument above took advantage of this possibility, it was unnecessary, and potentially misleading. This is clarified below.

[20.11] Remark: Without prior experience, it may be hard to believe that the measure of a set is the sup of the compacts contained in it, since the set $E = [0,1] - (\mathbb{Q} \cap [0,1])$ obtained by removing all rational numbers from the unit interval $[0,1]$, which has measure 1, might appear to contain no compacts of positive measure.

However, E does have compact subsets with measures arbitrarily close to 1. For example, enumerate the rationals in the interval as r_n with $n = 1, 2, \ldots$, and for $j = 1, 2, \ldots$ consider the compact sets

$$C_j \;=\; [0,1] \;-\; \Big([0,1] \cap (r_n - \frac{1}{(n+j)!}, r_n + \frac{1}{(n+j)!})\Big)$$

inside E. Certainly

$$\operatorname{meas} C_j \;\geq\; 1 \;-\; \Big(\frac{1}{(1+j)!} + \frac{1}{(2+j)!} + \ldots\Big) \;\longrightarrow\; 1$$

Generalized ideal class numbers: The class number above is the *absolute* class number. An element $\alpha \in k$ is *totally positive* when $\sigma(\alpha) > 0$ for every *real* imbedding $\sigma : k \to \mathbb{R}$. For example, $2 + \sqrt{2}$ is totally positive, while $1 + \sqrt{2}$ is *not.*

The *narrow* class number is ideals modulo principal ideals generated by *totally positive* elements.

Congruence conditions can be imposed at *finite* places: given an ideal $\mathfrak{a}$, we can form an ideal class group of ideals modulo principal ideals possessing generators $\alpha = 1 \bmod \mathfrak{a}$, for example.

Positivity conditions can be combined with *congruence* conditions: *generalized ideal class groups* are quotients of (fractional) ideals by principal ideals meeting the positivity and congruence constraints. The ideal class groups corresponding to conditions $\alpha = 1 \bmod \mathfrak{a}$ are called *ray class groups.*

[20.12] Proposition: Generalized ideal class groups are presentable as *idele* class groups, specifically, as quotients of $\mathbb{J}^1/k^\times$ by *open* subgroups. [Proof later]

[20.13] Corollary: Generalized ideal class groups are *finite.*

Proof: First, note that an *open* subgroup of a topological group is also *closed*, because it the *complement* of the union of its cosets *not* containing the identity.

For U be an open subgroup of a *compact* abelian topological group K (such as $\mathbb{J}^1/k^\times$), K/U is *finite*, because the cover of K by (disjoint!) cosets of U has a *finite* subcover. Thus, K/U is *finite.* It is Hausdorff because U is also *closed.* ///

[20.14] Remark: The ray class groups with total-positivity thrown in are visibly *cofinal* in the collection of all generalized ideal class groups.

Generalized units: Let S be a finite collection of places of k, including all archimedean places. The S-integers $\mathfrak{o}_S$ in k are

$$\mathfrak{o}_S \;=\; k \cap \Big(\prod_{v \in S} k_v \times \prod_{v \notin S} \mathfrak{o}_v\Big) \;=\; \{\alpha \in k : \alpha \text{ is } v\text{-integral for } v \notin S\}$$

The group of S-units is $\mathfrak{o}_S^\times = k^\times \cap \big(\prod_{v \in S} k_v^\times \times \prod_{v \notin S} \mathfrak{o}_v^\times\big)$

[20.15] Theorem: *(Generalized Units Theorem)* $\mathfrak{o}_S^\times$ modulo roots of unity is free of rank $|S|-1$.

Proof: To treat the non-archimedean places in S, proceed slightly differently than for the classic units theorem: let $S_\infty = \{v|\infty\}$, S_o the non-archimedean places in S, and for $\alpha \in \mathbb{J}$

$$L(\alpha) = \{\log|\alpha_v|_v : v \in S_\infty\} \oplus \{\mathrm{ord}_v \alpha_v : v \in S_o\} \ \in \ \mathbb{R}^{|S_\infty|} \oplus \mathbb{Z}^{|S_o|}$$

The image $L(G^1)$ is

$$L(G^1) \ = \ \{\{x_v\} \in \mathbb{R}^{|S_\infty|} \oplus \mathbb{Z}^{|S_o|} \ : \ \sum_v x_v \ = \ 0\}$$

From

$$\begin{tikzcd}
G^1 \arrow[r, "L"] \arrow[d] & L(G^1) \arrow[r, dash, "\subset"] \arrow[d] & \mathbb{R}^{|S_\infty|} \oplus \mathbb{Z}^{|S_o|} \\
G^1/\mathfrak{o}_S^\times \arrow[r] & L(G^1)/L(\mathfrak{o}_S^\times) &
\end{tikzcd}$$

$L(G^1)/L(\mathfrak{o}_S^\times)$ is *compact*. Classification of discrete subgroups Γ of groups $\mathbb{R}^m \oplus \mathbb{Z}^n$ with compact quotients $(\mathbb{R}^m \oplus \mathbb{Z}^n)/\Gamma$ gives the result. ///

[20.16] Remaining details

Apart from generalities about Haar measure and subgroups of $\mathbb{R}^m \oplus \mathbb{Z}^n$, ... to know that the torsion subgroups of $\mathfrak{o}^\times$ and $\mathfrak{o}_S^\times$ consist only of *roots of unity*, we need to know that if $\alpha \in k$ has $|\alpha|_v = 1$ for all places $v \le \infty$, then α is a root of unity. In fact, recall Kronecker's sharper result we proved earlier:

[20.17] Theorem: (*Kronecker)* For $\alpha \in \mathfrak{o}$, if $|\alpha|_v = 1$ for all places $v|\infty$ then α is a root of unity. ///

[20.18] Remark: There is no analogous result replacing S_∞ by all places lying over a rational prime p, because there are infinitely-many rational integers meeting the conditions of *integrality* and being p-adically bounded.

[20.19] Generalized ideal class groups are idele class groups

Again, the class number above is the *absolute* class number. The *narrow* class group is ideals modulo principal ideals generated by *totally positive* elements.

For non-zero ideal $\mathfrak{a}$, the *narrow ray class group* mod $\mathfrak{a}$ is fractional ideals *prime to* $\mathfrak{a}$ modulo principal ideals $\alpha\mathfrak{o}$ generated by *totally positive* $\alpha = 1 \bmod \mathfrak{a}$.

Every generalized ideal class group is a quotient of one of these. That is, the narrow ray class groups are *cofinal* in the collection of generalized ideal class groups.

For example, $(\mathbb{Z}/N)^\times$ is the ray class group mod N for $\mathbb{Z}$ and $\mathbb{Q}$.

[20.20] Lemma: Generalized ideal class groups are *idele* class groups, quotients of the compact group $\mathbb{J}^1/k^\times$ by *open* subgroups.

Proof: Let i be the *ideal map* from ideles to non-zero fractional ideals:

$$i(\alpha) \ = \ \prod_{v<\infty} \mathfrak{p}_v^{\mathrm{ord}_v \alpha} \qquad\qquad (\text{for } \alpha \in \mathbb{J})$$

where $\mathfrak{p}_v$ is the prime ideal in $\mathfrak{o}$ attached to the place v. The subgroup that maps to ideals prime to $\mathfrak{a}$ is

$$G_\mathfrak{a} \ = \ \{\alpha \in \mathbb{J} \ : \ \alpha_v \in \mathfrak{o}_v^\times, \text{ for } v|\mathfrak{a}\}$$

With $k^\times$ imbedded diagonally in $\mathbb{J}$, the totally positive $\alpha \in k^\times$ congruent to 1 mod $\mathfrak{a}$ are the intersection of $k^\times$ with

$$U_\mathfrak{a} \;=\; \{\alpha \in \mathbb{J} \;:\; \alpha_v > 0 \text{ at } v \approx \mathbb{R},\; \alpha \in 1 + \mathfrak{a}\mathfrak{o}_v, \text{ for } v|\mathfrak{a}\}$$

The kernel of the ideal map on $\mathbb{J}$ is

$$K \;=\; \prod_{v|\infty} k_v^\times \;\times\; \prod_{v<\infty} \mathfrak{o}_v^\times \;\subset\; G_\mathfrak{a} \;\subset\; \mathbb{J}$$

That is, the corresponding generalized ideal class group is immediately rewrite-able as

$$C \;=\; i(G_\mathfrak{a})/i\big(U_\mathfrak{a} \cap k^\times\big) \;\approx\; G_\mathfrak{a}/\big(K \cdot (U_\mathfrak{a} \cap k^\times)\big)$$

Note that $G_\mathfrak{a} = K \cdot U_\mathfrak{a}$. The explicit claim is that

$$G_\mathfrak{a}/\big(K \cdot (U_\mathfrak{a} \cap k^\times)\big) \;\approx\; \mathbb{J}/\big((K \cap U_\mathfrak{a}) \cdot k^\times\big)$$

Subordinate to this: claim that, given an idele x there is $\alpha \in k^\times$ such that $\alpha^{-1} \cdot x$ is totally positive at $v \approx \mathbb{R}$, and $= 1 \bmod \mathfrak{a}\mathfrak{o}_v$ at $v|\mathfrak{a}$. That is, $k^\times \cdot U_\mathfrak{a} = \mathbb{J}$.

Toward the subordinate claim, consider the weaker claim that, given $x \in \mathbb{J}$, there is $\alpha \in k^\times$ with $\alpha^{-1}x \in \mathfrak{o}_v^\times$ for $v|\mathfrak{a}$. To prove this weaker claim, let $\mathfrak{o}_{(\mathfrak{a})}$ be $\mathfrak{o}$ localized at $\mathfrak{a}$: denominators prime to $\mathfrak{a}$ are allowed. This Dedekind domain has finitely-many primes, in bijection with those dividing $\mathfrak{a}$, and is a PID.

Thus, there is $\alpha \in \mathfrak{o}_{(\mathfrak{a})}$ such that $\alpha \cdot \mathfrak{o}_{(\mathfrak{a})} = i(x) \cdot \mathfrak{o}_{(\mathfrak{a})}$. Then $\alpha^{-1}x \in \mathfrak{o}_v^\times$ for all $v|\mathfrak{a}$, proving the weaker subordinate claim.

Sharpening this, Sun-Ze's theorem in $\mathfrak{o}_{(\mathfrak{a})}$ produces $\beta \in k^\times$ such that $\beta = \alpha^{-1}x_v \bmod \mathfrak{a}\mathfrak{o}_v$. Thus, $\beta^{-1}(\alpha^{-1}x) = 1 \bmod \mathfrak{a}\mathfrak{o}_v$ at $v|\mathfrak{a}$.

To prove the subordinate claim, it remains to adjust ideles at $v \approx \mathbb{R}$ without disturbing things at $v|\mathfrak{a}$.

We want $\gamma \in k^\times$ with $\gamma = 1 \bmod \mathfrak{a}\mathfrak{o}_v$ at $v|\mathfrak{a}$, and of specified *sign* at $v \approx \mathbb{R}$.

Recall that $\mathfrak{o}$ and any non-zero $\mathfrak{a}$ are *lattices* in k_∞, that is, $\mathfrak{a}$ is a *discrete* subgroup such that $k_\infty/\mathfrak{a}$ is *compact*. Thus, there is $\gamma \in 1 + \mathfrak{a}$ of specified sign at all $v \approx \mathbb{R}$. Thus, given $\beta^{-1}\alpha^{-1}x$, there exists $\gamma \in 1 + \mathfrak{a}$ such that $\gamma \cdot \beta^{-1}\alpha^{-1}x > 0$ at $v \approx \mathbb{R}$ and $= 1 \bmod \mathfrak{a}\mathfrak{o}_v$ at $v|\mathfrak{a}$. This proves the subordinate claim.

From the subordinate claim, the canonical injection

$$U_\mathfrak{a}/(U_\mathfrak{a} \cap k^\times) \;\approx\; (U_\mathfrak{a} \cdot k^\times)/k^\times \;\longrightarrow\; \mathbb{J}/k^\times$$

is an *isomorphism.* Recalling that $G_\mathfrak{a} = K \cdot U_\mathfrak{a}$, we obtain an isomorphism

$$G_\mathfrak{a}/\big(K \cdot (U_\mathfrak{a} \cap k^\times)\big) \;\approx\; U_\mathfrak{a}/\big((K \cap U_\mathfrak{a}) \cdot (U_\mathfrak{a} \cap k^\times)\big)$$

$$\approx\; (U_\mathfrak{a} \cdot k^\times)/\big((K \cap U_\mathfrak{a}) \cdot k^\times\big) \;\approx\; \mathbb{J}/\big((K \cap U_\mathfrak{a}) \cdot k^\times\big)$$

Thus, generalized ideal class groups are quotients of $\mathbb{J}/k^\times$ by open subgroups, so are finite. ///

[20.21] Closed subgroups of $\mathbb{R}^n$

The closed topological subgroups H of $V \approx \mathbb{R}^n$ are the following: for a *vector subspace* W of V, and for a *discrete* subgroup Γ of V/W,

$$H \;=\; q^{-1}(\Gamma) \qquad\qquad \text{(with } q : V \to V/W \text{ the quotient map)}$$

The *discrete* subgroups Γ of $V \approx \mathbb{R}^n$ are free $\mathbb{Z}$-modules $\mathbb{Z}v_1 + \ldots + \mathbb{Z}v_m$ on $\mathbb{R}$-linearly-independent vectors $v_j \in V$, with $m \le n$.

Proof: Induction on $n = \dim_{\mathbb{R}} V$. We already treated $n = 1$. When H contains a *line* L, reduce to a lower-dimensional question, as follows. Let $q : V \to V/L$ be the quotient map. Then $H = q^{-1}(q(H))$. With $H' = q(H)$, by induction, there is a vector subspace W' of V/L and discrete subgroup Γ' of $(V/L)/W'$ such that

$$H' \;=\; q'^{-1}(q'(\Gamma')) \qquad\qquad (\text{quotient } q' : V/L \to (V/L)/W')$$

Then

$$H \;=\; q^{-1}\Big(q(H)\Big) \;=\; q^{-1}\Big(q'^{-1}(\Gamma')\Big) \;=\; (q' \circ q)^{-1}(\Gamma')$$

The kernel of $q' \circ q$ is the vector subspace $N = q^{-1}(W')$ of V. It is necessary to check that $q(H) = H/N$ is a *closed* subgroup of V/N. It suffices to prove that $q^{-1}(V/N - q(H))$ is *open*. Since H contains N, $q^{-1}\big(q(H)\big) = H$, and

$$q^{-1}(V/N - qH) = V - q^{-1}(qH) \;=\; V - H \;=\; V - (\text{closed}) \;=\; \text{open}$$

This shows that $q(H)$ is closed, and completes the induction step when $\mathbb{R} \cdot h \subset H$.

Next show that H containing *no* lines is *discrete*. If not, then there are distinct h_i in H with an accumulation point h_o. Since H is closed, $h_o \in H$, and replace h_i by $h_i - h_o$ so that, without loss of generality, the accumulation point is 0. Without loss of generality, remove any 0s from the sequence. The sequence $h_i/|h_i|$ has an accumulation point e on the *unit sphere*, since the sphere is *compact*. Replace the sequence by a subsequence so that the $h_i/|h_i|$ *converge* to e. Given real $t \neq 0$, let $n \neq 0$ be an integer so that $|n - \frac{t}{|h_i|}| \le 1$. Then

$$|n \cdot h_i - te| \;\le\; \big|(n - \frac{t}{|h_i|})h_i\big| + \big|\frac{th_i}{|h_i|} - te\big| \;\le\; 1 \cdot |h_i| + |t| \cdot \big|\frac{h_i}{|h_i|} - e\big|$$

Since $|h_i| \to 0$ and $h_i/|h_i| \to e$, this goes to 0. Thus, te is in the closure of $\bigcup_i \mathbb{Z} \cdot h_i$. Thus, H contains the line $\mathbb{R} \cdot e$, *contradiction.* That is, H is discrete.

We claim that *discrete* H is generated as a $\mathbb{Z}$-module by at most n elements, and that these are $\mathbb{R}$-linearly independent. For $h_1, \ldots, h_m$ in H linearly *dependent* over $\mathbb{R}$, there are real numbers r_i so that

$$r_1 h_1 + \ldots + r_m h_m \;=\; 0$$

Re-ordering if necessary, suppose that $r_1 \neq 0$. Given a large integer N, let $a_i^{(N)}$ be integers so that $|r_i - a_i^{(N)}/N| < 1/N$. Then

$$\sum_i a_i^{(N)} h_i \;=\; N \sum_i \Big(\frac{a_i^{(N)}}{N} - r_i\Big) h_i + N \sum_i r_i h_i \;=\; N \sum_i \Big(\frac{a_i^{(N)}}{N} - r_i\Big) h_i + 0$$

Then

$$\Big|\sum_i a_i^{(N)} h_i\Big| \;\le\; N \sum_i \frac{1}{N} |h_i| \;\le\; \sum_i |h_i|$$

That is, for every N, the $\mathbb{Z}$-linear combination $\sum_i a_i^{(N)} h_i \in H$ is inside the ball of radius $\sum_i |h_i|$ centered at 0. Since H is discrete, there are only finitely-many *different* points of this form. Since $r_1 \neq 0$ and $|Nr_1 - a_1^{(N)}| < 1$, for large varying N the corresponding integers $a_1^{(N)}$ are *distinct.* Thus, for some large $N < N'$,

$$\sum_i a_i^{(N)} h_i \;=\; \sum_i a_i^{(N')} h_i$$

Subtracting,

$$\sum_i \big(a_i^{(N)} - a_i^{(N')}\big) h_i \;=\; 0 \qquad\qquad (\text{with } a_1^{(N)} - a_1^{(N')} \neq 0)$$

This is a non-trivial $\mathbb{Z}$-linear dependence relation among the h_i. Thus, $\mathbb{R}$-linear dependence implies $\mathbb{Z}$-linear dependence of the h_i in a *discrete* subgroup H. ///

[20.22] Topology on $\mathbb{J}$ versus subspace topology from $\mathbb{A}$ The topology on $\mathbb{J}$ is strictly finer than the subspace topology from $\mathbb{J} \subset \mathbb{A}$. In particular, it is obtained from the inclusion

$$\mathbb{J} \subset \mathbb{A} \times \mathbb{A} \qquad \text{by} \qquad \alpha \longrightarrow (\alpha, \alpha^{-1})$$

Proof: The crucial idea is that

$$\prod_{v<\infty} \mathfrak{o}_v \cap \big(\prod_{v<\infty} \mathfrak{o}_v\big)^{-1} \;=\; \prod_{v<\infty} \mathfrak{o}_v^\times$$

That is, a typical open in $\mathbb{J}_{\text{fin}}$ is the intersection of a typical open from $\mathbb{A}$ and its image under inversion.

The archimedean and finite-prime components truly are factors in $\mathbb{A} = k_\infty \times \mathbb{A}_{\text{fin}}$ and $\mathbb{J} = k_\infty^\times \times \mathbb{J}_{\text{fin}}$. The topology on $k_\infty^\times$ is *both* the subspace topology from $k_\infty^\times \subset k_\infty$, *and* from $k_\infty^\times \to k_\infty \times k_\infty$ by $\alpha \to (\alpha, \alpha^{-1})$. Thus, it suffices to prove the claim for the finite-prime parts. ///

21. *Toward Iwasawa-Tate on L-functions*

In complete parallel to the way Fourier transform on $\mathbb{R}$ and Fourier series on $\mathbb{R}/\mathbb{Z}$ give *Poisson summation*, which gives the *meromorphic continuation* and *functional equation* of the zeta function $\zeta(s)$, Fourier transform on archimedean *and* non-archimedean completions k_v, and on the adeles $\mathbb{A} = \mathbb{A}_k$, give *adelic Poisson summation*, then giving the Iwasawa-Tate modernization of [Hecke 1918], [Hecke 1920]'s treatment of the most general $GL(1)$ L-functions and zeta functions.

The idea to recast Hecke's discussion of zeta and L-functions of number fields using Chevalley's adeles and ideles was evidently in circulation by the mid 1940s. E. Artin's student Margaret Matchett's 1946 Ph.D. thesis [Matchett 1946] predated [Iwasawa 1950/1952], [Iwasawa 1952/1992], and [Tate 1950/1967]. Both Iwasawa and Tate gave more robust treatments, but neither appeared in print throughout the 1950s. Iwasawa's contributions on this subject are less well known than Tate's, as is visible in the common reference to *Tate's thesis* for what should arguably be *Iwasawa-Tate* theory.

The new ideas significantly diverge from 19th-century number theory, which was dominated by complex analysis and nascent commutative algebra, rather than harmonic analysis.

[21.1] Unitary duals of abelian topological groups:

For an abelian topological group G, the unitary dual $G^\vee$ is the collection of continuous group homomorphisms of G to the unit circle in $\mathbb{C}^\times$. For example, $\mathbb{R}^\vee \approx \mathbb{R}$, by $\xi \to (x \to e^{i\xi x})$.

[21.2] Claim:

$\mathbb{Q}_p^\vee \approx \mathbb{Q}_p$ and $\mathbb{A}^\vee \approx \mathbb{A}$. Since $\mathbb{C}^\times$ contains no *small subgroups* (below), and since $\mathbb{Q}_p$ is a union of *compact* subgroups, every element of $\mathbb{Q}_p^\vee$ has image in roots of unity in $\mathbb{C}^\times$, identified with $\mathbb{Q}/\mathbb{Z}$, so

$$\mathbb{Q}_p^\vee \;\approx\; \mathrm{Hom}^o(\mathbb{Q}_p,\, \mathbb{Q}/\mathbb{Z}) \qquad\qquad \text{(continuous homomorphisms)}$$

where $\mathbb{Q}/\mathbb{Z} = \mathrm{colim}\, \frac{1}{N}\mathbb{Z}/\mathbb{Z}$ is *discrete*. As a topological group, $\mathbb{Z}_p = \lim \mathbb{Z}/p^\ell\mathbb{Z}$, and $\mathbb{Z}_p$ is also a limit of the corresponding quotients of *itself*, namely,

$$\mathbb{Z}_p \;\approx\; \lim \mathbb{Z}_p/p^\ell\mathbb{Z}_p$$

More generally, an abelian *totally disconnected* topological group G is such a limit of quotients:

$$G \;\approx\; \lim_K G/K \qquad\qquad (K \text{ compact open subgroup})$$

As a topological group,

$$\mathbb{Q}_p \;=\; \bigcup \frac{1}{p^\ell}\mathbb{Z}_p \;=\; \mathrm{colim}\, \frac{1}{p^\ell}\mathbb{Z}_p$$

Because of the *no small subgroups* (below) property of the unit circle in $\mathbb{C}^\times$, every continuous element of $\mathbb{Z}_p^\vee$ factors through some limitand

$$\mathbb{Z}_p/p^\ell\mathbb{Z}_p \;\approx\; \mathbb{Z}/p^\ell\mathbb{Z}$$

Thus,

$$\mathbb{Z}_p^\vee \;=\; \mathrm{colim}\, \Big(\mathbb{Z}_p/p^\ell\mathbb{Z}_p\Big)^\vee \;=\; \mathrm{colim}\, \frac{1}{p^\ell}\mathbb{Z}_p/\mathbb{Z}_p$$

since $\frac{1}{p^\ell}\mathbb{Z}_p/\mathbb{Z}_p$ is the dual to $\mathbb{Z}_p/p^\ell\mathbb{Z}_p$ under the pairing

$$\frac{1}{p^\ell}\mathbb{Z}_p/\mathbb{Z}_p \,\times\, \mathbb{Z}_p/p^\ell\mathbb{Z}_p \;\approx\; \frac{1}{p^\ell}\mathbb{Z}/\mathbb{Z} \,\times\, \mathbb{Z}/p^\ell\mathbb{Z}$$

by

$$(\frac{x}{p^\ell} + \mathbb{Z}) \,\times\, (y + p^\ell\mathbb{Z}) \;\longrightarrow\; xy + \mathbb{Z} \,\in\, \mathbb{Q}/\mathbb{Z}$$

The transition maps in the colimit expression for $\mathbb{Z}_p^\vee$ are inclusions, so

$$\mathbb{Z}_p^\vee \;=\; \mathrm{colim}\, \frac{1}{p^\ell}\mathbb{Z}_p/\mathbb{Z}_p \;\approx\; \Big(\mathrm{colim}\, \frac{1}{p^\ell}\mathbb{Z}_p\Big)/\mathbb{Z}_p \;\approx\; \mathbb{Q}_p/\mathbb{Z}_p$$

Thus,

$$\mathbb{Q}_p^\vee \;=\; \Big(\mathrm{colim}\, \frac{1}{p^\ell}\mathbb{Z}_p\Big)^\vee \;=\; \lim \frac{1}{p^\ell}\mathbb{Z}_p^\vee$$

As a topological group, $\frac{1}{p^\ell}\mathbb{Z}_p \approx \mathbb{Z}_p$ by multiplying by p^ℓ, so the dual of $\frac{1}{p^\ell}\mathbb{Z}_p$ is isomorphic to $\mathbb{Z}_p^\vee \approx \mathbb{Q}_p/\mathbb{Z}_p$. However, the inclusions for varying ℓ are not the identity map, so for compatibility take

$$\Big(\frac{1}{p^\ell}\mathbb{Z}_p\Big)^\vee \;=\; \mathbb{Q}_p/p^\ell\mathbb{Z}_p$$

Thus,

$$\mathbb{Q}_p^\vee \;=\; \lim \mathbb{Q}_p/p^\ell\mathbb{Z}_p \;\approx\; \mathbb{Q}_p$$

because, $\mathbb{Q}_p$ is the projective limit of its quotients by compact open subgroups. ///

[21.3] Claim: Both $\mathbb{A}^\vee \approx \mathbb{A}$ and $\mathbb{A}_{\mathrm{fin}}^\vee \approx \mathbb{A}_{\mathrm{fin}}$.

Proof: The same argument applies to $\widehat{\mathbb{Z}} = \lim \mathbb{Z}/N\mathbb{Z}$ and finite adeles $\mathbb{A}_{\mathrm{fin}} = \mathrm{colim}\, \frac{1}{N}\widehat{\mathbb{Z}}$, proving the self-duality of $\mathbb{A}_{\mathrm{fin}}$. Then the self-duality of $\mathbb{R}$ gives the self-duality of $\mathbb{A}$. ///

[21.4] Remark: $\widehat{\mathbb{Z}}$ does also refer to $\mathrm{Hom}^o(\mathbb{Z}, \mathbb{Q}/\mathbb{Z})$, but needs to be *topologized* by the compact-open topology [later].

[21.5] Remark: Essentially the same argument applies for an arbitrary finite extension k of $\mathbb{Q}$.

[21.6] Corollary: Given *non-trivial* $\psi \in \mathbb{Q}_p^\vee$, every other element of $\mathbb{Q}_p^\vee$ is of the form $x \to \psi(\xi \cdot x)$ for some $\xi \in \mathbb{Q}_p$. Similarly, given *non-trivial* $\psi \in \mathbb{A}^\vee$, every other element of $\mathbb{A}^\vee$ is of the form $x \to \psi(\xi \cdot x)$ for some $\xi \in \mathbb{A}$. [Proof below]

[21.7] Remark: This sort of result is already familiar from the analogue for $\mathbb{R}$, that $x \to e^{i\xi x}$ for $\xi \in \mathbb{R}$ are all the unitary characters of $\mathbb{R}$.

[21.8] Compact-discrete duality For abelian topological groups G, pointwise multiplication makes $\widehat{G}$ an abelian group. A reasonable topology on $\widehat{G}$ is the *compact-open* topology, with a sub-basis

$$U \;=\; U_{C,E} \;=\; \{f \in \widehat{G} \;:\; f(C) \subset E\}$$

for compact $C \subset G$, open $E \subset S^1$.

[21.9] Remark: The reasonable-ness of this topology is functional. For a compact topological space X, $C^o(X)$ with the *sup-norm* is a *Banach space* . On non-compact X, the semi-norms given by *sups on compacts* make $C^o(X)$ a *Fréchet space.* The compact-open topology is the analogue for $C^o(X,Y)$ where the target Y is not normed. When X, Y are topological groups, the continuous functions $f : X \to Y$ consisting of *group homomorphisms* is a (locally compact, Hausdorff) topological group. [Later]

Granting (for now) that the compact-open topology makes $\widehat{G}$ an abelian (locally-compact, Hausdorf) topological group,

[21.10] Theorem: The unitary dual of a *compact* abelian group is *discrete.* The unitary dual of a *discrete* abelian group is *compact.*

Proof: Let G be compact. Let E be a small-enough open in S^1 so that E contains no non-trivial subgroups of G. Using the compactness of G itself, let $U \subset \widehat{G}$ be the open

$$U \;=\; \{f \in \widehat{G} \;:\; f(G) \subset E\}$$

Since E is *small*, $f(G) = \{1\}$. That is, f is the trivial homomorphism. This proves discreteness of $\widehat{G}$ for compact G.

For G discrete, *every* group homomorphism to S^1 is continuous. The space of *all* functions $G \to S^1$ is the cartesian product of copies of S^1 indexed by G. By Tychonoff's theorem, this product is *compact*. For *discrete* X, the compact-open topology on the space $C^o(X,Y)$ of continuous functions from $X \to Y$ *is* the product topology on copies of Y indexed by X.

The set of functions f satisfying the group homomorphism condition

$$f(gh) \;=\; f(g)\cdot f(h) \qquad\qquad (\text{for } g,h \in G)$$

is *closed*, since the group multiplication $f(g) \times f(h) \to f(g)\cdot f(h)$ in S^1 is continuous. Since the product is also *Hausdorff*, $\widehat{G}$ is also compact. ///

[21.11] Theorem: $(\mathbb{A}/k)^\frown \approx k$. In particular, given any non-trivial character ψ on $\mathbb{A}/k$, *all* characters on $\mathbb{A}/k$ are of the form $x \to \psi(\alpha\cdot x)$ for some $\alpha \in k$.

Proof: For a (discretely topologized) number field k with adeles $\mathbb{A}$, $\mathbb{A}/k$ is *compact*, and $\mathbb{A}$ is *self-dual*.

Because $\mathbb{A}/k$ is compact, $(\mathbb{A}/k)^\frown$ is *discrete*. Since multiplication by elements of k respects cosets $x+k$ in $\mathbb{A}/k$, the unitary dual has a k-vectorspace structure given by

$$(\alpha\cdot\psi)(x) \;=\; \psi(\alpha\cdot x) \qquad\qquad (\text{for } \alpha \in k,\, x \in \mathbb{A}/k)$$

There is no topological issue in this k-vectorspace structure, because $(\mathbb{A}/k)^\frown$ is discrete. The quotient map $\mathbb{A} \to \mathbb{A}/k$ gives a natural *injection* $(\mathbb{A}/k)^\frown \to \widehat{\mathbb{A}}$.

Given non-trivial $\psi \in (\mathbb{A}/k)^\frown$, the k-vectorspace $k\cdot\psi$ inside $(\mathbb{A}/k)^\frown$ injects to a copy of $k\cdot\psi$ inside $\widehat{\mathbb{A}} \approx \mathbb{A}$. *Assuming* for a moment that the image in $\mathbb{A}$ is essentially the same as the diagonal copy of k, $(\mathbb{A}/k)^\frown/k$ injects to $\mathbb{A}/k$. The topology of $(\mathbb{A}/k)^\frown$ is discrete, and the quotient $(\mathbb{A}/k)^\frown/k$ is still discrete. These maps are continuous group homs, so the image of $(\mathbb{A}/k)^\frown/k$ in $\mathbb{A}/k$ is a discrete subgroup of a compact group, so is *finite*. Since $(\mathbb{A}/k)^\frown$ is a k-vectorspace, $(\mathbb{A}/k)^\frown/k$ is a singleton. Thus, $(\mathbb{A}/k)^\frown \approx k$, if the image of $k\cdot\psi$ in $\mathbb{A} \approx \widehat{\mathbb{A}}$ is the usual diagonal copy.

To see how $k\cdot\psi$ is imbedded in $\mathbb{A} \approx \widehat{\mathbb{A}}$, fix non-trivial ψ on $\mathbb{A}/k$, and let ψ be the induced character on $\mathbb{A}$. The self-duality of $\mathbb{A}$ is that the action of $\mathbb{A}$ on $\widehat{\mathbb{A}}$ by $(x\cdot\psi)(y) = \psi(xy)$ gives an *isomorphism*. The subgroup $x\cdot\psi$ with $x \in k$ is certainly the usual diagonal copy. ///

[21.12] No small subgroups

The circle group S^1 *has no small subgroups*, in the sense that there is a neighborhood U of the identity $1 \in S^1$ such that the only subgroup of S^1 inside U is the trivial group $\{1\}$.

Essentially the same proof works for *real Lie groups*. Use the copy of S^1 inside the complex plane. We claim that taking

$$U \;=\; S^1 \cap \{z \in \mathbb{C} : \mathrm{Re}(z) > 0\}$$

suffices: the only subgroup G of S^1 inside this U is $G = \{1\}$. Indeed, suppose not. Let $1 \neq e^{i\theta} \in G \cap U$. We can take $0 < \theta < \pi/2$, since both $\pm\theta$ must appear. Let $0 < \ell \in \mathbb{Z}$ be the smallest such that $\ell\cdot\theta > \pi/2$. Then, since $(\ell-1)\cdot\theta < \pi/2$ and $0 < \theta < \pi/2$,

$$\frac{\pi}{2} \;<\; \ell\cdot\theta \;=\; (\ell-1)\cdot\theta+\theta \;<\; \frac{\pi}{2}+\frac{\pi}{2} \;=\; \pi$$

Thus, $\ell\cdot\theta$ falls outside U, contradiction. ///

[21.13] Intrinsic integration on $\mathbb{R}/\mathbb{Z}$ Quotients $\Gamma\backslash G$ such as $\mathbb{R}/\mathbb{Z}$ have a reasonable integration theory *without* finding/constructing/using a so-called *fundamental domain.* Intrinsic integration on quotients is essential for situations $\Gamma\backslash G$ where determination of a fundamental domain is complicated or impossible.

[21.14] Example: We *want* a continuous linear map (integral!) $F \to \int_{\mathbb{R}/\mathbb{Z}} F(x)\,dx$ on $C_c^o(\mathbb{R}/\mathbb{Z})$ (think of the Riesz-Markov-Kakutani representation theorem), translation-invariant, non-negative for non-negative F, and with the essential compatibility

$$\int_{\mathbb{R}/\mathbb{Z}} \Big(\sum_{n\in\mathbb{Z}} f(x+n)\Big)\,dx \;=\; \int_{\mathbb{R}} f(x)\,dx \qquad (\text{for } f\in C_c^o(\mathbb{R}))$$

Try to *define* the integral on $\mathbb{R}/\mathbb{Z}$ by this relation. *Well-definedness* is an issue, since the same $F(x) = \sum_n f(x+n)$ in $C_c^o(\mathbb{R}/\mathbb{Z})$ can arise by *periodicizing* two functions f in $C_c^o(\mathbb{R})$. The complementary question is whether every $F\in C_c^o(\mathbb{R}/\mathbb{Z})$ is obtained by periodicizing *some* $f\in C_c^o(\mathbb{R})$.

Later, we will prove that this succeeds even in very general circumstances, but first consider the simple case of $\mathbb{R}\to\mathbb{R}/\mathbb{Z}$.

[21.15] Lemma: The averaging map

$$\alpha : C_c^o(\mathbb{R}) \to C_c^o(\mathbb{R}/\mathbb{Z}) \qquad\text{by}\qquad \alpha f(x) \;=\; \sum_{n\in\mathbb{Z}} f(x+n)$$

is *surjective.*

Proof: Let q be the quotient map $q:\mathbb{R}\to\mathbb{R}/\mathbb{Z}$. Given $F\in C_c^o(\mathbb{R}/\mathbb{Z})$, let C' be a compact subset of $\mathbb{R}$ such that $q(C')\supset \mathrm{spt}(F)$. For example, $C'=[0,2]$ suffices. Let φ be in $C_c^o(\mathbb{R})$ identically 1 on C', and non-negative everywhere. Let

$$g(x) \;=\; \varphi(x)\cdot F(x) \in C_c^o(\mathbb{R})$$

Since F is already left $\mathbb{Z}$-invariant

$$\alpha(g) \;=\; \alpha(\varphi\cdot F) \;=\; \alpha\varphi\cdot F$$

Since $\alpha(\varphi)>0$ on C', it has a strictly positive lower bound there. Thus, we can divide g by $\alpha\varphi$, and

$$\alpha(g/\alpha\varphi) \;=\; \alpha\varphi\cdot F/\alpha\varphi \;=\; F$$

This gives surjectivity. ///

For *well-definedness*, it suffices to prove that $\alpha f = 0$ implies $\int_{\mathbb{R}} f(x)\,dx = 0$. Suppose $\alpha f=0$. For all $F\in C_c^o(\mathbb{R})$, the integral of F against αf is certainly 0, and we rearrange

$$0 \;=\; \int_{\mathbb{R}} F(x)\,\alpha f(x)\,dx \;=\; \int_{\mathbb{R}} \sum_{n\in\mathbb{Z}} F(x)\,f(x+n)\,dx$$

$$=\; \sum_{n\in\mathbb{Z}} \int_{\mathbb{R}} F(x)\,f(x+n)\,dx \;=\; \int_{\mathbb{R}} \sum_{n\in\mathbb{Z}} F(x-n)\,f(x)\,dx$$

Replace n by $-n$, giving

$$0 \;=\; \int_{\mathbb{R}} \alpha F(x)\, f(x)\, dx$$

By surjectivity of α, there is F with $\alpha F = 1$ on the support of f. Then the integral of f is 0, proving the well-definedness. ///

More generally, replace $\mathbb{R}$ by a topological group G, and $\mathbb{Z}$ by a closed subgroup H. Given right-translation-invariant measures on G and H, we want a unique measure $d\dot{g}$ on $H\backslash G$ such that

$$\int_{H\backslash G} \int_H f(h\dot{g})\; dh\, d\dot{g} \;=\; \int_G f(g)\; dg$$

The same proof almost works.

[21.16] Left-invariant versus right-invariant measures

When H and G are non-abelian and non-compact, a technical issue can arise: *left* translation produces a slightly different *right* translation-invariant measure. By uniqueness of Haar measure, this translated measure differs at most by a constant from the given Haar measure.

In general, left translation *does* change the right translation-invariant measure by a non-trivial constant, called the *modular function*

$$d(xg) = \Delta_G(x)\cdot dg \qquad\qquad d(yh) = \Delta_H(y)\cdot dh$$

For straightforward reasons, the condition for existence of a right G-invariant measure on $H\backslash G$ is that

$$\Delta_G \text{ restricted to } H \quad = \quad \Delta_H$$

This modular function condition is obtained from

$$\int_{H\backslash G} \int_H f(hg)\; dh\, dg \;=\; \int_G f(g)\; dg$$

by change of variables: replace h by hx for $x \in H$, and g by $x^{-1}g$.

Having a non-trivial modular function is not a pathology, but very reasonable in certain circumstances. Nevertheless, it is convenient that $\Delta_G \cong 1$ for many G. Such G are called *unimodular*.

$\Delta_G \cong 1$ for *abelian* G, because $d(xg) = d(gx)$. Below, we show that Δ_G is a *continuous group homomorphism* to $(0, +\infty)$ with multiplication.

Since $(0, +\infty)$ has no proper compact subgroups, $\Delta_G \cong 1$ for *compact* G.

Since $(0, +\infty)$ is *abelian*, Δ_G is 1 on the commutator subgroup $[G, G]$ of G, generated by all commutators $[g, h] = ghg^{-1}h^{-1}$. Thus, G is unimodular when $G = [G, G]$ or even when $G/[G, G]$ is *compact*.

We show later that $G = SL_2(\mathbb{R})$, the group of two-by-two real matrices with determinant 1, is equal to its commutator subgroup $[G, G]$, so is unimodular.

A non-pathological *not*-unimodular example is

$$G \;=\; \{\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} \;:\; y > 0,\; x \in \mathbb{R}\}$$

In those coordinates, *right* Haar measure is (!) $dg \;=\; dx\,\dfrac{dy}{y}$ with Lebesgue measures on $\mathbb{R}$. *Left* multiplication by $\begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix}$ changes the measure by t, so $\Delta_G \begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix} = t$.

[21.17] Minkowski's results on convex bodies Minkowski showed that, a *convex* subset C of V, symmetric about 0, with measure strictly greater than 2^n times the measure of V/L, contains a point of L other than 0. This is a foundational element of his *Geometry of Numbers.*

This is a corollary of the measure-theoretic pigeon-hole principle: with $E = \frac{1}{2} \cdot C$, the measure of E is more than the measure of V/L, and we've shown that there are $x \neq y \in E$ such that $x - y \in L$. The condition $x \neq y$ gives $x - y \neq 0$. Evidently, we claim $E - E = C$.

One half of $E - E = C$ is easy: using the symmetry of C,

$$E - E \;=\; \tfrac{1}{2} \cdot C - \tfrac{1}{2} \cdot C \;=\; \tfrac{1}{2} \cdot C + \tfrac{1}{2} \cdot C \;\supset\; C$$

The other direction uses the convexity, also:

$$\tfrac{1}{2} \cdot C + \tfrac{1}{2} \cdot C \;=\; \{\frac{x+y}{2} : x, y \in C\} \;\subset\; C$$

Thus, $E - E = C$, and Minkowski's theorem follows from the measure-theoretic pigeon-hole principle.
///

[21.18] Remark: The convexity and symmetry and having the ambient group be $\mathbb{R}^n$ are misleading specifics, even though this is a very important application.

[21.19] Invariant integrals on quotients Inspection of the arguments shows that we want very few things from (right-invariant) integrals on groups G, and these few features *characterize* the integrals completely, as we see:

$$\begin{cases} f \to \int_G f(g)\,dg \text{ defined on } C_c^o(G) & \text{(functionals on } C_c^o(G)) \\ \int_G f(gh)\,dg = \int_G f(g)\,dg \text{ for } h \in G & \text{(right invariance)} \\ f \geq 0 \Longrightarrow \int_G f(g)\,dg \geq 0 & \text{(positivity)} \end{cases}$$

In fact, the positivity condition implies that $f \to \int_G f$ is a *continuous* linear functional on $C_c^o(G)$ in its natural topology, but the arguments here only use the positivity.

For context: the usual *Riesz-Markov-Kakutani representation theorem* (*not* the more elementary Riesz-Fréchet theorem about continuous functionals on Hilbert spaces), also uses only *positivity*, not giving any topology on $C_c^o(X)$, for X the locally compact, Hausdorff, preferably countably-based topological space in question.

The theorem asserts that, given a *positive* linear functional λ on $C_c^o(X)$, there is a positive Borel measure μ so that

$$\lambda(f) \;=\; \int_X f(x)\; d\mu(x)$$

The countably-based hypothesis promises that there is *regular* μ, meaning that $\mu(E)$ is both the *sup* of $\mu(C)$ for compact $C \subset E$, and the *inf* of $\mu(U)$ for open $U \supset E$.

Without this hypothesis, regularity is not guaranteed, but we are almost entirely interested in countably-based topological spaces, such as $\mathbb{R}, \mathbb{Q}_p, \mathbb{A}, \mathbb{J}$.

Minkowski's theorem about lattice-points in convex bodies in $\mathbb{R}^n$ abstracts to:

[21.20] Claim: For *discrete* Γ in *unimodular* topological group G, such that $\Gamma\backslash G$ has finite invariant measure, if a set $E \subset G$ has measure strictly greater than $\Gamma\backslash G$, then there are $x \neq y \in E$ such that $x^{-1}y \in \Gamma$.

Proof: Recapitulating the argument: the modular-function condition for existence of measures is met. With f the characteristic function of E, if there were *no* such x, y, then $\sum_{\gamma\in\Gamma} f(\gamma \cdot x) \leq 1$. But then

$$\text{meas}\,(\Gamma\backslash G) \;< \int_G f(g)\,dg \;=\; \int_{\Gamma\backslash G} \Big(\sum_{\gamma\in\Gamma} f(\gamma \cdot g)\Big)\; dg \;\leq\; \text{meas}\,(\Gamma\backslash G)$$

Impossible. So there *is* $1 \neq x^{-1}y \in \Gamma$. ///

[21.21] Finite volume quotients

We understand that quotients of real vector spaces by lattices, such as $\mathbb{R}^n/\mathbb{Z}^n$, have finite volume, but we have much less experience with discrete subgroups Γ in *non-abelian* G. The exemplar of a finite-volume but non-compact quotient is

$$SL_n(\mathbb{Z})\backslash SL_n(\mathbb{R}) \qquad\qquad (SL_n(R) = n \times n \text{ matrices, entries in } R)$$

Minkowski and Siegel knew that this quotient had finite volume long ago. It is not obvious that this volume is finite. Below, we compute the volume in terms of special values of $\zeta(s)$.

Back to the main existence theorem: given right-translation-invariant measures on $H \subset G$, and assuming the compatibility

$$\Delta_G \text{ restricted to } H \;=\; \Delta_H$$

there is a unique measure $d\dot{g}$ on $H\backslash G$ such that

$$\int_{H\backslash G} \int_H f(h\dot{g})\, dh\, d\dot{g} \;=\; \int_G f(g)\, dg$$

As in the prototypical case of $H = \mathbb{Z}$ and $G = \mathbb{R}$, the idea is to *define* the integral on $H\backslash G$ by this condition, and show that it is sufficiently-defined, and well-defined.

We (re-) prove the sufficiency starting from the existence of Haar measures on G and on H. First suppose that both are *unimodular*. With averaging map $\alpha : C_c^o(G) \to C_c^o(H\backslash G)$

$$\alpha f(g) \;=\; \int_H f(hg)\, dh \qquad\qquad (\text{for } f \in C_c^o(G))$$

attempt to define an integral on $C_c^o(H\backslash G)$ by

$$\int_{H\backslash G} \alpha f(\dot{g})\, d\dot{g} \;=\; \int_G f(g)\, dg$$

We (re-) prove surjectivity of the averaging map α. Let q be the quotient map $q : G \to H\backslash G$.

Given $F \in C_c^o(H\backslash G)$, we need a compact subset C' of G such that $q(C') \supset \mathrm{spt}(F)$. By *local compactness* of G, there is open $U \ni 1$ with compact closure $\overline{U}$. Quotient maps are *open*, so $q(U)$ is open in $H\backslash G$, as are $q(U) \cdot G$ for $g \in G$. Certainly

$$\mathrm{spt}F \;\subset\; \bigcup_{g \in G} q(U) \cdot g$$

so by compactness of sptFC there is a finite subcover $\bigcup_i q(U) \cdot g_i$. The set $\bigcup_i \overline{U} \cdot g_i$ is compact in G, and its image under q contains spt$F$.

Let φ be in $C_c^o(G)$ identically 1 on a neighborhood of C', by Urysohn's lemma. [5] Let

$$g(x) \;=\; \varphi(x) \cdot F(x) \in C_c^o(G)$$

Since F is already left H-invariant

$$\alpha(g) \;=\; \alpha(\varphi \cdot F) \;=\; \alpha\varphi \cdot F$$

[5] Recall that, for open set U containing compact C in a locally-compact Hausdorff topologicaly space X, Urysohn's Lemma constructs $f \in C_c^o(X)$ which is identically 1 on C, and identically 0 off U.

Since $\alpha(\varphi) > 0$ on a compact containing the support of F, it has a strictly positive bound on that compact.

$$\alpha(F/\alpha\varphi) = \alpha\varphi \cdot F/\alpha\varphi = F$$

and the quotient $F/\alpha(\varphi)$ is continuous. [6] This gives surjectivity.

Now (re-) prove *well-definedness*: if $\alpha f = 0$, then $\int_G f(g)\,dg = 0$. Suppose $\alpha f = 0$. For all $F \in C_c^o(G)$, the integral of F against αf is certainly 0, and we rearrange

$$0 \;=\; \int_G F(g)\,\alpha f(g)\,dg \;=\; \int_G\int_H F(g)\,f(hg)\,dh\,dg$$

$$=\; \int_H\int_G F(h^{-1}g)\,f(g)\,dg\,dh$$

replacing g by $h^{-1}g$. Replace h by h^{-1}, so $0 = \displaystyle\int_G \alpha F(g)\,f(g)\,dg$ Surjectivity of α gives F with αF is identically 1 on the support of f. Thus, the integral of f is 0, proving the well-definedness for unimodular H and G. ///

[21.22] **Remark:** We did *not* use formulas for the integrals.

[21.23] **Another missing item** In the proof of Fujisaki's lemma we presumed that, for *idele* α, the change-of-measure on $\mathbb{A}$ is

$$\frac{\text{meas}\,(\alpha E)}{\text{meas}\,(E)} = |\alpha| \qquad\qquad \text{(for measurable } E \subset \mathbb{A})$$

This will be examined a bit later.

22. *Volume of* $SL_n(\mathbb{Z})\backslash SL_n(\mathbb{R})$

Finite volume of $\mathbb{R}^n/\mathbb{Z}^n$ is familiar, but we have essentially *no* experience with discrete subgroups Γ in non-abelian G. The following is a prototype both for the assertion and for the proof mechanisms.

[22.1] **Claim:** The quotient $\Gamma\backslash G = SL_n(\mathbb{Z})\backslash SL_n(\mathbb{R})$ has finite invariant volume (where $SL_n(R) = n \times n$ matrices with entries in ring R). In fact, in a natural normalization,

$$\text{vol}\,(SL(n,\mathbb{Z})\backslash SL(n,\mathbb{R})) \;=\; \zeta(2)\,\zeta(3)\,\zeta(4)\,\zeta(5)\ldots\zeta(n)$$

[22.2] **Remark:** Indeed, mysterious $\zeta(\text{odd})$ values appear. Minkowski knew the finiteness, and Siegel computed the value. We grant the finiteness, and compute the volume *without* a *fundamental domain.*

Proof: (modernization of Siegel's argument) The point is

$$\int_{\Gamma\backslash G}\sum_{\gamma\in\Gamma} f(\gamma g)\,dg \;=\; \int_G f(g)\,dg$$

Treat $n = 2$, $G = SL(2,\mathbb{R})$, and $\Gamma = SL(2,\mathbb{Z})$. We showed that a right G-invariant measure on $\Gamma\backslash G$ is described by integrals of $C_c^o(\Gamma\backslash G)$. Every $F \in C_c^o(\Gamma\backslash G)$ is expressible as

$$F(g) \;=\; \sum_{\gamma\in\Gamma} f(\gamma\cdot g) \qquad\qquad \text{(for some } f \in C_c^o(G))$$

[6] One might worry about what happens off C', but this is a subordinate, easier issue.

and the integral of F is sufficiently-defined and well-defined by

$$\int_{\Gamma\backslash G} F(g)\,dg \;=\; \int_{\Gamma\backslash G}\sum_{\gamma\in\Gamma} f(\gamma\cdot g)\,dg \;=\; \int_G f(g)\,dg$$

Although we do *not* describe the geometry of $\Gamma\backslash G$, we *do* need details about the Haar measure on G, since a constant ambiguous by a constant is not interesting.

[22.3] Claim: $G = SL_n(\mathbb{R})$ is *unimodular*, since G is its own commutator subgroup. In particular, any group homomorphism from G to an abelian group is *trivial.*

Proof: We prove that, for a field k with at least 4 elements, $SL_2(k)$ is generated by commutants $[g,h] = ghg^{-1}h^{-1}$. The case $n > 2$ is easy to obtain from this. First,

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1}\end{pmatrix}\begin{pmatrix} 1 & b \\ 0 & 1\end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & a^{-1}\end{pmatrix}^{-1}\begin{pmatrix} 1 & b \\ 0 & 1\end{pmatrix}^{-1} \;=\; \begin{pmatrix} 1 & b(a^2-1) \\ 0 & 1\end{pmatrix}$$

Thus, for k such that a^2 is not 1 for all $a \in k^\times$, every element $\begin{pmatrix} 1 & * \\ 0 & 1\end{pmatrix}$ is a commutant. Similarly, every element $\begin{pmatrix} 1 & 0 \\ * & 1\end{pmatrix}$ is a commutant. Then

$$\begin{pmatrix} 1 & 0 \\ c & 1\end{pmatrix}\begin{pmatrix} 1 & b \\ 0 & 1\end{pmatrix} \;=\; \begin{pmatrix} 1 & b \\ c & 1+cb\end{pmatrix}$$

And toward diagonal matrices:

$$\begin{pmatrix} 1 & b \\ c & 1+cb\end{pmatrix}\begin{pmatrix} 1 & 0 \\ \frac{-c}{1+cb} & 1\end{pmatrix} \;=\; \begin{pmatrix} \frac{1}{1+cb} & b \\ 0 & 1+cb\end{pmatrix}$$

and

$$\begin{pmatrix} \frac{1}{1+cb} & b \\ 0 & 1+cb\end{pmatrix}\begin{pmatrix} 1 & \frac{-b}{1+cb} \\ 0 & 1\end{pmatrix} \;=\; \begin{pmatrix} \frac{1}{1+cb} & 0 \\ 0 & 1+cb\end{pmatrix}$$

In particular, this works with $c = 1$. Thus, given $a \in k^\times$, take $b = a^{-1} - 1$ to obtain $\begin{pmatrix} a & 0 \\ 0 & a^{-1}\end{pmatrix}$. The *Bruhat decomposition* is directly verifiable here:

$$SL_2(k) \;=\; \begin{pmatrix} * & * \\ 0 & *\end{pmatrix} \cup \begin{pmatrix} * & * \\ 0 & *\end{pmatrix} w \begin{pmatrix} 1 & * \\ 0 & 1\end{pmatrix} \qquad\qquad (\text{with } w = \begin{pmatrix} 0 & -1 \\ 1 & 0\end{pmatrix})$$

it suffices to show that the Weyl element w is in the subgroup generated by commutators. Starting from $\begin{pmatrix} 1 & b \\ c & 1+cb\end{pmatrix}$ again, with $c = 1$,

$$\begin{pmatrix} 1 & -1 \\ 0 & 1\end{pmatrix}\begin{pmatrix} 1 & b \\ 1 & 1+b\end{pmatrix} \;=\; \begin{pmatrix} 0 & -1 \\ 1 & 1+b\end{pmatrix}$$

and

$$\begin{pmatrix} 1 & 0 \\ b & 1\end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 1+b\end{pmatrix} \;=\; \begin{pmatrix} 0 & -1 \\ 1 & 0\end{pmatrix} \;=\; w$$

Thus, the commutants generate all of $SL_2(k)$. ///

To describe the measure on G usefully, we do need coordinates on G, but not the naive $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Let K be the usual *special orthogonal group*

$$K = SO(2) = \{g \in G : g^\top g = 1_2\} \;=\; \{\begin{pmatrix} \cos t & \sin t \\ -\sin t & \cos t \end{pmatrix}\}$$

and

$$P^+ = \{\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} : a > 0,\ b \in \mathbb{R}\}$$

Compact K is unimodular, while P^+ is *not*. The *Iwasawa decomposition* is directly verifiable here:

$$G \;=\; P^+ \cdot K \;\approx\; P^+ \times K$$

[22.4] Lemma: Haar measure on G is $d(pk) = dp \cdot dk$, where dp is *left* Haar measure on P^+, and dk is *right* Haar on K. That is,

$$\int_G \varphi(g)\, dg \;=\; \int_{P^+} \int_K \varphi(pk)\, dk\, dp \qquad\qquad (\text{for } \varphi \in C_c^o(G))$$

Proof: Let the group $P^+ \times K$ act on G by $(p \times k)(g) = p^{-1} g k$. (The inverse is for associativity!) The isotropy subgroup in $P^+ \times K$ of $1 \in G$ is $\{p \times k : p^{-1} \cdot 1 \cdot k = 1\} = P^+ \cap K = \{1\}$. By uniqueness of invariant measures, there is a unique $P^+ \times K$-invariant measure on G, and it fits into $\int_G = \int_P \int_K$. The Haar measure on G gives such a thing, as does a Haar measure on G. ///

Now completely specify the Haar measure on G. Normalize the Haar measure on the circle (!) $K = SO(2, \mathbb{R})$ to have total measure 2π. Normalize the left Haar measure dp on P^+ to (!)

$$d\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \;=\; \frac{1}{t^2}\, dx\, \frac{dt}{t} \qquad\qquad (x \in \mathbb{R} \text{ and } t > 0)$$

Corresponding to a nice (Schwartz?) function f on $\mathbb{R}^2$, let F on G be

$$F(g) \;=\; \sum_{v \in \mathbb{Z}^2} f(vg)$$

By design, this function F is left Γ-invariant. Evaluating

$$\int_{\Gamma\backslash G} F(g)\, dg$$

in two different ways will determine the volume of $\Gamma\backslash G$.

[22.5] Lemma: Given *coprime* $c, d \in \mathbb{Z}$, there exists $\begin{pmatrix} * & * \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$.

Proof: The ideal $\mathbb{Z}c + \mathbb{Z}d$ is $\mathbb{Z}$, so there are $a, b \in \mathbb{Z}$ such that $ad + bc = 1$. Then $\begin{pmatrix} a & -b \\ c & d \end{pmatrix} \in \Gamma$. ///

Thus, for a fixed positive integer ℓ, the set $\{(c, d) : \gcd(c, d) = \ell\}$ is an *orbit* of Γ in $\mathbb{Z}^2$. Take $(0, 1)$ as convenient base point and observe that

$$\mathbb{Z}^2 - \{0\} \;=\; \{\ell \cdot (0, 1) \cdot \gamma \;:\; \text{for } \gamma \in \Gamma,\ 0 < \ell \in \mathbb{Z}\}$$

Let

$$N \;=\; \{\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \in G\} \qquad\qquad N_{\mathbb{Z}} \;=\; N \cap \Gamma$$

The stabilizer of $(0,1)$ in Γ is $N_{\mathbb{Z}}$, and there is a bijection

$$\mathbb{Z}^2 - \{0\} \longleftrightarrow \{\ell > 0\} \times N_{\mathbb{Z}}\backslash\Gamma \qquad \text{by} \qquad \ell(0,1)\gamma \;\leftarrow\; \ell \times N_{\mathbb{Z}}\gamma$$

Then

$$\int_{\Gamma\backslash G} F(g)\,dg \;=\; \int_{\Gamma\backslash G} f(0)\,dg + \int_{\Gamma\backslash G} \sum_{x\neq 0} f(xg)\,dg \;=\; \int_{\Gamma\backslash G} f(0)\,dg + \sum_{\ell>0} \int_{N_{\mathbb{Z}}\backslash G} f(\ell\cdot(0,1)g)\,dg$$

Writing the integral on G as an iterated integral on P^+ and K, $\int_{\Gamma\backslash G} F$ is

$$\int_{\Gamma\backslash G} f(0)\,dg + \sum_{\ell>0} \int_{N_{\mathbb{Z}}\backslash P} \int_K f(\ell\cdot(0,1)pk)\,dg$$

With f *rotation invariant*, so $f(\ell(0,1)pk) = f(\ell(0,1)p)$, the integral is

$$\int_{\Gamma\backslash G} f(0)\,dg + 2\pi\cdot \sum_{\ell>0} \int_{N_{\mathbb{Z}}\backslash P} f(\ell(0,1)p)\,dp$$

since the total measure of K is 2π. Expressing the Haar measure on P^+ in coordinates as above, the integral is

$$\int_{\Gamma\backslash G} f(0)\,dg + 2\pi \sum_{\ell} \int_0^\infty \int_{\mathbb{Z}\backslash\mathbb{R}} f(\ell(0,1)\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix})\,dx\,\frac{dt}{t^2}$$

Note that N fixes $(0,1)$, so the integral over $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ is $\int_{\mathbb{Z}\backslash\mathbb{R}} 1\,dx = 1$, and the whole integral is

$$\int_{\Gamma\backslash G} F(g)\,dg = \int_{\Gamma\backslash G} f(0)\,dg + 2\pi \sum_{\ell} \int_M f(\ell(0,1)\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix})\,\frac{1}{t^2}\,\frac{dt}{t}$$

$$= \int_{\Gamma\backslash G} f(0)\,dg + 2\pi \sum_{\ell} \int_0^\infty f(\ell(0,t^{-1}))\,\frac{1}{t^2}\,\frac{dt}{t} \;=\; f(0)\cdot \mathrm{vol}\,(\Gamma\backslash G) + 2\pi \sum_{\ell} \int_0^\infty f(0,\ell t)\,t^2\,\frac{dt}{t}$$

replacing t by t^{-1}. Replacing t by t/ℓ gives

$$\int_{\Gamma\backslash G} F(g)\,dg \;=\; f(0)\cdot \mathrm{vol}\,(\Gamma\backslash G) + 2\pi\cdot \sum_{\ell} \ell^{-2} \int_0^\infty f(0,t)\,t^2\,\frac{dt}{t} \;=\; f(0)\cdot \mathrm{vol}\,(\Gamma\backslash G) + 2\pi\,\zeta(2)\cdot \int_0^\infty f(0,t)\,t^2\,\frac{dt}{t}$$

Using the rotation invariance of f,

$$\int_0^\infty f(0,t)\,t^2\,\frac{dt}{t} \;=\; \int_0^\infty f(0,t)\,t\,dt \;=\; \frac{1}{2\pi} \int_{\mathbb{R}^2} f(x)\,dx = \frac{1}{2\pi}\,\hat{f}(0)$$

The 2π's cancel, and

$$\int_{\Gamma\backslash G} F(g)\,dg \;=\; \int_{\Gamma\backslash G} \sum_{x\in\mathbb{Z}^2} f(xg)\,dg \;=\; f(0)\cdot \mathrm{vol}\,(\Gamma\backslash G) + \zeta(2)\,\hat{f}(0)$$

On the other hand, by Poisson summation,

$$\sum_{x \in \mathbb{Z}^2} f(xg) = \frac{1}{|\det g|} \sum_{x \in \mathbb{Z}^2} \hat{f}(x\,{}^\top g^{-1}) = \sum_{x \in \mathbb{Z}^2} \hat{f}(x\,{}^\top g^{-1})$$

(since $\det g = 1$). Γ is stable under transpose-inverse, allowing an analogous computation with the roles of f and $\hat{f}$ reversed, obtaining

$$f(0) \cdot \mathrm{vol}\,(\Gamma\backslash G) + \zeta(2)\,\hat{f}(0) \;=\; \int_{\Gamma\backslash G} F(g)\,dg \;=\; \hat{f}(0) \cdot \mathrm{vol}\,(\Gamma\backslash G) + \zeta(2)\,f(0)$$

from which

$$(f(0) - \hat{f}(0)) \cdot \mathrm{vol}\,(\Gamma\backslash G) \;=\; (f(0) - \hat{f}(0)) \cdot \zeta(2)$$

With $f(0) \neq \hat{f}(0)$, $\mathrm{vol}\,(\Gamma\backslash G) = \zeta(2)$. ///

[22.6] **Remark:** The proof does *not* use a fundamental domain for the quotient $SL_n(\mathbb{Z})\backslash SL_n(\mathbb{A})$, but *does* use Poisson summation, the *unwinding* of integration on quotients, and the *Iwasawa decomposition*

$$SL_n(\mathbb{R}) \;=\; P^+ \cdot K \;=\; \big(\text{upper-triang, diagonal} > 0\big) \cdot \big(\text{rotations}\big)$$

We can replace $\mathbb{Z}$ by the ring of integers $\mathfrak{o}$ of a number field k, $\mathbb{R}$ by the product $\prod_{v|\infty} k_v = k \otimes_{\mathbb{Q}} \mathbb{R}$ of archimedean completions of k, and by the same argument prove (up to reasonable normalization)

$$\mathrm{vol}\; SL_n(\mathfrak{o})\backslash SL_n(k \otimes_{\mathbb{Q}} \mathbb{R}) \;=\; \zeta_k(2)\,\zeta_k(3)\,\zeta_k(4)\,\zeta_k(5)\ldots\zeta_k(n)$$

Over number fields, the best proof is in modern (adelic) terms:

$$\mathrm{vol}\; SL_n(k)\backslash SL_n(\mathbb{A}_k) \;=\; \zeta_k(2)\,\zeta_k(3)\,\zeta_k(4)\,\zeta_k(5)\ldots\zeta_k(n)$$

Modern (adelic) Poisson summation and presentation of $\zeta_k(s)$ also appear in the Iwasawa-Tate modernization of Hecke's continuation and functional equation of Dedekind zeta functions, and of grossencharacter L-functions of number fields.

23. *Knowability of $\zeta_k(n)$ and other special values*

Some known results are summarized:

Over $k = \mathbb{Q}$, at even integers $\pi^{-2n}\zeta(2n) \in \mathbb{Q}$, with an explicit formula in terms of Bernouilli numbers.

$\zeta(3)$ was proven *irrational* by Apery [1978], which is not the same as asserting that $\pi^{-3}\zeta(3)$ is irrational. Rivoal [2000] gave a similar result, expanded to address $\zeta(3), \zeta(5), \zeta(7), \ldots$.

The volume computation shows the values $\zeta(\text{odd})$ are not mere sums-of-series, being volumes of natural, canonical objects.

Physical occurrence of zeta values was taken up by A. Borel in his study of *regulators*, and also by Bloch, Kato, and Beilinson.

Knowability of $\zeta(\text{even})$ fits into a conjecture of Deligne (1978) on *motivic* L-functions. All known special-value results fit Deligne's conjecture, although verification of compatibility is often difficult.

The larger conjectures *may* subsume Deligne's, ...

Half the values of Dirichlet L-functions over $\mathbb{Q}$ are knowable:

$$\pi^{-n}\,L(n,\chi) \;=\; \text{algebraic} \qquad\qquad (\text{for } n,\, \chi \text{ of equal parity})$$

with explicit Galois behavior. Recall: χ is *odd* when $\chi(-1) = -1$. There are explicit formulas in terms of generalized Bernoulli numbers, from Fourier series expansions of polynomials. (See notes from 2005-6.)

Values for *mismatched* parity are presumed of the same nature as $\zeta(3)$, though this seems not known.

With $k = \mathbb{Q}(\sqrt{D})$, quadratic reciprocity for $\chi(p) = (D/p)_2$ gives

$$\zeta_k(s) \;=\; \zeta(s)\cdot L(s,\chi) \;=\; \begin{cases} \zeta(s)\cdot L(s,\text{even}) & \text{for } D > 0 \\ \\ \zeta(s)\cdot L(s,\text{odd}) & \text{for } D < 0 \end{cases}$$

The trivial character in $\zeta(s)$ is *even.* Thus, the results for Dirichlet L-functions give

$$(\pi^{-n})^2\,\zeta_k(n) \;=\; \begin{cases} \text{algebraic} & (\text{for } n \text{ even, } D > 0) \\ \\ \text{unknown} & (\text{otherwise}) \end{cases}$$

Similarly, using reciprocity laws, zetas of *totally real* (archimedean completions are *real*, not *complex*) subfields of cyclotomic fields $\mathbb{Q}(\zeta_n)$ are products of Dirichlet L-functions with *even* χ, so are knowable at positive even integer arguments.

No analogous special values over not-totally-real number fields.

Beyond reciprocity: by the 1960s, Siegel and Klingen had gotten around the condition of abelian-ness over $\mathbb{Q}$, proving

$$\pi^{-2n[k:\mathbb{Q}]}\,\zeta_k(2n) \;=\; \text{algebraic} \qquad\qquad (2n \text{ even, } k \text{ totally real})$$

In fact, Klingen showed that, for *totally even* or *totally odd* finite-order Hecke-character χ on totally real k, values at integers n of matching parity were knowable:

$$\pi^{-n[k:\mathbb{Q}]}\,L(n,\chi) \;=\; \text{algebraic} \qquad\qquad (\text{parities of } n, \chi \text{ match})$$

In modern (adelic) terms, a grossencharacter χ is *totally even* when $\chi(k_v^\times) = 1$ for all archimedean v. It is *totally odd* when it takes both ±1 values on $k_v^\times$ for all archimedean v.

Proofs use Eisenstein series on *Hilbert modular groups* $SL_2(\mathfrak{o}_k)$.

[23.1] Example: Siegel also computed the volume of another family of *arithmetic quotients* $\Gamma\backslash G$. Apart from interest in the *possibility* of the computation, it is noteworthy that only *known* (knowable?) values of $\zeta(s)$ appear.

Let $J = \begin{pmatrix} 0_n & -1_n \\ 1_n & 0_n \end{pmatrix}$, and define the *symplectic group*

$$Sp_n \;=\; \{g \in GL_{2n} \;:\; g^\top J g \;=\; J\}$$

Then (Siegel)

$$\text{vol } Sp_n(\mathbb{Z})\backslash Sp_n(\mathbb{R}) \;=\; \zeta(2)\zeta(4)\zeta(6)\ldots\zeta(2n-2)\zeta(2n)$$

Just as with SL_n, the analogous result holds over number fields.

24. *Change-of-measure and Haar measure on $\mathbb{A}$ and k_v*

Another ingredient in Fujisaki's lemma was that, for *idele* α, the change-of-measure on $\mathbb{A}$ is

$$\frac{\mathrm{meas}\,(\alpha E)}{\mathrm{meas}\,(E)} = |\alpha| \qquad\qquad \text{(for measurable } E \subset \mathbb{A})$$

This is the full, modern version of the familiar fact for Lebesgue measure on the real line: for $\alpha \in \mathbb{R}^\times$ and measurable $E \subset \mathbb{R}$, written exactly the same way

$$\frac{\mathrm{meas}\,(\alpha E)}{\mathrm{meas}\,(E)} = |\alpha| \qquad\qquad \text{(for measurable } E \subset \mathbb{R})$$

[24.1] Local version for p-adic completions

What is the measure on $\mathbb{Q}_p$? We could tell how to integrate functions in $C_c^o(\mathbb{Q}_p)$, and invoke the Riesz-Markov-Kakutani theorem.

In any case, of course we want the *regularity* on locally compact, Hausdorff, countably-based topological spaces: the measure of a set is the *inf* of measure of opens containing it, and *sup* of measure of compacts contained in it.

For (locally compact...) *totally disconnected abelian groups* such as $\mathbb{Q}_p$, there is a local basis $U_n = p^n\mathbb{Z}_p$ at 0 consisting of open *subgroups*. Since Z_p is also *compact* (and closed), so is each U_n. Since Z_p is the disjoint union of p^n of these cosets,

$$\mathrm{meas}\,(p^n\mathbb{Z}_p) \;=\; p^{-n}\cdot\mathrm{meas}\,(\mathbb{Z}_p)$$

Probably normalize $\mathrm{meas}\,(\mathbb{Z}_p) = 1$. Even without *uniqueness* of Haar measure, this specifies a regular measure on $\mathbb{Q}_p$.

For (locally compact, ...) *totally disconnected abelian groups* such as $\mathbb{Q}_p$, there is a local basis $U_n = p^n\mathbb{Z}_p$ at 0 consisting of open *subgroups*. Since $\mathbb{Z}_p$ is also *compact* (and closed), so is each U_n. Since $\mathbb{Z}_p$ is the disjoint union

$$\mathbb{Z}_p \;=\; p^n\mathbb{Z}_p \sqcup (1+p^n\mathbb{Z}_p) \sqcup (2+p^n\mathbb{Z}_p) \sqcup \ldots \sqcup ((p^n-1)+p^n\mathbb{Z}_p)$$

of p^n of these cosets, by additivity

$$\mathrm{meas}\,(p^n\mathbb{Z}_p) \;=\; p^{-n}\cdot\mathrm{meas}\,(\mathbb{Z}_p)$$

Normalizing $\mathrm{meas}\,(\mathbb{Z}_p) = 1$ specifies a regular measure on $\mathbb{Q}_p$. Totally disconnected spaces have the advantage that many *simple functions* (meaning assuming only finitely-many values) are *continuous*, because many nice open sets are also closed:

$$p^n\mathbb{Z}_p \;=\; \{x \in \mathbb{Q}_p : |x|_p < \frac{1}{p^{n+1}}\} \;=\; \{x \in \mathbb{Q}_p : |x|_p \le \frac{1}{p^n}\}$$

Since addition is continuous, $x \to x+y$ is a homeomorphism of $\mathbb{Q}_p$ to itself, so $p^n\mathbb{Z}_p + y$ is both open and closed.

[24.2] Claim: every $f \in C_c^o(\mathbb{Q}_p)$ can be *approximated* by finite linear combinations of characteristic functions of sets $p^n\mathbb{Z}_p + y$.

[24.3] Remark: The appropriate topology on $C_c^o(\mathbb{Q}_p)$, or on $C_c^o(\mathbb{R})$, is *not* sup-norm. But each subspace $C_c^o(p^{-k}\mathbb{Z}_p)$ *is* topologized by sup-norm, and is *complete metric*. The topology on the whole space $C_c^o(\mathbb{Q}_p)$ is the *colimit* of the spaces $C_c^o(p^{-k}\mathbb{Z}_p)$. It is (quasi-) complete, but is not complete metric, since it violates the conclusion of Baire category, namely, it is a countable union of nowhere-dense subsets.

Proof: Since all the sets $p^{-k}\mathbb{Z}_p$ are homeomorphic, without loss of generality take $k = 0$. Let $f \in C_c^o(\mathbb{Z}_p)$. Fix $\varepsilon > 0$. For each $x \in \mathbb{Z}_p$, let $U_{n_x} = p^{n_x}\mathbb{Z}_p$ be a small-enough neighborhood of 0 so that $|f(x) - f(x')| < \varepsilon$ for $x' \in x + U_{n_x}$.

By compactness of $\mathbb{Z}_p$, there is a finite subcover $x_i + U_i$ of $\mathbb{Z}_p$. Let $U = \bigcap_i U_i$. The intersection is finite, so is open. We *claim* that for $x, x' \in \mathbb{Z}_p$ with $x - x' \in U$, necessarily $|f(x) - f(x')| < 2\varepsilon$. To see this, let $x \in x_i + U_i$. Then

$$x' \;\in\; x + U \;\subset\; (x_i + U_i) + U \;=\; x_i + (U_i + U) \;=\; x_i + U_i$$

As U is a sub*group*, $\mathbb{Z}_p$ is a finite *disjoint* union of cosets $U + y$. Define a simple function

$$\varphi(x) \;=\; f(y) \text{ for } x \in U + y$$

This differs from f by at most 2ε. ///

The continuity of these simple functions allows definition of integrals of $C_c^o(\mathbb{Q}_p)$ functions without going outside $C_c^o(\mathbb{Q}_p)$, by taking continuous simple function φ approximating f within ε, and

$$\int_{\mathbb{Q}_p} f \;=\; \lim_{\varepsilon\to 0} \sum_y \varphi(y) \cdot \text{meas}\,(U + y) \;=\; \lim_{\varepsilon\to 0} \text{meas}\,(U) \cdot \sum_y \varphi(y)$$

Let $S(\varphi) = \sum_y \varphi(y) \cdot \text{meas}\,(U)$, noting that this does depend on the finite cover by U-cosets.

It is not surprising that the limit is *well-defined*, much as Riemann sums approximating integrals of continuous functions on $\mathbb{R}$ give a well-defined limit: given simple φ, ψ approximating f within ε,

$$|S(\varphi) - S(\psi)| \;<\; 2 \cdot \varepsilon \cdot \text{meas}\,(\text{spt} f)$$

Thus, the sums $S(\varphi)$ are a *Cauchy net* of complex numbers, proving the well-definedness.

Translation-invariance: Again, take advantage of the total-disconnectedness. Given $f \in C_c^o(\mathbb{Q}_p)$ and $g \in \mathbb{Q}_p$, let $k \in \mathbb{Z}$ be large enough so that $p^{-k}\mathbb{Z}_p$ contains both spt$f$ and g. Then $x \to f(x + g)$ also has support inside $p^{-k}\mathbb{Z}_p$.

For a simple function φ approximating f, with φ a linear combination of characteristic functions of cosets $U + y$, $x \to x + g$ simply permutes these cosets. Thus,

$$\sum_y \varphi(y) \cdot \text{meas}\,(U) \;=\; \sum_y \varphi(y + g) \cdot \text{meas}\,(U + g)$$

Thus, $\int_{\mathbb{Q}_p} f(x + g)\, dx \;=\; \int_{\mathbb{Q}_p} f(x)\, dx$. ///

Uniqueness!?! Does taking meas $(\mathbb{Z}_p) = 1$ and the above construction of an integral give the only possible invariant integral/measure on $\mathbb{Q}_p$?

Temporarily ignoring any *general* assertion of uniqueness of Haar measure, let's take advantage of the special features here: $\mathbb{Z}_p$ is *open*, so is measurable. It is compact, so its measure is *finite*. Thus, we can renormalize a given Haar measure μ so that $\mu(\mathbb{Z}_p) = 1$.

Since $\mathbb{Z}_p$ is a disjoint union of p^n *translates* of $p^n\mathbb{Z}_p$, all with the same measure, by translation-invariance. Thus, $\mu(p^n\mathbb{Z}_p) = p^{-n}$. Thus, integrals of simple functions are completely determined.

We saw that each $C_c^o(p^{-k}\mathbb{Z}_p)$ can be approximated by simple functions. By the required positivity/continuity of the invariant integral, this determines integrals of $C_c^o(\mathbb{Q}_p)$ completely. ///

[24.4] Change-of-measure

We probably believe the assertion for $\mathbb{R}$:

$$\frac{\text{meas}\,(\alpha E)}{\text{meas}\,(E)} = |\alpha| \qquad\qquad (\alpha \in \mathbb{R}^\times, \text{ measurable } E \subset \mathbb{R})$$

Before considering the p-adic case, the *complex* claim is

$$\frac{\text{meas}\,(\alpha E)}{\text{meas}\,(E)} = |\alpha|_{\mathbb{C}} = |\alpha|^2 \qquad (\alpha \in \mathbb{C}^\times, \text{ measurable } E \subset \mathbb{C})$$

Recall that the product-formula normalization of the norm on $\mathbb{C}$ is $|\alpha|_{\mathbb{C}} = |N_{\mathbb{R}}^{\mathbb{C}}\alpha|_{\mathbb{R}}$, giving the square of the *extension* normalization. To prove this, use the usual parallelogram argument: take $\mathbb{R}$ basis $1, i$ of $\mathbb{C}$, and $\alpha = a + bi$. Then $\alpha \cdot 1 = a + bi$ and $\alpha \cdot i = -b + a$, and

$$\Big|\det\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\Big| = a^2 + b^2 = |\alpha|^2 = |\alpha|_{\mathbb{C}}$$

For the p-adic case, take advantage of the special nature of things here: for $\alpha \in \mathbb{Q}^p$ with $\alpha = p^{-k} \cdot \eta$ with $\eta \in \mathbb{Z}_p$ and $k \geq 0$, the set $\alpha \cdot \mathbb{Z}_p = p^{-k}\mathbb{Z}_p$ is a disjoint union of p^k copies of $\mathbb{Z}_p$, so has measure p^k. Oppositely, for $\alpha = p^k \cdot \eta$ with $k \geq 0$, $\mathbb{Z}_p$ is a disjoint union of p^k copies of $\alpha \cdot \mathbb{Z}_p$, so the measure of $\alpha \cdot \mathbb{Z}_p$ is p^{-k}. In both cases,

$$\frac{\text{meas}\,(\alpha \cdot \mathbb{Z}_p)}{\text{meas}\,(\mathbb{Z}_p)} = |\alpha|_p$$

Since $\nu(E) = \text{meas}\,(\alpha \cdot E)$ is another translation-invariant measure, by uniqueness it is a constant multiple of our constructed measure. We need only determine the constant, and computing the measure of $\alpha \cdot \mathbb{Z}_p$ does this. ///

Change-of-measure: adeles The rational adele group is not a product, but it is an ascending union (colimit) of products

$$\mathbb{A}_S = \mathbb{R} \times \prod_{v \in S} \mathbb{Q}_v \times \prod_{v \notin S} \mathbb{Z}_v$$

over finite sets S of places outside of which elements are locally integral. Countable products $\mathbb{A}_S$ of *countably-based* locally-compact spaces with regular Borel measures have well-behaved product measures specified (up to completion, irrelevant for us) by the measures on the factors: the product topology has a countable basis, and any open is a countable union of basis opens, so measures of opens are completely determined.

Uniqueness by re-usable methods: a topological group G with *at least* one invariant measure has *at most* one, up to scalar multiples. The argument is *re-usable*. For simplicity, suppose G is *unimodular*, that is, that a left-invariant measure is right-invariant.

Recall that an *approximate identity* is a sequence $\{\psi_i\}$ of non-negative $\psi_i \in C_c^o(G)$ such that $\int_G \psi_i = 1$ for all i, and such that, given a neighborhood U of 1, there is i_o such that for $i \geq i_o$ the support of ψ_i is inside U.

[24.5] Remark: This is strictly stronger than requiring that these functions approach the Dirac delta measure in a weak topology.

R, L are the usual right and left translation actions of G on functions f on G:

$$R_g f(h) = f(hg) \qquad L_g f(h) = f(g^{-1}h)$$

It is a two-epsilon argument, using the *uniform* continuity of continuous functions on compacts, to see that

$$g \times f \to R_g f \qquad g \times f \to L_g f$$

are *continuous* maps $G \times C_c^o(G) \to C_c^o(G)$.

Proof: *(for right translation)* A two-epsilon argument. The claim is that, given $\varepsilon > 0$, there is a neighborhood N of $1 \in G$ and $\delta > 0$ such that, for $g, g' \in G$ with $g' \in gN$, and $\sup_x |f(x) - f'(x)| < \delta$, we have $\sup_x |f(xg) - f'(xg')| < \varepsilon$.

$f \in C_c^o(K)$ is *uniformly* continuous, by the same proof as on $\mathbb{R}$, by the local compactness of G. That is, given $\varepsilon > 0$, there is a neighborhood U of $1 \in G$ such that $|f(x) - f(x')| < \varepsilon$ for all $x, x' \in G$ with $x' \in xU$. Let U be small-enough so that this holds for two $f, f' \in C_c^o(K)$.

Given x in compact K, let $g' \in gU$. Then

$$|f(xg) - f'(xg')| \;=\; |f(xg) - f(xg')| + |f(xg') - f'(xg')| \;<\; \varepsilon + \varepsilon$$

since $xg' \in x(gN) = (xg)N$ and $\sup_x |f(x) - f'(x)| < \varepsilon$. This proves the continuity.

[24.6] Remark: This continuity is exactly what is required for the action of G on $C_c^o(G)$ to be a *representation* of G.

For F a continuous $C_c^o(G)$-valued function on G, such as $F(g) = R_g f$, and for $\psi \in C_c^o(G)$, the function-valued integral

$$F \;\longrightarrow\; \int_G \psi(g)\, F(g)\, dg$$

is characterized by

$$\lambda\Big(\int_G \psi(g)\, F(g)\, dg\Big) = \int_G \psi(g)\, \lambda\big(F(g)\big)\, dg \qquad \text{(for all } \lambda \in C_c^o(G)^*\text{)}$$

By Hahn-Banach, there is *at most one* such integral: the continuous linear functionals separate points.

Further, granting *existence* of the integral, Hahn-Banach in fact shows that

$$\int_G \psi(g)\, F(g)\, dg \;\in\; \text{closure of convex hull of } \{F(g) : g \in \text{spt}\psi\}$$

Proposition:

$$\int_G \psi_i(g)\, F(g)\, dg \longrightarrow F(1) \qquad \text{(in the } C_c^o(G) \text{ topology)}$$

Proof: given $\varepsilon > 0$ and F, let $U \ni 1$ be small-enough so that $|F(x) - F(1)| < \varepsilon$, where $|*|$ is sup-norm on a particular $C_c^o(K)$. Let i be large enough so that the support of ψ_i is inside U. Then

$$F(1) - \int_G \psi_i(g)\, F(g)\, dg \;=\; F(1)\int_G \psi_i(g)\, dg - \int_G \psi_i(g)\, F(g)\, dg \;=\; \int_G \psi_i(g)\, \big(F(1) - F(g)\big)\, dg$$

The absolute value estimate, with $|*|$ sup-norm on K, gives

$$\Big|F(1) - \int_G \psi_i(g)\, F(g)\, dg\Big| \;\le\; \int_G \psi_i(g)\, \Big|F(1) - F(g)\Big|\, dg \;<\; \int_G \psi_i(g) \cdot \varepsilon\, dg \;=\; \varepsilon$$

This is the proposition. ///

Returning to the main thread of the proof, with $F(h) = f(gh)$, for invariant u in $C_c^o(G)^*$, by *continuity* of u,

$$u(f) \;=\; \lim_i u\left(g \to \int_G \psi_i(h)\, f(gh)\, dh\right)$$

which is

$$\lim_i u\left(g \to \int_G f(h)\,\psi_i(g^{-1}h)\,dh\right)$$

replacing h by $g^{-1}h$. Moving the functional u inside the integral the above becomes

$$u(f) \;=\; \lim_i \int_G f(h)\,u\left(g \to \psi_i(g^{-1}h)\right)\,dh$$

By *left* invariance of u,

$$u(f) \;=\; \lim_i \int_G f(h)\,u(g \to \psi_i(g))\,dh \;=\; \lim_i u(\psi_i)\cdot \int_G f(h)\,dh$$

Thus, for f with $\int_G f \neq 0$, $\lim_i u(\psi_i)$ *exists*. We conclude that $u(f)$ is a constant multiple of the indicated integral with *given* invariant measure. ///

[24.7] Remark: A nearly identical argument proves that G-invariant *distributions* on Lie groups G are unique up to constants, assuming existence.

25. *Toward Iwasawa-Tate: Fourier series on* $\mathbb{A}/k$

Elements of *harmonic analysis* on $\mathbb{R}$, $\mathbb{R}/\mathbb{Z}$, $\mathbb{Q}_p$, $\mathbb{A}$, and $\mathbb{A}_k/k$, are the key ingredients in Iwasawa-Tate's 1950 modernization of Hecke's 1918-20 proof of continuation and functional equation of zeta functions of all number fields, and *all* L-functions for $GL(1)$.

Ideas from Riemann's treatment of $\zeta_{\mathbb{Q}}(s)$ suffice for Dirichlet L-functions over $\mathbb{Q}$, and complex quadratic extensions of $\mathbb{Q}$. Reciprocity laws reduce factor zetas of abelian extensions of $\mathbb{Q}$ into Dirichlet L-functions over $\mathbb{Q}$.

Dedekind (∼1870) meromorphically continued zetas of number fields to small neighborhoods of $s = 1$, but this is insufficient for serious applications.

Hecke's 1918-20 proofs used Poisson summation for $\mathfrak{o} \subset k \otimes_{\mathbb{Q}} \mathbb{R}$. Iwasawa and Tate (1950) used the Weil-Pontryagin-Godement harmonic analysis on abelian topological groups, and everything became simpler.

We need the abelian topological group analogue of *characters* $x \to e^{2\pi i x\xi}$ for $\xi \in \mathbb{R}$, on $\mathbb{R}$, and *Fourier transforms*

$$\widehat{f}(\xi) \;=\; \mathscr{F}f(\xi) \;=\; \int_{\mathbb{R}} e^{-2\pi i x\xi}\, f(x)\,dx$$

and *inversion*

$$f(x) \;=\; \mathscr{F}^{-1}\widehat{f}(x) \;=\; \int_{\mathbb{R}} e^{2\pi i \xi x}\,\widehat{f}(\xi)\,d\xi$$

for nice functions f on $\mathbb{Q}_p$ and $\mathbb{A}$. Similarly for all completions k_v and adeles $\mathbb{A}_k$ of number fields. And *adelic Poisson summation*

$$\sum_{x\in k} f(x) \;=\; \sum_{x\in k} \mathscr{F}f(x) \qquad\qquad \text{(for suitable } f \text{ on } \mathbb{A}_k)$$

Fujisaki's lemma packs up the Units Theorem and finiteness of class groups exactly as needed by Iwasawa-Tate.

After these preparations, the argument will be identical to Riemann's.

[25.1] Fourier transforms, Fourier inversion, Schwartz spaces of functions, adelic Poisson summation The *ad hoc* classsical manipulations of *congruence conditions* (strangely, continuing to this day) are transparent when re-packaged as p-adic and adelic Fourier transforms.

This organizational principle applies not only to zeta functions and $GL(1)$ L-functions, but also to automorphic forms for $GL(2)$ and $GL(n)$ and other groups.

Unsurprisingly, the Fourier transform on k_v is

$$\mathscr{F} f(\xi) \;=\; \widehat{f}(\xi) \;=\; \int_{k_v} \overline{\psi}_\xi(x)\, f(x)\, dx$$

where, given the characters ψ_ξ (for example, the standard ones), the Haar measures are normalized so that *Fourier inversion* holds exactly:

$$f(x) \;=\; \int_{k_v} \psi_\xi(x)\, \widehat{f}(\xi)\, d\xi \qquad\qquad \text{(for nice functions } f\text{)}$$

It is not obvious that Fourier inversion could hold at all... Recall how/why Fourier inversion works on $\mathbb{R}$. First, a natural approach fails, but suggestively:

$$\int_{\mathbb{R}} \psi_\xi(x)\, \widehat{f}(\xi)\, d\xi \;=\; \int_{\mathbb{R}} \psi_\xi(x) \Big(\int_{\mathbb{R}} \overline{\psi}_\xi(t)\, f(t)\, dt \Big)\, d\xi \;=\; \int_{\mathbb{R}} f(t) \Big(\int_{\mathbb{R}} \psi_\xi(x-t)\, dt \Big)\, dt$$

If we could *justify* asserting that the inner integral is $\delta_x(t)$, which it *is*, then Fourier inversion follows:

$$\int_{\mathbb{R}} \psi_\xi(x)\, \widehat{f}(\xi)\, d\xi \;=\; \int_{\mathbb{R}} f(t)\, \delta_x(t)\, dt \;=\; f(x)$$

However, this is circular: Fourier inversion, and more, is used to make sense of that inner integral in the first place.

The usual space $\mathscr{S}(\mathbb{R})$ of *Schwartz functions* on $\mathbb{R}$ consists of infinitely-differentiable functions all of whose derivatives are of *rapid decay*, decaying more rapidly at $\pm\infty$ than every $1/|x|^N$. Its topology is given by semi-norms

$$\nu_{k,N}(f) \;=\; \sup_{0\le i\le k} \sup_{x\in\mathbb{R}} \Big((1+|x|)^N \cdot \big| f^{(i)}(x) \big| \Big)$$

for $0 \le k \in \mathbb{Z}$ and $0 \le N \in \mathbb{Z}$. There are countably-many associated (pseudo-) metrics $d_{k,N}(f,g) = \nu_{k,N}(f-g)$, so $\mathscr{S}(\mathbb{R})$ is naturally *metrizable*. The usual two-or-three-epsilon arguments show that $\mathscr{S}(\mathbb{R})$ is *complete* metrizable. [7]

When we know how to justify moving the differentiation under the integral,

$$\frac{d}{d\xi} \widehat{f}(\xi) \;=\; \frac{d}{d\xi} \int_{\mathbb{R}} \overline{\psi}_\xi(x)\, f(x)\, dx \;=\; \int_{\mathbb{R}} \frac{\partial}{\partial x} \overline{\psi}_\xi(x)\, f(x)\, dx$$

$$=\; \int_{\mathbb{R}} (-2\pi i x)\, \overline{\psi}_\xi(x)\, f(x)\, dx \;=\; (-2\pi i x) \widehat{f}(\xi)$$

Similarly, with an integration by parts,

$$-2\pi i \xi \cdot \widehat{f}(\xi) \;=\; \int_{\mathbb{R}} \frac{\partial}{\partial x} \overline{\psi}_\xi(x) \cdot f(x)\, dx \;=\; -\mathscr{F} \frac{df}{dx}(\xi)$$

[7] There is *no* canonical metric on $\mathscr{S}(\mathbb{R})$, despite the space being unambiguously *metrizable*.

It follows that $\mathscr{F}$ maps $\mathscr{S}(\mathbb{R})$ to itself, and, further, is an isomorphism of topological vector spaces.

Despite the impasse in the natural argument for Fourier inversion, the situation is encouraging. A dummy *convergence factor* will legitimize the idea.

For example, let $g(x) = e^{-\pi x^2}$ be the Gaussian. It is its own Fourier transform: moving the contour of integration after a change of variables,

$$\int_{\mathbb{R}} e^{-2\pi i\xi x}\, e^{-\pi x^2}\, dx \;=\; \int_{\mathbb{R}} e^{-\pi(x+i\xi)^2}\, e^{-\pi\xi^2}\, dx \;=\; e^{-\pi\xi^2}\int_{i\xi+\mathbb{R}} e^{-\pi x^2}\, dx \;=\; e^{-\pi\xi^2}\int_{\mathbb{R}} e^{-\pi x^2}\, dx \;=\; e^{-\pi\xi^2}$$

For $f \in \mathscr{S}(\mathbb{R})$, with $f_\varepsilon(x) = f(\varepsilon\cdot x)$, as $\varepsilon \to 0^+$ the dilated f_ε approaches $f(0)$ uniformly on compacts. Thus, as $\varepsilon \to 0^+$, the dilated Gaussian $g_\varepsilon(x) = g(\varepsilon\cdot x)$ approaches 1 uniformly on compacts, and

$$\int_{\mathbb{R}} \psi_\xi(x)\, \widehat{f}(\xi)\, d\xi \;=\; \int_{\mathbb{R}} \lim_{\varepsilon\to 0^+} g(\varepsilon\xi)\, \psi_\xi(x)\, \widehat{f}(\xi)\, d\xi \;=\; \lim_{\varepsilon\to 0^+}\int_{\mathbb{R}} g(\varepsilon\xi)\, \psi_\xi(x)\, \widehat{f}(\xi)\, d\xi$$

by *monotone convergence* or more elementary reasons.

The iterated integral can be legitimately rearranged:

$$\int_{\mathbb{R}} g(\varepsilon\xi)\, \psi_\xi(x)\, \widehat{f}(\xi)\, d\xi \;=\; \int_{\mathbb{R}}\int_{\mathbb{R}} g(\varepsilon\xi)\, \psi_\xi(x)\, \overline{\psi}_\xi(t)\, f(t)\, dt\, d\xi \;=\; \int_{\mathbb{R}}\int_{\mathbb{R}} g(\varepsilon\xi)\, \psi_\xi(x-t)\, f(t)\, d\xi\, dt$$

Changing variables in the definition of Fourier transform shows $\widehat{g_\varepsilon} = \frac{1}{\varepsilon} g_{1/\varepsilon}$. Thus,

$$\int_{\mathbb{R}} \psi_\xi(x)\, \widehat{f}(\xi)\, d\xi \;=\; \int_{\mathbb{R}} \frac{1}{\varepsilon}\, g\big(\frac{x-t}{\varepsilon}\big)\, f(t)\, dt \;=\; \int_{\mathbb{R}} \frac{1}{\varepsilon}\, g\big(\frac{t}{\varepsilon}\big)\cdot f(x+t)\, dt$$

The functions $g_{1/\varepsilon}/\varepsilon$ are not an *approximate identity* in the strictest sense, since the supports do not shrink to $\{0\}$. Nevertheless, the integral of each is 1, and as $\varepsilon \to 0^+$, the mass is concentrates on smaller and smaller neighborhoods of $0 \in \mathbb{R}$.

Thus, for $f \in \mathscr{S}(\mathbb{R})$, we have *Fourier inversion*

$$\int_{\mathbb{R}} \psi_\xi(x)\, \widehat{f}(\xi)\, d\xi \;=\; \ldots \;=\; \lim_{\varepsilon\to 0^+}\int_{\mathbb{R}} \frac{1}{\varepsilon}\, g\big(\frac{t}{\varepsilon}\big)\cdot f(x+t)\, dt \;=\; f(x)$$

An analogous argument succeeds for $\mathbb{Q}_p$, but is actually much simpler... (!)

Before describing the Schwartz space $\mathscr{S}(\mathbb{Q}_p)$ and proving Fourier inversion, sample computations of Fourier transforms are useful.

In particular, we need a simply-described function on $\mathbb{Q}_p$ which is its own Fourier transform, to play a role analogous to that of the Gaussian in the archimedean case.

[25.2] Claim: With Fourier transform on $\mathbb{Q}_p$ defined via the standard character $\psi_1(x) = e^{-2\pi i x'}$ (where $x' \in p^{-\infty}\mathbb{Z}_p$ and $x - x' \in \mathbb{Z}_p$), the characteristic function of $\mathbb{Z}_p$ is its own Fourier transform.

Proof: Let f be the characteristic function of $\mathbb{Z}_p$. Then

$$\widehat{f}(\xi) \;=\; \int_{\mathbb{Q}_p} \overline{\psi}_\xi(x)\, f(x)\, dx \;=\; \int_{\mathbb{Z}_p} \overline{\psi}_1(\xi\cdot x)\, dx \;=\; \int_{\mathbb{Z}_p} \psi_1(-\xi\cdot x)\, dx$$

Recall a form of the *cancellation lemma:* (a tiny case of *Schur orthogonality...*)

[25.3] Lemma: Let $\psi : K \to \mathbb{C}^\times$ be a continuous group homomorphism on a compact group K. Then

$$\int_K \psi(x)\,dx \;=\; \begin{cases} \text{meas}\,(K) & (\text{for } \psi = 1) \\ \\ 0 & (\text{for } \psi \neq 1) \end{cases}$$

Proof: *(of Lemma)* Yes, of course, the measure is a Haar measure on K. Since K is *compact*, it is *unimodular*. For ψ trivial, of course the integral is the total measure of K. For ψ non-trivial, there is $y \in K$ such that $\psi(y) \neq 1$. Using the invariance of the measure, change variables by replacing x by xy:

$$\int_K \psi(x)\,dx = \int_K \psi(xy)\,d(xy) = \int_K \psi(x)\,\psi(y)\,dx = \psi(y)\int_K \psi(x)\,dx$$

Since $\psi(y) \neq 1$, the integral is 0. ///

Apply the lemma to the integrals computing the Fourier transform of the characteristic function f of $\mathbb{Z}_p$. Giving the compact group $\mathbb{Z}_p$ measure 1,

$$\widehat{f}(\xi) \;=\; \int_{\mathbb{Z}_p} \psi_1(-\xi\cdot x)\,dx \;=\; \begin{cases} 1 & (\psi_1(-\xi x) = 1 \text{ for } x \in \mathbb{Z}_p) \\ \\ 0 & (\text{otherwise}) \end{cases}$$

On one hand, for $\xi \in \mathbb{Z}_p$, certainly $\psi_1(\xi x) = 1$ for $x \in \mathbb{Z}_p$. On the other hand, for $\xi \notin \mathbb{Z}_p$, there is $x \in \mathbb{Z}_p$ such that, for example, $\xi \cdot x = 1/p$. Then

$$\psi_1(-\xi\cdot x) \;=\; \psi_1(\tfrac{-1}{p}) \;=\; e^{+2\pi i\cdot\frac{1}{p}} \;\neq\; 1$$

Thus, ψ_ξ is not trivial on $\mathbb{Z}_p$, so the integral is 0. Thus, the characteristic function of $\mathbb{Z}_p$ is its own Fourier transform. ///

[25.4] Claim: With standard Fourier transform on $\mathbb{Q}_p$, the Fourier transform of the characteristic function of $p^k\mathbb{Z}_p$ is p^{-k} times the characteristic function of $p^{-k}\mathbb{Z}_p$.

Proof: Let f be the characteristic function of $p^k\mathbb{Z}_p$, so

$$\widehat{f}(\xi) \;=\; \int_{\mathbb{Q}_p} \overline{\psi}_\xi(x)\,f(x)\,dx \;=\; \int_{p^k\mathbb{Z}_p} \overline{\psi}_1(\xi\cdot x)\,dx$$

$$=\; |p^k|_p \cdot \int_{\mathbb{Z}_p} \psi_1(-\xi\cdot x/p^k)\,dx \;=\; p^{-k}\cdot \int_{\mathbb{Z}_p} \psi_1(-\xi\cdot x/p^k)\,dx$$

This reduces to the previous computation: by *cancellation*, for $\xi/p^k \notin \mathbb{Z}_p$ the character $x \to \psi_1(-\xi x/p^k)$ is non-trivial, so the integral is 0. Otherwise, the integral is 1. ///

[25.5] Claim: With standard Fourier transform on $\mathbb{Q}_p$, the Fourier transform of the characteristic function of $\mathbb{Z}_p + y$ is ψ_y times the characteristic function of $\mathbb{Z}_p$.

Proof: Let f be the characteristic function of $\mathbb{Z}_p + y$, so

$$\widehat{f}(\xi) \;=\; \int_{\mathbb{Q}_p} \overline{\psi}_\xi(x)\,f(x)\,dx \;=\; \int_{\mathbb{Z}_p+y} \overline{\psi}_1(\xi\cdot x)\,dx \;=\; \int_{\mathbb{Z}_p} \psi_1(-\xi\cdot(x+y))\,dx$$

$$=\; \psi_1(-\xi\cdot y)\,dx \int_{\mathbb{Z}_p} \psi_1(-\xi\cdot x)\,dx \;=\; \psi_1(-\xi\cdot y)\cdot f(\xi)$$

by the previous computation. ///

Combining the two computations above,

$$\mathscr{F}\Big(\text{char fcn } p^k\mathbb{Z}_p + y\Big) \;=\; \psi_y \cdot p^{-k} \cdot (\text{char fcn } p^{-k}\mathbb{Z}_p)$$

Conveniently, products $\psi_y \cdot (\text{char fcn } p^{-k}\mathbb{Z}_p)$ are in the same class of functions, since ψ_y has a kernel which is an open (and compact) neighborhood of 0, so we *this class of functions is mapped to itself under Fourier transform.*

Recall the earlier lemma proving that these *special* simple functions consisting of finite linear combinations of characteristic functions of sets $p^k\mathbb{Z}_p + y$ are *dense* in $C_c^o(\mathbb{Q}_p)$.

The space of **Schwartz functions** $\mathscr{S}(\mathbb{Q}_p)$ on $\mathbb{Q}_p$ is the vector space of these special simple functions, that is, finite linear combinations of characteristic functions of sets $p^k\mathbb{Z}_p + y$. Unlike the archimedean case, p-adic Schwartz functions are *compactly supported.*

p-adic Fourier inversion is the assertion

$$f(x) \;=\; \int_{\mathbb{Q}_p} \psi_\xi(x)\; \widehat{f}(\xi)\; d\xi \qquad\qquad (\text{for } f \in \mathscr{S}(\mathbb{Q}_p))$$

Proof: We have essentially proven this in the computations above, if we keep track, as follows. Let f^o be the characteristic function of $\mathbb{Z}_p$. We computed $\widehat{f^o} = f$. Let δ_t be the dilation operator $\delta_t f(x) = f(t \cdot x)$ for $t \in \mathbb{Q}_p^\times$. We computed, by changing variables in the integral defining the Fourier transform, that

$$\mathscr{F}(\delta_t f) \;=\; \frac{1}{|t|_p} \cdot \delta_{1/t}(\mathscr{F} f)$$

Let τ_y be the translation operator $\tau_y f(x) = f(x+y)$. By changing variables,

$$\mathscr{F}(\tau_y f) \;=\; \psi_y \cdot (\mathscr{F} f)$$

It is convenient to also compute that

$$\mathscr{F}(\psi_y \cdot f)(\xi) \;=\; \int_{\mathbb{Q}_p} \overline{\psi}_\xi(x) \cdot \psi_y(x)\, f(x)\; dx \;=\; \int_{\mathbb{Q}_p} \overline{\psi}_{\xi - y}(x)\, f(x)\; dx \;=\; \widehat{f}(\xi - y) \;=\; \tau_{-y}(\mathscr{F} f)$$

Let $\mathscr{F}^*$ be the integral for Fourier inversion, namely,

$$\mathscr{F}^* f(x) \;=\; \int_{\mathbb{Q}_p} \psi_\xi(x)\; f(\xi)\; d\xi$$

Similar computations give

$$\mathscr{F}^*(\delta_t f) \;=\; \frac{1}{|t|_p} \delta_{1/t}(\mathscr{F}^* f) \qquad\qquad \mathscr{F}^*(\tau_y f) \;=\; \psi_{-y}(\mathscr{F}^* f)$$

and

$$\mathscr{F}^*(\psi_y f) \;=\; \tau_y(\mathscr{F}^* f)$$

Since every element of $\mathscr{S}(\mathbb{Q}_p)$ is a linear combination of images of f^o under dilation and translation, it suffices to give a sort of inductive proof of Fourier inversion:

$$\mathscr{F}^*\mathscr{F}(\tau_y\, f) \;=\; = \;\mathscr{F}^*\psi_y \mathscr{F} f \;=\; \tau_y \mathscr{F}^*\mathscr{F} f$$

$$\mathscr{F}^*\mathscr{F}(\delta_t\, f) \;=\; \mathscr{F}^*\frac{1}{|t|_p}\delta_{1/t}\mathscr{F}f \;=\; \frac{1}{|t|_p}\frac{1}{|1/t|_p}\delta_t\mathscr{F}^*\mathscr{F}f \;=\; \delta_t\mathscr{F}^*\mathscr{F}f$$

Similarly for multiplication by ψ_y. Since $\mathscr{F}^*\mathscr{F}f^o = \mathscr{F}^*f^o = f^o$, we have Fourier inversion on $\mathscr{S}(\mathbb{Q}_p)$. ///

[25.6] Remark: p-adic Fourier inversion is much easier than on $\mathbb{R}$.

The space $\mathscr{S}(\mathbb{A})$ of Schwartz functions on the adeles is finite linear combinations of *monomial* functions

$$\Big(\bigotimes_{v\le\infty} f_v\Big)(\{x_v\}) \;=\; \prod_v f_v(x_v)$$

with $f_v \in \mathscr{S}(\mathbb{Q}_v)$, and where *for all but finitely-many* v the local function f_v is the characteristic function of $\mathbb{Z}_v$.

Fourier transform on $\mathscr{S}(\mathbb{A})$ is the product of all the local Fourier transforms, and Fourier inversion follows for $\mathscr{S}(\mathbb{A})$ because it holds for each $\mathscr{S}(\mathbb{Q}_v)$.

[25.7] Remark: We do not directly need it, but one might reflect on what the natural topology is on $\mathscr{S}(\mathbb{Q}_p)$, especially to have it be *complete*.

The harmonic analysis on $\mathbb{R}$ really is parallel to that on $\mathbb{Q}_p$ and $\mathbb{A}$ in many regards. For example,

Plancherel theorem: As on $\mathbb{R}$, $\int_{\mathbb{Q}_p} \widehat{f}\cdot\overline{\widehat{g}} = \int_{\mathbb{Q}_p} f\cdot\overline{g}$ for $f, g \in \mathscr{S}(\mathbb{Q}_p)$.

Proof: The key point is the surjectivity of $\mathscr{F} : \mathscr{S}(\mathbb{Q}_p) \to \mathscr{S}(\mathbb{Q}_p)$:

$$\int_{\mathbb{Q}_p} f\cdot\overline{g} \;=\; \int_{\mathbb{Q}_p} f\cdot\overline{\mathscr{F}^{-1}\widehat{g}} \;=\; \int_{\mathbb{Q}_p}\int_{\mathbb{Q}_p} f(x)\cdot\psi_1(-\xi x)\cdot\overline{\widehat{g}}(\xi)\,d\xi\,dx$$

$$=\; \int_{\mathbb{Q}_p}\Big(\int_{\mathbb{Q}_p} f(x)\cdot\psi_1(-\xi x)\,dx\Big)\cdot\overline{\widehat{g}}(\xi)\,d\xi \;=\; \int_{\mathbb{Q}_p}\widehat{f}\cdot\overline{\widehat{g}}$$

This is the same proof as for $\mathbb{R}$, and also applies to $\mathbb{A}$. ///

Then $\mathscr{F}$ is extended to $L^2(\mathbb{Q}_p)$ *by continuity*, giving the *Fourier-Plancherel* transform, no longer defined literally by the integrals.

[25.8] Fourier series on $\mathbb{A}/k$: For a unimodular topological group G, let $L^2(G)$ be the *completion* of $C_c^o(G)$ with respect to the usual L^2-norm

$$|f|^2 \;=\; \int_G |f(g)|^2\,dg \qquad\qquad (\text{for } f\in C_c^o(G))$$

[25.9] Theorem: For a compact abelian group G, with total measure 1, the continuous group homomorphisms (*characters*) $\psi : G \to \mathbb{C}^\times$ form an orthonormal *Hilbert-space basis* for $L^2(G)$. That is,

$$L^2(G) \;=\; \text{completion of} \bigoplus_{\psi\in G^\vee} \mathbb{C}\cdot\psi$$

The usual *inner product* is

$$\langle f, F\rangle \;=\; \int_G f\cdot\overline{F}$$

As usual, the completeness makes $L^2(G)$ a *Hilbert space.*

[25.10] Remark: This applies to the circle $\mathbb{R}/\mathbb{Z}$!

[25.11] Remark: For *finite* abelian groups, this follows from the spectral theorem for commuting *unitary* operators on finite-dimensional $\mathbb{C}$-vectorspaces.

[25.12] Remark: As in the elementary example of the circle $\mathbb{R}/\mathbb{Z}$, convergence in L^2 says nothing directly about *pointwise* convergence, much less *uniform* pointwise convergence.

Proof: Orthonormality is easy: for $\psi \neq \varphi$ characters,

$$\langle \psi, \varphi \rangle \;=\; \int_G \psi(g) \cdot \overline{\varphi}(g)\; dg \;=\; \int_G \psi\varphi^{-1}(g)\; dg$$

By the *cancellation lemma*, this is 0 for $\psi \neq \varphi$.

Completeness is more serious. We must prove existence of sufficiently many continuous group homomorphisms $\chi : G \to \mathbb{C}^\times$ so that the closure of their algebraic span in $L^2(G)$ is the whole Hilbert space $L^2(G)$.

The translation action of G on complex-valued functions on G is

$$g \cdot f(x) \;=\; f(xg) \qquad\qquad (\text{for } f \in C_c^o(G) \text{ and } x, g \in G)$$

For f to be a simultaneous *eigenfunction* for this action of G means that

$$g \cdot f \;=\; \lambda_f(g) \cdot f \qquad\qquad (\text{for all } g \in G, \text{ with } \lambda_f(g) \in \mathbb{C})$$

The eigenvalues $\lambda_f(g)$ cannot be unrelated: for $g, h \in G$,

$$\lambda_f(gh) \cdot f \;=\; (gh) \cdot f \;=\; g \cdot (h \cdot f) \;=\; g \cdot (\lambda_f(h)\, f) \;=\; \lambda_f(h)\, g \cdot f \;=\; \lambda_f(h)\, \lambda_f(g)\, f$$

so the eigenvalue $\lambda_f : G \to \mathbb{C}^\times$ is a *group homomorphism.* The translation action $G \times L^2(G) \to L^2(G)$ is *continuous*, so $g \to \lambda_f(g)$ is continuous. [8] Conversely, for continuous group homomorphisms $\chi : G \to \mathbb{C}^\times$,

$$(g \cdot \chi)(h) \;=\; \chi(hg) \;=\; \chi(h)\, \chi(g)$$

so χ is a simultaneous eigenfunction for G.

The action of G on $L^2(G)$ is *unitary*:

$$\langle g \cdot f,\, g \cdot F \rangle \;=\; \int_G f(xg)\, \overline{\varphi}(xg)\, dx \;=\; \int_G f(x)\, \overline{\varphi}(x)\, dx \;=\; \langle f, F \rangle$$

so eigenvectors with distinct eigenvalues are *orthogonal.*

Given a continuous group homomorphism $\chi : G \to \mathbb{C}^\times$, the space V_χ of χ-eigenvectors in $V = L^2(G)$ is *one-dimensional*: χ itself is in V_χ, and, given $f \in V_\chi$,

$$f(g) \;=\; f(1 \cdot g) \;=\; f(1) \cdot \chi(g)$$

so f is a scalar multiple of χ.

It remains to prove that nothing non-zero is orthogonal to all characters χ.

[8] The continuity of the translation action of G on $L^2(G)$ is demonstrated by approximating functions in $L^2(G)$ by *continuous* functions, and using the *uniform* continuity of continuous functions on the compact space G.

Warm-up: finite G: For G *finite*, $L^2(G)$ is finite-dimensional. By finite-dimensional spectral theory for *unitary* operators, $L^2(G)$ is a direct sum of eigenspaces V_λ, for group homomorphism $\lambda : G \to \mathbb{C}^\times$. Each λ-eigenfunction f is itself a constant multiple of the group homomorphism $\lambda : G \to \mathbb{C}^\times$, by the above argument. Thus,

$$L^2(G) \;=\; \bigoplus_{\lambda \in G^\vee} \mathbb{C}\cdot\lambda \qquad\qquad (G \text{ finite abelian})$$

This proves the decomposition for finite abelian groups G *without* the structure theorem for finite abelian groups.

For non-finite compact abelian groups G, we need a spectral decomposition of $L^2(G)$ with respect to the translation action of G. On infinite-dimensional Hilbert spaces, even for *unitary* operators, general spectral theory does *not* guarantee *eigenvectors.*

From a spectral viewpoint, the best operators on infinite-dimensional Hilbert spaces are *self-adjoint compact* operators, since (as we will show) they have enough eigenvectors. The *self-adjointness* is the usual $\langle Tv, w\rangle = \langle v, Tw\rangle$. The *compactness* is that the image TB of the unit ball B has *compact closure.* Thus, the image $\{Tv_i\}$ of a *bounded* sequence $\{v_i\}$ has a *convergent subsequence* $\{T_{v_{i_k}}\}$. On finite-dimensional vector spaces, *every* linear operator is compact. The utility of compact self-adjoint operators resides in the fundamental result:

[25.13] Theorem: For a set F of compact, self-adjoint, mutually commuting operators on a Hilbert space, there is an orthonormal Hilbert-space basis of simultaneous eigenvectors. Except for the 0-eigenspace (for all the operators), all simultaneous eigenspaces are *finite-dimensional.* (Proof in the following section.)

Except for finite G, the translation action of G on $L^2(G)$ is *not* by compact operators. Fortunately, *averaging* the translation action *does* give compact operators, as follows.

Compact operators often arise as *integral operators*, sometimes misleadingly called *convolution operators*: $\eta \in C^o_c(G)$ acts on $L^2(G)$ by the integral operator

$$(\eta\cdot f)(x) \;=\; \int_G \eta(g)\, f(xg)\, dg$$

There is the compatibility

$$\alpha\cdot(\beta\cdot f)(x) \;=\; \int_G\int_G \alpha(h)\,\beta(g)\,f(xhg)\;dg\,dh \;=\; \int_G \Big(\int_G \alpha(hg^{-1})\,\beta(g)\;dg\Big) f(xh)\;dh$$

$$=\; \int_G (\alpha*\beta)(h)\; f(xh)\;dh \;=\; \big((\alpha*\beta)\cdot f\big)(x)$$

The function $\alpha*\beta$ *is* convolution, but the action on vector spaces on which G may act is much more general than convolution of functions.

For G *abelian*, the composition of these integral operators is *commutative*: using the *unimodularity* of an abelian topological group, changing variables,

$$(\alpha*\beta)(g) \;=\; \int_G \alpha(gh^{-1})\,\beta(h)\;dh \;=\; \int_G \alpha(h^{-1}g)\,\beta(h)\;dh \;=\; \int_G \alpha(hg)\,\beta(h^{-1})\;dh$$

$$=\; \int_G \alpha(h)\,\beta(gh^{-1})\;dh \;=\; (\beta*\alpha)(g)$$

An innocent change of variables gives

$$(\alpha\cdot f)(x) \;=\; \int_G \alpha(y)\,f(xy)\;dy \;=\; \int_G \alpha(x^{-1}y)\;f(y)\;dy$$

Write $K(x,y) = \alpha(x^{-1}y)$ to suggest viewing $\alpha(x^{-1}y)$ as a *kernel* for an *integral operator*, analogous to a *matrix*, but indexed by $x, y \in G$. The connection to compact operators is:

[25.14] Claim: For compact topological spaces X, Y with finite total measure, for $K(x,y) \in C_c^o(X \times Y)$, the linear operator $T : L^2(Y) \to L^2(X)$ by

$$Tf(x) \;=\; \int_Y K(x,y)\, f(y)\, dy$$

is *compact*. For $X = Y$ and $K(y,x) = \overline{K(x,y)}$, the operator T is *self-adjoint*. (Proof in the following section.)

The spectral theorem for compact self-adjoint operators, and the previous claim, together immediately yield existence of sufficiently-many continuous group homomorphisms $G \to \mathbb{C}^\times$ for G compact abelian, as follows. Invoking the spectral theorem for the collection of self-adjoint compact operators $f \to \alpha \cdot f$ given by real-valued $\alpha \in C^o(G)$, let $V = L^2(G)$ decompose into simultaneous eigenspaces by

$$V \;=\; (\text{completion of})\; \oplus_{\lambda : G \to \mathbb{C}^\times} V_\lambda$$

where λ ranges over continuous group homomorphisms and $V_\lambda \neq \{0\}$. Above, we showed that $V_\lambda = \mathbb{C} \cdot \lambda$ for $V_\lambda \neq \{0\}$. Thus, finite linear combinations of continuous group homomorphisms $\lambda : G \to C^\times$ are dense in $L^2(G)$. ///

[25.15] Remark: Fredholm, Volterra, Hilbert, Riesz, and others inverted certain ordinary *differential* operators *(Sturm-Liouville problems)* to *integral* operators, which happened to be *compact*, thus giving a basis of eigenfunctions, enabling solution of such problems.

[25.16] Remark: This same strategy applies to compact G that are not necessarily *abelian*, to decompose $L^2(G)$ into *irreducible representations*, although most of the irreducibles are not one-dimensional, *not* spanned by group homomorphisms $G \to \mathbb{C}^\times$. Even for G *non-compact, non-abelian*, for discrete subgroups Γ with $\Gamma\backslash G$ *compact*, the same mechanism decomposes $L^2(\Gamma\backslash G)$.

---

26. *Spectral theorem for compact self-adjoint operators*

The key point of the decomposition of $L^2(G)$ for compact abelian groups G is the spectral theorem for self-adjoint compact operators $T : V \to V$ on Hilbert spaces, and for *mutually commuting* families of self-adjoint compact operators. We prove this spectral theorem.

[26.1] Theorem: *(Spectral theorem)* The non-zero eigenvalues of a self-adjoint compact operator T on a Hilbert space are *real*, have finite multiplicities, and have no accumulation point but $\{0\}$. For $0 \neq \lambda \in \mathbb{C}$ not among the eigenvalues, $T - \lambda$ is *invertible* (as continuous linear operator). Finite linear combinations of eigenvectors are *dense* in the Hilbert space. (Proof just below.)

An *eigenvalue* λ and corresponding *(simultaneous) eigenspace* V_λ for a ring R of mutually commuting operators on a Hilbert space V is a *ring homomorphism* $\lambda : R \to \mathbb{C}$, such that

$$Tv \;=\; \lambda(T) \cdot v \qquad\qquad (\text{for all } v \in V_\lambda \text{ and } T \in R)$$

[26.2] Corollary: A ring of *mutually commuting*, self-adjoint, compact operators on a Hilbert space has eigenspaces whose algebraic direct sum is dense in the whole Hilbert space. For $\lambda \neq 0$, the λ^{th} simultaneous eigenspace is finite-dimensional.

[26.3] Lemma: A continuous *self-adjoint* operator T on a Hilbert space V has operator norm $|T| = \sup_{|v| \le 1} |Tv|$ expressible as

$$|T| \;=\; \sup_{|v| \le 1} |\langle Tv, v\rangle|$$

Proof: On one hand, certainly $|\langle Tv, v\rangle| \le |Tv| \cdot |v|$, giving the easy direction of inequality. On the other hand, let $\sigma = \sup_{|v|\le 1} |\langle Tv, v\rangle|$. A polarization identity gives

$$2\langle Tv, w\rangle + 2\langle Tw, v\rangle \;=\; \langle T(v+w), v+w\rangle - \langle T(v-w), v-w\rangle$$

With $w = t \cdot Tv$ with $t > 0$, since $T = T^*$, both $\langle Tv, w\rangle$ and $\langle Tw, v\rangle$ are non-negative real. Taking absolute values,

$$\begin{aligned} 4\langle Tv, t\cdot Tv\rangle \;&=\; \sigma \cdot |v + t\cdot Tv|^2 + \sigma \cdot |v - t \cdot Tv|^2 \\ &=\; \Big|\langle T(v+t\cdot Tv), v + t\cdot Tv\rangle - \langle T(v - t\cdot Tv), v - t\cdot Tv\rangle\Big| \\ &\le\; \sigma \cdot |v + t\cdot Tv|^2 + \sigma\cdot |v - t\cdot Tv|^2 \;=\; 4\sigma \cdot \big(|v|^2 + t^2 \cdot |Tv|^2\big) \end{aligned}$$

Divide through by $4t$ and set $t = |v|/|Tv|$ to minimize the right-hand side, obtaining

$$|Tv|^2 \;\le\; \sigma \cdot |v| \cdot |Tv|$$

giving the other inequality, proving the Lemma. ///

Key Lemma: A compact self-adjoint operator T has largest eigenvalue $\pm|T|$.

Proof: Take $|T| > 0$, or else $T = 0$. Using the characterization of operator norm, let v_i be a sequence of unit vectors such that $|\langle Tv_i, v_i\rangle| \to |T|$. On one hand, using $\langle Tv, v\rangle = \langle v, Tv\rangle = \overline{\langle Tv, v\rangle}$,

$$\begin{aligned} 0 \;\le\; |Tv_i - \lambda v_i|^2 \;&=\; |Tv_i|^2 - 2\lambda\langle Tv_i, v_i\rangle + \lambda^2 |v_i|^2 \\ &\le\; \lambda^2 - 2\lambda\langle Tv_i, v_i\rangle + \lambda^2 \end{aligned}$$

By assumption, the right-hand side goes to 0. Using compactness, replace v_i with a subsequence such that Tv_i has limit w. Then the inequality shows that $\lambda v_i \to w$, so $v_i \to \lambda^{-1} w$. Thus, by continuity of T, $Tw = \lambda w$. ///

Proof: (of spectral theorem for a single self-adjoint compact operator on a Hilbert space.) In part, this is similar to the proof for self-adjoint operators on *finite*-dimensional spaces.

If $|T| = 0$, then $T = 0$. Otherwise, the key lemma gives a non-zero eigenvalue. The orthogonal complement of the corresponding eigenvector v is T-stable: for $w \perp v$,

$$\langle v, Tw\rangle = \langle Tv, w\rangle = \lambda\langle v, w\rangle = 0 \qquad (\text{for } Tv = \lambda v \text{ and } \langle v, w\rangle = 0)$$

The restriction of T to that orthogonal complement is still compact (!), so unless that restriction is 0, T has a non-zero eigenvalue there, too. Continue...

For $\lambda \ne 0$, the λ-eigenspace being infinite-dimensional would contradict the compactness of T: the unit ball in an infinite-dimensional inner-product space is not compact, as any infinite orthonormal set is a sequence with no convergent subsequence.

Similarly, for $c > 0$, the set of eigenvalues (counting multiplicities) larger than c being infinite would contradict compactness. Thus, 0 is the only limit-point of eigenvalues.

Finally, the restriction of T to the orthogonal complement of the sum of all its non-zero eigenspaces is still compact. If its operator norm were positive, there would be a further non-zero eigenvalue, contradiction. Thus, that restriction has 0 norm, so is 0. This proves the spectral theorem for a single self-adjoint compact operator. ///

Proof: ... for a commuting family of operators: as usual, the commutativity ensures that the operators stabilize each others' eigenspaces: for v a λ-eigenvalue for T, for another operator S,

$$T(Sv) \;=\; (TS)v \;=\; (ST)v \;=\; S(Tv) \;=\; S(\lambda v) \;=\; \lambda \cdot Sv$$

Thus, the spectral theorem for single self-adjoint compact operators gives the result. ///

[26.4] Remark: For proving existence of eigenfunctions, there is no alternative to self-adjoint compact operators. Meanwhile, compact operators have been understood, in terms appropriate for the time, for at least 120 years.

[26.5] Claim: *Hilbert-Schmidt* operators given by kernel functions $K(x,y) \in C_c^o(X \times Y)$ give compact operators $T : L^2(Y) \to L^2(X)$ by

$$Tf(x) \;=\; \int_Y K(x,y)\, f(y)\; dy$$

[26.6] Remark: The class of *Hilbert-Schmidt* operators often is taken to include not only operators with kernels in $C^o(X \times Y)$, but also kernels in $L^2(X \times Y)$. In practice, usually kernels are in L^2 because they are in C_c^o.

Proof: We show that T is an operator-norm limit of *finite-rank* operators, that is, operators with finite-dimensional images. Fix $\varepsilon > 0$, find a *finite* collection of functions f_i, F_i such that

$$\sup_{x,y} \Big| K(x,y) - \sum_i f_i \otimes F_i \Big| \;<\; \varepsilon$$

For each (x,y) in the support of K, let $U_x \times V_y$ be a neighborhood of (x,y) such that $|K(x,y) - K(x',y')| < \varepsilon$ for $x' \in U_x$ and $y' \in V_y$, where U_x and V_y are neighborhoods of x, y.

By compactness of the support of $K(x,y)$, there are finitely-many x_j, y_j such that $U_j \times V_j$ (abbreviating $U_{x_j} \times V_{y_j}$) cover the support of $K(x,y)$. Let

$$\varphi_j \;=\; \text{char fcn } U_j \qquad \text{and} \qquad \Phi_j \;=\; K(x_j,y_j) \cdot (\text{char fcn } U_j)$$

The sets $U_j \times V_j$ *overlap*, so $K \neq \sum_j \varphi_j \otimes \Phi_j$, necessitating minor adjustments. One way to compensate for the overlaps is by subtracting two-fold overlaps, adding back three-fold overlaps, subtracting four-fold, and so on: let

$$Q \;=\; \sum_i \varphi_i \otimes \Phi_i - \sum_{i_1<i_2} \min(\varphi_{i_1}, \varphi_{i_2}) \otimes \min(\Phi_{i_1}, \Phi_{i_2}) + \sum_{i_1<i_2<i_3} \min(\varphi_{i_1}, \varphi_{i_2}, \varphi_{i_3}) \otimes \min(\Phi_{i_1}, \Phi_{i_2}, \Phi_{i_3}) - \ldots$$

Because the subcover is finite, Q is a finite linear combination $Q = \sum_j f_j \otimes F_j$. By construction, $\sup_{x,y} \big|K(x,y) - Q(x,y\big| < \varepsilon$. The operator

$$f \;\longrightarrow\; \int_G Q(x,y)\, f(y)\; dy$$

is finite-rank, because the image is in the span of the finitely-many f_i appearing in the definition of $Q(x,y)$.

Let χ be the characteristic function of the closure $\overline{U}$ of a compact-closure open U containing the support of K. For every $\varepsilon > 0$, the opens U_x and U_y can be chosen inside U. Then

$$\Big| \int_G Q(x,y)\, f(y)\; dy \;-\; \int_G K(x,y)\, f(y)\; dy \Big| \;\leq\; \int_G |Q(x,y) - K(x,y)| \cdot |f(y)|\; dy$$

$$<\; \varepsilon \int_G |\chi(x,y)| \cdot |f(y)|\; dy \;\leq\; \varepsilon \cdot |\chi|_{L^2} \cdot |f|_{L^2}$$

Thus, the operator norm of the difference can be made arbitrarily small, proving that the operator T given by $K(x,y) \in C_c^o(X \times Y)$ is an operator-norm limit of finite-rank operators. The following lemma will complete the proof of compactness. ///

[26.7] Lemma: Operator-norm limits of finite-rank operators are compact.

[26.8] Remark: for operators on Hilbert spaces, the converse is also true, namely, that *all* compact operators are operator-norm limits of finite-rank ones. On Banach spaces, the converse is false, with difficult counter-examples due to Per Enflo.

Proof: Let $T = \lim_i T_i$, where $T_i : X \to Y$ is finite-rank $X \to Y$. Let B be the unit ball in X. We show that TB has compact closure by showing that it is *totally bounded*, that is, for every $\varepsilon > 0$ it can be covered by finitely-many ε-balls.

Given $\varepsilon > 0$, let i be large-enough so that $|T - T_i| < \varepsilon$. Since T_i is finite-rank, T_iB is covered by finitely-many ε-balls $B_1, \ldots, B_n$ in Y with respective centers $y_1, \ldots, y_n$. For $x \in B$, with $T_ix \in B_j$,

$$|Tx - y_j| \;\le\; |Tx - T_ix| + |T_ix - y_j| \;<\; \varepsilon + \varepsilon$$

Thus, TB is covered by a finite number of 2ε-balls. This holds for every $\varepsilon > 0$, so TB is *totally bounded*. ///

Recall the proof that *total boundedness* of a set E in a complete metric space implies compact closure:

Since metric spaces have countable local bases, it suffices to show *sequential* compactness. That is, a sequence $\{v_i\}$ in E, exhibit a convergent subsequence.

Cover E by finitely-many 2^{-1}-balls, choose one, call it B_1, with infinitely-many v_i in $E \cap B_1$, and let w_1 be one of those infinitely-many v_i.

Next, cover E by finitely-many 2^{-2}-balls. Certainly $E \cap B_1$ is covered by these, and $E \cap B_1 \cap B_2$ contains infinitely-many v_i for at least one of these, call it B_2. Let $w_2 \in E \cap B_1 \cap B_2$ be one of these v_i, other than w_1.

Inductively, find an infinite subsequence w_n of distinct points, with $w_n \in E \cap B_1 \cap \ldots \cap B_n$, where B_n is of radius 2^{-n}. The sequence w_i is Cauchy. ///

---

27. *Iwasawa-Tate for Riemann's* $\zeta(s)$

We carry out the main part of the argument first for the simplest case, Riemann's zeta in this section, then for Dirichlet L-functions, Dedekind zeta functions of number fields, and the general case of Hecke L-functions with grossencharacters in following sections. At each stage, there are further complications.

Some issues are postponed: adelic Poisson summation, evaluation of local integrals, ...

A virtue of the modern (Tate-Iwasawa) viewpoint is that issues about *units* and *class numbers* evaporate completely.

The modern argument is completely parallel to Riemann's. Let $d^\times x$ be a Haar measure on $\mathbb{J}$. Define **global zeta integrals**

$$Z(s,f) \;=\; \int_{\mathbb{J}} |x|^s\, f(x)\, d^\times x \qquad\qquad (f \in \mathscr{S}(\mathbb{A}),\ s \in \mathbb{C},\ \mathrm{Re}\, s > 1)$$

We will see later that, for suitable choice of f, the zeta integral is the zeta function with its gamma factor. We prove that *every* such global zeta integral has a meromorphic continuation with poles at worst at $s = 1, 0$, with predictable residues, with functional equation

$$Z(s,f) \;=\; Z(1-s, \widehat{f}) \qquad\qquad (\text{for arbitrary } f \in \mathscr{S}(\mathbb{A}))$$

where $\widehat{f}$ is the adelic Fourier transform. Part of the point is that meromorphic continuation and functional equation of $Z(s,f)$ follow for *all* f, *without* worrying about best choice of Schwartz function f.

[27.1] Euler products and local zeta integrals Let $d_v^\times x$ be a Haar measure on $\mathbb{Q}_v^\times$ with $d^\times x = \prod_v d_v^\times x$. For *monomial* Schwartz functions $f = \bigotimes f_v$, for Re $s > 1$, the zeta integral factors over primes:

$$Z(s,f) \;=\; \int_{\mathbb{J}} |x|^s\, f(x)\, d^\times x \;=\; \prod_v \int_{\mathbb{Q}_v^\times} |x|_v^s\, f_v(x)\, d_v^\times x$$

as an infinite product of *local* integrals. That is, zeta integrals of *monomial* Schwartz functions have *Euler product* expansions in the region of convergence. This motivates defining *local zeta integrals* to be those local integrals

$$Z_v(s, f_v) \;=\; \int_{\mathbb{Q}_v^\times} |x|_v^s\, f_v(x)\, d_v^\times x$$

and

$$Z(s,f) \;=\; \prod_v Z_v(s,f_v) \qquad \text{(for Re } s > 1\text{, with } f = \textstyle\bigotimes_v f_v)$$

We see later that a reasonable choice for f, with $\widehat{f} = f$, produces the standard factors:

$$Z_v(s,f_v) \;=\; \begin{cases} \dfrac{1}{1 - \dfrac{1}{p^s}} & \text{(for finite } v \sim p) \\[2ex] \pi^{-\frac{s}{2}}\Gamma\left(\dfrac{s}{2}\right) & \text{(for } v = \infty) \end{cases}$$

That is, for reasonable choices, in this situation,

$$Z(s,f) \;=\; \xi(s) \;=\; \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\, \zeta(s)$$

[27.2] Functional equation of a theta function The analogue of the *theta function* appearing in Riemann's and Hecke's classical arguments is

$$\theta_f(x) \;=\; \sum_{\alpha \in \mathbb{Q}} f(\alpha x) \qquad \text{(for } x \in \mathbb{J},\ f \in \mathscr{S}(\mathbb{A}))$$

Adelic Poisson summation will give the functional equation of the theta function. From the obvious change of variables,

$$\int_{\mathbb{A}} \overline{\psi}(\xi\alpha)\; f(\alpha x)\; d\alpha \;=\; \int_{\mathbb{A}} \overline{\psi}(\xi\alpha/x)\; f(\alpha)\; d(\alpha/x)$$

The adelic change of measure is the idele norm, and

$$\int_{\mathbb{A}} \overline{\psi}(\xi\alpha/x)\; f(\alpha)\; d(\alpha/x) \;=\; \frac{1}{|x|}\int_{\mathbb{A}} \overline{\psi}(\xi\alpha/x)\; f(\alpha)\; d\alpha \;=\; \frac{1}{|x|}\widehat{f}\Big(\frac{\xi}{x}\Big)$$

Then Poisson summation gives the functional equation

$$\theta_f(x) \;=\; \sum_{\alpha\in\mathbb{Q}} f(\alpha x) \;=\; \frac{1}{|x|}\sum_{\alpha\in\mathbb{Q}} \widehat{f}\big(\frac{\alpha}{x}\big) \;=\; \frac{1}{|x|}\,\theta_{\widehat{f}}\big(\frac{1}{x}\big)$$

[27.3] Main argument: analytic continuation and functional equation of global zeta integrals The analytic continuation and functional equation arise from *winding up*, breaking the integral into two pieces, and applying the functional equation of θ's, as in the classical scenario. Let

$$\mathbb{J}^+ \;=\; \{x \in \mathbb{J} : |x| \ge 1\} \qquad \mathbb{J}^- \;=\; \{x \in \mathbb{J} : |x| \le 1\}$$

and $\mathbb{J}^1 \;=\; \{x \in \mathbb{J} : |x| = 1\}$. Let

$$\theta_f^*(x) \;=\; \theta_f(x) \;-\; f(0) \;=\; \sum_{\alpha \in \mathbb{Q}^\times} f(\alpha x) \qquad (x \in \mathbb{J} \text{ and } f \in \mathscr{S}(\mathbb{A}))$$

Wind up the zeta integral, use the product formula, and break the integral into two pieces:

$$Z(s,f) \;=\; \int_{\mathbb{J}} |x|^s\, f(x)\, d^\times x \;=\; \int_{\mathbb{J}/\mathbb{Q}^\times} \sum_{\alpha \in \mathbb{Q}^\times} |\alpha x|^s\, f(\alpha x)\, d^\times(\alpha x)$$

$$= \int_{\mathbb{J}/\mathbb{Q}^\times} |x|^s \sum_{\alpha \in \mathbb{Q}^\times} f(\alpha x)\, d^\times x \;=\; \int_{\mathbb{J}/\mathbb{Q}^\times} |x|^s\, \theta_f^*(x)\, d^\times x \;=\; \int_{\mathbb{J}^+/\mathbb{Q}^\times} |x|^s\, \theta_f^*(x)\, d^\times x \;+\; \int_{\mathbb{J}^-/\mathbb{Q}^\times} |x|^s\, \theta_f^*(x)\, d^\times x$$

just like classical

$$\xi(s) \;=\; \int_1^\infty y^{s/2}\, \frac{\theta(iy)-1}{2}\, \frac{dy}{y} \;+\; \int_0^1 y^{s/2}\, \frac{\theta(iy)-1}{2}\, \frac{dy}{y}$$

The integral over $\mathbb{J}^+/\mathbb{Q}^\times$ is *entire*. (Proof later.)

The functional equation of θ_f will transforms the integral over $\mathbb{J}^-/\mathbb{Q}^\times$ into an integral over $\mathbb{J}^+/\mathbb{Q}^\times$ plus two elementary terms describing the poles.

Replace x by $1/x$, and simplify:

$$\int_{\mathbb{J}^-/\mathbb{Q}^\times} |x|^s\, \theta_f^*(x)\, d^\times x \;=\; \int_{\mathbb{J}^+/\mathbb{Q}^\times} |1/x|^s\, \theta_f^*(1/x)\, d^\times(1/x) \;=\; \int_{\mathbb{J}^+/\mathbb{Q}^\times} |x|^{-s} \cdot \Big[|x|\theta_{\widehat{f}}(x) - f(0)\Big]\, d^\times x$$

$$= \int_{\mathbb{J}^+/\mathbb{Q}^\times} |x|^{1-s}\, \theta_{\widehat{f}}^*(x)\, d^\times x \;+\; \widehat{f}(0) \int_{\mathbb{J}^+/\mathbb{Q}^\times} |x|^{1-s}\, d^\times x \;-\; f(0) \int_{\mathbb{J}^+/\mathbb{Q}^\times} |x|^{-s}\, d^\times x$$

The integral of $\theta_{\widehat{f}}^*$ over $\mathbb{J}^+/\mathbb{Q}^\times$ is *entire*. The elementary integrals can be evaluated:

$$\int_{\mathbb{J}^+/\mathbb{Q}^\times} |x|^{1-s}\, d^\times x \;=\; \big|J^1/\mathbb{Q}^\times\big| \cdot \int_1^\infty x^{1-s}\, \frac{dx}{x} \;=\; \frac{\big|J^1/\mathbb{Q}^\times\big|}{s-1}$$

In this case, the natural measure of $\mathbb{J}^1/\mathbb{Q}^\times$ is 1, so

$$Z(s,f) \;=\; \int_{\mathbb{J}^+/\mathbb{Q}^\times} \Big(|x|^s \sum_{\alpha \in \mathbb{Q}^\times} f(\alpha x) + |x|^{1-s} \sum_{\alpha \in \mathbb{Q}^\times} \widehat{f}(\alpha x)\Big)\, d^\times x \;+\; \frac{\widehat{f}(0)}{s-1} \;-\; \frac{f(0)}{s}$$

The integral is entire, so the latter expression gives the *analytic continuation*. There is visible symmetry under $s \longleftrightarrow 1-s$ and $f \longleftrightarrow \widehat{f}$, so we have the *functional equation*

$$Z(s,f) \;=\; Z(1-s, \widehat{f})$$

28. *Iwasawa-Tate for Dirichlet L-functions*

We adapt the argument to prove *analytic continuation* and *functional equation* for Dirichlet L-functions. One should observe how *few* changes are needed from the argument for Riemann's $\zeta(s)$.

[28.1] Dirichlet characters as idele-class characters

For a Dirichlet character χ_d with conductor N. The main adaptation necessary is rewriting χ_d as a character χ on $\mathbb{J}/k^\times$.

Given idele α, by unique factorization in $\mathbb{Z}$, adjust α by $\mathbb{Q}^\times$ to put its local component inside $\mathbb{Z}_v^\times$ at all finite places. Adjust by ± 1 to make the archimedean component *positive.* Thus, an idele-class character is completely determined by its values on

$$U \;=\; \mathbb{R}^+ \cdot \prod_{v<\infty} \mathbb{Z}_v^\times$$

As the diagonal copy of $\mathbb{Q}^\times$ meets U just at $\{1\}$, there is no risk of ill-definedness. Continuity on U implies continuity on $\mathbb{J}$.

At finite places $v \sim p$ *not* dividing N, we declare χ to be trivial on the local units: $\chi(\mathbb{Z}_v^\times) = 1$ for $v \sim p$ not dividing N.

For $v \sim p$ with $N = p^e M$ and $p \not| M$, given $x \in \mathbb{Z}_v^\times$, let $n \in \mathbb{Z}$ such that $n = x \bmod p^e\mathbb{Z}_v$, and $n = 1 \bmod M$, and define $\chi(x) = \chi_d(n)$. Say χ is *unramified* at v when $\chi(\mathbb{Z}_v^\times) = 1$. At finite places v where χ is *non-trivial* on the local units, χ is *ramified.*

[28.2] Global zeta integrals

We consider only idele-class characters χ *trivial* on the copy $\{(t, 1, 1, \ldots, 1) : t > 0\}$ of positive reals inside $\mathbb{J}$. Define **global zeta integrals**

$$Z(s, \chi, f) \;=\; \int_{\mathbb{J}} |x|^s\, \chi(x)\, f(x)\, d^\times x \qquad (f \in \mathscr{S}(\mathbb{A}),\ s \in \mathbb{C},\ \mathrm{Re}\, s > 1)$$

For suitable f, $Z(s, \chi, f)$ is the Dedekind zeta function with its gamma factor, except for complications at ramified primes. *Every* zeta integral has a meromorphic continuation with poles at worst at $s = 1, 0$, with predictable residues, with functional equation

$$Z(s, \chi, f) \;=\; Z(1 - s, \chi^{-1}, \widehat{f}) \qquad\qquad (\text{for arbitrary } f \in \mathscr{S}(\mathbb{A}))$$

[28.3] Euler products and local zeta integrals

For *monomial* Schwartz functions $f = \bigotimes f_v$, for $\mathrm{Re}\, s > 1$,

$$Z(s, f) \;=\; \int_{\mathbb{J}} |x|^s\, \chi(x)\, f(x)\, d^\times x \;=\; \prod_v \int_{k_v^\times} |x|_v^s\, \chi_v(x)\, f_v(x)\, d_v^\times x$$

with χ_v the restriction of χ to $\mathbb{Q}_v^\times$. That is, $Z(s, f)$ is an infinite product of *local* integrals. That is, zeta integrals of *monomial* Schwartz functions have *Euler product* expansions, in the region of convergence. This motivates defining *local zeta integrals* to be those local integrals

$$Z_v(s, \chi_v, f_v) \;=\; \int_{k_v^\times} |x|_v^s\, \chi_v(x)\; f_v(x)\; d_v^\times x$$

Without clarifying the nature of the local integrals, the Euler product assertion is

$$Z(s, f) \;=\; \prod_v Z_v(s, \chi_v, f_v) \qquad\qquad (\mathrm{Re}\, s > 1, \text{ with } f = \textstyle\bigotimes_v f_v)$$

[28.4] Usual Euler factors, with a complication

We see later that a reasonable choice of f produces the standard factors:

$$Z_v(s,\chi_v,f_v) = \begin{cases} \dfrac{1}{1-\dfrac{\chi(p)}{p^s}} & (v \sim p,\, p \not| N) \\ \pi^{-\frac{s}{2}}\Gamma\left(\dfrac{s}{2}\right) & (\ v \approx \mathbb{R} \text{ and } \chi_d(-1)=1) \\ \pi^{-\frac{s+1}{2}}\Gamma\left(\dfrac{s+1}{2}\right) & (\ v \approx \mathbb{R} \text{ and } \chi_d(-1)=-1) \end{cases}$$

There is a complication at finite $v \sim$ with $p|N$: typically there is no Schwartz function f recovering the factor $N^{-s/2}$ in the known functional equations

$$N^{\frac{s}{2}}\,\pi^{-\frac{s}{2}}\,\Gamma(\tfrac{s}{2})\,L(s,\chi) = \varepsilon(\chi)\,N^{(1-s)/2}\,\pi^{-(1-s)/2}\,\Gamma(\tfrac{1-s}{2})\,L(1-s,\chi^{-1})$$

for χ even, and for χ odd

$$N^{\frac{s}{2}}\pi^{-\frac{(s+1)}{2}}\Gamma(\tfrac{s+1}{2})\,L(s,\chi) = \varepsilon(\chi)N^{\frac{(1-s)}{2}}\pi^{-\frac{(2-s)}{2}}\,\Gamma(\tfrac{2-s}{2})\,L(1-s,\chi^{-1})$$

Nevertheless, a reasonable choice will produce $Z(s,\chi,f)$ and $Z(s,\chi^{-1},\widehat{f})$ such that, letting $\Lambda(s,\chi)$ be the L-function with its gamma factor and *with* factor of $N^{s/2}$,

$$\begin{aligned} Z(s,\chi,f) &= N^{-s/2}\cdot\Lambda(s,\chi) \\ Z(1-s,\chi^{-1},\widehat{f}) &= \varepsilon\cdot N^{-s/2}\cdot\Lambda(1-s,\chi^{-1}) \end{aligned}$$

with $|\varepsilon|=1$. Thus, from $Z(s,\chi,f)=Z(1-s,\chi^{-1},f)$ the symmetrical functional equation can be obtained.

[28.5] Functional equation of a theta function

As before, the *theta function* attached to a Schwartz function f is

$$\theta_f(x) \;=\; \sum_{\alpha\in k} f(\alpha x) \qquad (\text{for } x\in\mathbb{J},\ f\in\mathscr{S}(\mathbb{A}))$$

and Poisson summation gives the functional equation

$$\theta_f(x) \;=\; \sum_{\alpha\in k} f(\alpha x) \;=\; \frac{1}{|x|}\sum_{\alpha\in k}\widehat{f}(\frac{\alpha}{x}) \;=\; \frac{1}{|x|}\,\theta_{\widehat{f}}(\frac{1}{x})$$

[28.6] Main argument: analytic continuation and functional equation of global zeta integrals

Again, analytic continuation and functional equation arise from *winding up*, breaking the integral into two pieces, and applying the functional equation of θ, as in the classical scenario.

For non-trivial χ, the Schwartz function f can be taken so that

$$f(0) \;=\; 0 \qquad \text{and} \qquad \widehat{f}(0) \;=\; 0$$

relieving us of tracking those values, and giving the simpler presentation

$$\theta_f(x) \;=\; \sum_{\alpha\in\mathbb{Q}^\times} f(\alpha x) \qquad (\text{for } x\in\mathbb{J} \text{ and } f\in\mathscr{S}(\mathbb{A}))$$

Wind up the zeta integral, use the product formula and $\mathbb{Q}^\times$-invariance of χ, and break the integral into two pieces:

$$Z(s,\chi,f) \;=\; \int_{\mathbb{J}} |x|^s\,\chi(x)\,f(x)\,d^\times x \;=\; \int_{\mathbb{J}/\mathbb{Q}^\times}\sum_{\alpha\in k^\times}|\alpha x|^s\,\chi(\alpha x)\,f(\alpha x)\,d^\times(\alpha x)$$

$$= \int_{\mathbb{J}/\mathbb{Q}^\times} |x|^s\,\chi(x) \sum_{\alpha\in k^\times} f(\alpha x)\,d^\times x \;=\; \int_{\mathbb{J}/\mathbb{Q}^\times} |x|^s\,\chi(x)\,\theta_f(x)\,d^\times x$$

$$= \int_{\mathbb{J}^+/\mathbb{Q}^\times} |x|^s\,\chi(x)\,\theta_f(x)\,d^\times x \;+\; \int_{\mathbb{J}^-/\mathbb{Q}^\times} |x|^s\,\chi(x)\,\theta_f(x)\,d^\times x$$

The integral over $\mathbb{J}^+/\mathbb{Q}^\times$ is *entire*. The functional equation of θ_f will give a transformation of the integral over $\mathbb{J}^-/\mathbb{Q}^\times$ into an integral over $\mathbb{J}^+/\mathbb{Q}^\times$. Replace x by $1/x$, and simplify:

$$\int_{\mathbb{J}^-/\mathbb{Q}^\times} |x|^s\,\chi(x)\,\theta_f(x)\,d^\times x \;=\; \int_{\mathbb{J}^+/\mathbb{Q}^\times} |1/x|^s\,\chi(1/x)\,\theta_f(1/x)\,d^\times(1/x)$$

$$= \int_{\mathbb{J}^+/\mathbb{Q}^\times} |x|^{-s}\,\chi^{-1}(x)|x|\theta_{\widehat{f}}(x)\,d^\times x = \int_{\mathbb{J}^+/\mathbb{Q}^\times} |x|^{1-s}\,\chi^{-1}(x)\,\theta_{\widehat{f}}(x)\,d^\times x$$

The integral of $\theta_{\widehat{f}}$ over $\mathbb{J}^+/\mathbb{Q}^\times$ is *entire*. Thus,

$$Z(s,\chi,f) \;=\; \int_{\mathbb{J}^+/\mathbb{Q}^\times} \Big(|x|^s\,\chi(x) \sum_{\alpha\in\mathbb{Q}^\times} f(\alpha x) + |x|^{1-s}\,\chi^{-1}(x) \sum_{\alpha\in\mathbb{Q}^\times} \widehat{f}(\alpha x)\Big)\,d^\times x$$

The integral is entire, and gives the *analytic continuation*. Further, there is visible symmetry $\chi \leftrightarrow \chi^{-1}$, $s \leftrightarrow 1-s$, $f \leftrightarrow \widehat{f}$, so we have the *functional equation*

$$Z(s,\chi,f) \;=\; Z(1-s,\chi^{-1},\widehat{f})$$

[28.7] **Remark:** There was no compulsion to track of $|x|^s$ and $\chi(x)$ separately in the above argument. We could rewrite the above to treat an *arbitrary* χ on $\mathbb{J}/\mathbb{Q}^\times$, define

$$Z(\chi,f) \;=\; \int_{\mathbb{J}} \chi(x)\,f(x)\,d^\times x$$

and obtain the slightly cleaner functional equation

$$Z(\chi,f) \;=\; Z(|.|\,\chi^{-1},\widehat{f})$$

That is, rather than $s \to 1-s$ and $\chi \to \chi^{-1}$, simply replace χ by $x \to |x| \cdot \chi^{-1}(x)$.

29. *Iwasawa-Tate for Dedekind zetas of number fields*

The argument is repeated, proving *analytic continuation* and *functional equation* for Dedekind zetas of number fields.

[29.1] Global zeta integrals

$$Z(s,f) \;=\; \int_{\mathbb{J}} |x|^s\,f(x)\,d^\times x \qquad (f \in \mathscr{S}(\mathbb{A}),\ s\in\mathbb{C},\ \mathrm{Re}\,s > 1)$$

We will see that, for suitable choice of f, the zeta integral is the Dedekind zeta function with its gamma factors. Just below, we prove that *every* such global zeta integral has a meromorphic continuation with poles at worst at $s = 1, 0$, with predictable residues, with functional equation

$$Z(s,f) \;=\; Z(1-s,\widehat{f}) \qquad (\text{for arbitrary } f \in \mathscr{S}(\mathbb{A}))$$

[29.2] Euler products and local zeta integrals

For *monomial* Schwartz functions $f = \bigotimes f_v$, for Re $s > 1$, the zeta integral factors over primes as a product of local integrals

$$Z(s,f) \;=\; \int_{\mathbb{J}} |x|^s\, f(x)\, d^\times x \;=\; \prod_v \int_{k_v^\times} |x|_v^s\; f_v(x)\; d_v^\times x$$

Letting

$$Z_v(s,f_v) \;=\; \int_{k_v^\times} |x|_v^s\; f_v(x)\; d_v^\times x$$

and without clarifying the nature of the local integrals, the Euler product assertion is

$$Z(s,f) \;=\; \prod_v Z_v(s,f_v) \qquad\qquad (\text{ Re } s > 1, \text{ monomial } f = \textstyle\bigotimes_v f_v)$$

[29.3] Usual Euler factors, with a complication

We see later that a reasonable choice of f (and measures $d_v^\times x$) produces the standard factors at *all but finitely-many primes*: with q_v the cardinality of the residue field for non-archimedean v,

$$Z_v(s,f_v) \;=\; \begin{cases} \dfrac{1}{1-\dfrac{1}{q_v^s}} & (\text{for } k_v \text{ unramified over } \mathbb{Q}_w) \\ \pi^{-\frac{s}{2}}\Gamma\left(\dfrac{s}{2}\right) & (\text{for } v \approx \mathbb{R}) \\ (2\pi)^{-s}\Gamma(s) & (\text{for } v \approx \mathbb{C}) \end{cases}$$

However, there is a complication due to finite v with $k_v/\mathbb{Q}_w$ *ramified.* The Dedekind zeta function of k is

$$\zeta_k(s) \;=\; \prod_{v<\infty} \frac{1}{1-\dfrac{1}{q_v^s}}$$

Let

$$\Gamma_{\mathbb{R}}(s) \;=\; \pi^{-\frac{s}{2}}\,\Gamma\big(\frac{s}{2}\big) \qquad\qquad \Gamma_{\mathbb{C}}(s) \;=\; (2\pi)^{-s}\,\Gamma(s)$$

and let r_1,r_2 be the number or real and complex places. Hecke found that the functional equation of the Dedekind zeta function $\zeta_k(s)$ involves the *discriminant* D_k of $\mathfrak{o}_k$ over $\mathbb{Z}$, with symmetrical form

$$\Gamma_{\mathbb{R}}(s)^{r_1}\Gamma_{\mathbb{C}}(s)^{r_2}\cdot|D_k|^{-\frac{s}{2}}\cdot\zeta_k(s)$$

$$=\; \Gamma_{\mathbb{R}}(1-s)^{r_1}\Gamma_{\mathbb{C}}(1-s)^{r_2}\cdot|D_k|^{-\frac{1-s}{2}}\cdot\zeta_k(1-s)$$

The discriminant is

$$D_k \;=\; \text{vol}\,(k\otimes_{\mathbb{Q}}\mathbb{R}/\mathfrak{o})^2 \;=\; |\det\begin{pmatrix} \sigma_1(\alpha_1) & \sigma_2(\alpha_1) & \ldots & \sigma_r(\alpha_1) \\ \vdots & & & \vdots \\ \sigma_1(\alpha_r) & \sigma_2(\alpha_r) & \ldots & \sigma_r(\alpha_r) \end{pmatrix}|^2$$

where σ_j are the topologically distinct imbeddings $k \to \mathbb{C}$.

The factor $|D_k|^{-\frac{s}{2}}$ *is* a product of local contributions, as follows. The absolute value of the discriminant is the ideal-norm of the *absolute different*

$$\mathfrak{d}_{\mathfrak{o}/\mathbb{Z}} \;=\; \{\alpha\in k \;:\; \text{tr}_{\mathbb{Q}}^k(\alpha\mathfrak{o})\subset\mathbb{Z}\}^{-1} \qquad (\text{fractional ideal inverse})$$

This is essentially the product of *local* differents

$$\mathfrak{d}_v \;=\; \mathfrak{d}_{\mathfrak{o}_v/\mathbb{Z}_w} \;=\; \{\alpha \in k_v \;:\; \mathrm{tr}^{k_v}_{\mathbb{Q}_w}(\alpha\mathfrak{o}_v) \subset \mathbb{Z}_v\}^{-1}$$

Thus, to have the functional equation, the local factor at ramified v should be

$$\frac{[\mathfrak{o}_v : \mathfrak{d}_{\mathfrak{o}_v/\mathbb{Z}-w}]^{-\frac{s}{2}}}{1-\dfrac{1}{q_v^s}}$$

However, typically, there is no choice of f or local component f_v to produce this Euler factor as a local zeta integral!

In fact, typically, there is no choice of f such that $\widehat{f} = f$, because, typically, at ramified v there is no $f_v \in \mathscr{S}(k_v)$ with $\widehat{f_v} = f_v$. That is, there is no choice of Schwartz function to make the local zeta functions $Z_v(s, f_v)$ and $Z_v(s, \widehat{f_v})$ the same.

That is, while the functional equation

$$Z(s,f) \;=\; Z(1-s,\widehat{f})$$

holds, there is simply no choice of f to make the functional equation obviously relate a zeta integral to itself.

However, there are other options. A reasonable choice of $f = \bigotimes_v f_v$ will produce the expected factors at archimedean and unramified finite places, and at ramified finite v will produce

$$Z_v(s,f_v) \;=\; \frac{[\mathfrak{o}_v^* : \mathfrak{o}_v]^{-\frac{1}{2}}}{1-\dfrac{1}{q^s}} \qquad\qquad Z_v(s,\widehat{f_v}) \;=\; \frac{[\mathfrak{o}_v^* : \mathfrak{o}_v]^{s-\frac{1}{2}}}{1-\dfrac{1}{q^s}}$$

Thus,

$$Z(s,f) \;=\; |D_k|^{\frac{1}{2}} \cdot \Gamma_{\mathbb{R}}(s)^{r_1}\Gamma_{\mathbb{R}}(s)^{r_2} \cdot \zeta_k(s)$$

$$Z(s,\widehat{f}) \;=\; |D_k|^{s-\frac{1}{2}} \cdot \Gamma_{\mathbb{R}}(s)^{r_1}\Gamma_{\mathbb{R}}(s)^{r_2} \cdot \zeta_k(s)$$

From $Z(s,f) = Z(1-s,\widehat{f})$,

$$|D_k|^{\frac{1}{2}} \cdot \Gamma_{\mathbb{R}}(s)^{r_1}\Gamma_{\mathbb{R}}(s)^{r_2}\,\zeta_k(s) \;=\; |D_k|^{(1-s)-\frac{1}{2}} \cdot \Gamma_{\mathbb{R}}(1-s)^{r_1}\Gamma_{\mathbb{R}}(1-s)^{r_2} \cdot \zeta_k(1-s)$$

Divide through by $|D_k|^{s/2}$ to obtain the symmetrical form of the functional equation for $\zeta_k(s)$.

[29.4] Remark: Asymmetry in zeta integrals cannot be avoided, in general. Thus, zeta *functions*, including optimized gamma factors and powers of discriminants, are *not exactly* given by zeta *integrals*. Nevertheless, the zeta integrals *are* inevitably correct at all but finitely-many places.

[29.5] Functional equation of a theta function

The analogue of the *theta function* appearing in Riemann's and Hecke's classical arguments is

$$\theta_f(x) \;=\; \sum_{\alpha\in k} f(\alpha x) \qquad\qquad (\text{for } x \in \mathbb{J},\ f \in \mathscr{S}(\mathbb{A}))$$

Poisson summation gives the functional equation

$$\theta_f(x) \;=\; \sum_{\alpha\in k} f(\alpha x) \;=\; \frac{1}{|x|}\sum_{\alpha\in k} \widehat{f}\big(\frac{\alpha}{x}\big) \;=\; \frac{1}{|x|}\,\theta_{\widehat{f}}\big(\frac{1}{x}\big)$$

Analytic continuation and functional equation arise from *winding up*, and breaking the integral into two pieces, and applying the functional equation of θ's.

Notation for θ_f with its constant removed:

$$\theta^*_f(x) \;=\; \theta_f(x) \;-\; f(0) \;=\; \sum_{\alpha\in k^\times} f(\alpha x) \qquad\qquad (x\in\mathbb{J},\; f\in\mathscr{S}(\mathbb{A}))$$

Wind up the zeta integral, use the product formula, and break the integral into two pieces:

$$Z(s,f) \;=\; \int_{\mathbb{J}} |x|^s\, f(x)\, d^\times x \;=\; \int_{\mathbb{J}/k^\times} \sum_{\alpha\in k^\times} |\alpha x|^s\, f(\alpha x)\, d^\times(\alpha x) \;=\; \int_{\mathbb{J}/k^\times} |x|^s \sum_{\alpha\in k^\times} f(\alpha x)\, d^\times x$$

$$= \int_{\mathbb{J}/k^\times} |x|^s\, \theta^*_f(x)\, d^\times x \;=\; \int_{\mathbb{J}^+/k^\times} |x|^s\, \theta^*_f(x)\, d^\times x \;+\; \int_{\mathbb{J}^-/k^\times} |x|^s\, \theta^*_f(x)\, d^\times x$$

The integral over $\mathbb{J}^+/k^\times$ is *entire*. The functional equation of θ_f will give a transformation of the integral over $\mathbb{J}^-/k^\times$ into an integral over $\mathbb{J}^+/k^\times$ plus two elementary terms describing the poles.

Replace x by $1/x$, and simplify:

$$\int_{\mathbb{J}^-/k^\times} |x|^s\; \theta^*_f(x)\, d^\times x \;=\; \int_{\mathbb{J}^+/k^\times} |1/x|^s\; \theta^*_f(1/x)\, d^\times(1/x) \;=\; \int_{\mathbb{J}^+/k^\times} |x|^{-s}\cdot \Big[|x|\theta_{\widehat{f}}(x) - f(0)\Big]\, d^\times x$$

$$= \int_{\mathbb{J}^+/k^\times} |x|^{1-s}\; \theta^*_{\widehat{f}}(x)\, d^\times x \;+\; \widehat{f}(0)\int_{\mathbb{J}^+/k^\times} |x|^{1-s}\, d^\times x \;-\; f(0)\int_{\mathbb{J}^+/k^\times} |x|^{-s}\, d^\times x$$

The integral of $\theta^*_{\widehat{f}}$ over $\mathbb{J}^+/k^\times$ is *entire*. The elementary integrals can be evaluated:

$$\int_{\mathbb{J}^+/k^\times} |x|^{1-s}\, d^\times x \;=\; \mathrm{meas}\,(\mathbb{J}^1/k^\times)\cdot \int_1^\infty x^{1-s}\,\frac{dx}{x} \;=\; \frac{|\mathbb{J}^1/k^\times|}{s-1}$$

We will see later that the natural measure of $\mathbb{J}^1/k^\times$ is

$$\mathrm{meas}\,(\mathbb{J}^1/k^\times) \;=\; \frac{2^{r_1}\,(2\pi)^{r_2}\,h\,R}{|D_k|^{\frac{1}{2}}\,w}$$

where r_1, r_2 are the numbers of real and complex places, respectively, h is the class number of $\mathfrak{o}$, R is the *regulator*

$$R \;=\; \mathrm{vol}\Big(\{\alpha\in k\otimes_{\mathbb{Q}}\mathbb{R} \;:\; \prod_{v|\infty}|\alpha|_v = 1\}\Big/\mathfrak{o}^\times\Big)$$

D_k is the *discriminant*, and w is the number of roots of unity in k. Thus,

$$Z(s,f) \;=\; \int_{\mathbb{J}^+/k^\times} \Big(|x|^s\sum_{\alpha\in k^\times} f(\alpha x) + |x|^{1-s}\sum_{\alpha\in k^\times}\widehat{f}(\alpha x)\Big)\, d^\times x \;+\; \frac{|J^1/k^\times|\cdot\widehat{f}(0)}{s-1} \;-\; \frac{|J^1/k^\times|\cdot f(0)}{s}$$

The integral is entire, so the latter expression gives the *analytic continuation*. Further, there is visible symmetry under $s \longleftrightarrow 1-s$ and $f\longleftrightarrow\widehat{f}$ and so we have the *functional equation*

$$Z(s,f) \;=\; Z(1-s,\widehat{f})$$

30. *Iwasawa-Tate general case: Hecke L-functions*

Let χ be a character on the idele class group $\mathbb{J}/k^\times$ of k, trivial on the diagonal copy of $\mathbb{R}^+ = (0, +\infty)$ in archimedean factors inside $\mathbb{J}$. In particular,

$$\mathbb{J}/k^\times \;\approx\; \mathbb{J}^1/k^\times \;\times\; \mathbb{R}^+$$

and $|x|^s$ is trivial on $\mathbb{J}^1/k^\times$. Let f be a Schwartz function on the adeles $\mathbb{A}$ of a number field k. The Iwasawa-Tate *global zeta integral* is

$$Z(s,\chi,f) \;=\; \int_{\mathbb{J}} |x|^s\,\chi(x)\,f(x)\,d^\times x$$

for Haar measure $d^\times x$ on $\mathbb{J}$. Let

$$\kappa \;=\; \text{meas}\,(\mathbb{J}^1/k^\times) \;=\; \frac{2^{r_1}\,(2\pi)^{r_2}\,h\,R}{|D_k|^{\frac{1}{2}}\,w}$$

[30.1] Theorem: The zeta integral has a *meromorphic continuation* in s to a meromorphic function on $\mathbb{C}$, with poles at most at $s=0$ and $s=1$, with respective residues

$$\text{Res}_{s=1} Z(s,\chi,f) \;=\; \begin{cases} \kappa\cdot\widehat{f}(0) & \text{(for } \chi \text{ trivial)} \\ 0 & \text{(for } \chi \text{ non-trivial)} \end{cases}$$

$$\text{Res}_{s=0} Z(s,\chi,f) \;=\; \begin{cases} \kappa\cdot f(0) & \text{(for } \chi \text{ trivial)} \\ 0 & \text{(for } \chi \text{ non-trivial)} \end{cases}$$

There is the *functional equation*

$$Z(s,\chi,f) \;=\; Z(1-s,\chi^{-1},\widehat{f})$$

For *monomial* Schwartz functions $f = \prod f_v$, for Re $s > 1$, the zeta integral has an Euler product

$$Z(s,\chi,f) \;=\; \int_{\mathbb{J}} |x|^s\,\chi(x)\,f(x)\,d^\times x \;=\; \prod_v \int_{k_v^\times} |x|_v^s\,\chi_v(x)\,f_v(x)\,d_v^\times x$$

where χ_v is the restriction of χ to $k_v^\times$.

Proof: The *theta function* attached to a Schwartz function is

$$\theta_f(x) \;=\; \sum_{\alpha\in k} f(\alpha x) \qquad\qquad \text{(for } x\in\mathbb{J},\ f\in\mathscr{S}(\mathbb{A})\text{)}$$

and Poisson summation gives the functional equation

$$\theta_f(x) \;=\; \sum_{\alpha\in k} f(\alpha x) \;=\; \frac{1}{|x|}\sum_{\alpha\in k}\widehat{f}(\frac{\alpha}{x}) \;=\; \frac{1}{|x|}\,\theta_{\widehat{f}}(\frac{1}{x})$$

The analytic continuation and functional equation arise from *winding up*, breaking the integral into two pieces, and applying the functional equation of θs. Let

$$\theta_f^*(x) \;=\; \sum_{\alpha\in\mathbb{Q}^\times} f(\alpha x) \;=\; \theta_f(x) - f(0) \qquad\qquad \text{(for } x\in\mathbb{J} \text{ and } f\in\mathscr{S}(\mathbb{A})\text{)}$$

Computing directly,

$$Z(s,\chi,f) \;=\; \int_{\mathbb{J}} |x|^s\,\chi(x)\,f(x)\,d^\times x \;=\; \int_{\mathbb{J}/k^\times} \sum_{\alpha\in k^\times} |\alpha x|^s\,\chi(\alpha x)\,f(\alpha x)\,d^\times(\alpha x)$$

$$=\; \int_{\mathbb{J}/k^\times} |x|^s\,\chi(x) \sum_{\alpha\in k^\times} f(\alpha x)\,d^\times x \;=\; \int_{\mathbb{J}/k^\times} |x|^s\,\chi(x)\,\theta^*_f(x)\,d^\times x$$

$$=\; \int_{\mathbb{J}^+/k^\times} |x|^s\,\chi(x)\,\theta^*_f(x)\,d^\times x \;+\; \int_{\mathbb{J}^-/k^\times} |x|^s\,\chi(x)\,\theta^*_f(x)\,d^\times x$$

The integral over $\mathbb{J}^+/k^\times$ is *entire*. The functional equation of θ_f will give a transformation of the integral over $\mathbb{J}^-/k^\times$ into an integral over $\mathbb{J}^+/k^\times$ plus two elementary terms describing the poles. Replace x by $1/x$, and simplify:

$$\int_{\mathbb{J}^-/k^\times} |x|^s\,\chi(x)\,\theta^*_f(x)\,d^\times x \;=\; \int_{\mathbb{J}^+/k^\times} |1/x|^s\,\chi(1/x)\,\theta^*_f(1/x)\,d^\times(1/x)$$

$$=\; \int_{\mathbb{J}^+/k^\times} |x|^{-s}\,\chi^{-1}(x)\cdot\Big[|x|\theta_{\widehat{f}}(x) - f(0)\Big]\,d^\times x$$

$$=\; \int_{\mathbb{J}^+/k^\times} |x|^{1-s}\,\chi^{-1}(x)\,\theta^*_{\widehat{f}}(x)\,d^\times x \;+\; \widehat{f}(0)\int_{\mathbb{J}^+/k^\times} |x|^s\,\chi(x)\,d^\times x \;-\; f(0)\int_{\mathbb{J}^+/k^\times} |x|^{1-s}\,\chi^{-1}(x)\,d^\times x$$

The last two integrals are elementary:

$$\widehat{f}(0)\int_{\mathbb{J}^+/k^\times} |x|^s\,\chi(x)\,d^\times x \;-\; f(0)\int_{\mathbb{J}^+/k^\times} |x|^{1-s}\,\chi^{-1}(x)\,d^\times x \;=\; \frac{\kappa\,\widehat{f}(0)}{s-1} \;-\; \frac{\kappa\,f(0)}{s}$$

The integral of $\theta_{\widehat{f}}$ over $\mathbb{J}^+/k^\times$ is *entire*. Thus,

$$Z(s,\chi,f) \;=\; \int_{\mathbb{J}^+/\mathbb{Q}^\times} \Big(|x|^s\,\chi(x)\,\theta^*_f(x) + |x|^{1-s}\,\chi^{-1}(x)\theta^*_{\widehat{f}}(x)\Big)\,d^\times x \;+\; \frac{\kappa\,\widehat{f}(0)}{s-1} \;-\; \frac{\kappa\,f(0)}{s}$$

The integral is entire, and gives the *analytic continuation*. Further, there is visible symmetry under

$$\chi \;\longleftrightarrow\; \chi^{-1} \qquad\qquad s \;\longleftrightarrow\; 1-s \qquad\qquad f \;\longleftrightarrow\; \widehat{f}$$

Thus, we have the *functional equation*

$$Z(s,\chi,f) \;=\; Z(1-s,\chi^{-1},\widehat{f})$$

This proves the analytic continuation and functional equation. ///

31. *Recapitulation*

Dirichlet characters, ideal-class characters, and, generally, Hecke's Grössencharakters all need to be redescribed as idele-class characters.

The explicit forms of invariant measures on $\mathbb{J}$ and $k_v^\times$ are mostly irrelevant.

Once a single non-trivial additive character ψ_v is chosen, local fields k_v are canonically isomorphic to their own unitary duals, and the same is true of $\mathbb{A}$.

Notions of Schwartz functions on $\mathbb{R}$ and $\mathbb{C}$ are well-documented and reasonably well-known, but the p-adic versions deserve amplification.

After a discussion of characters ψ on $\mathbb{A}/k$ as well as ψ_v on k_v, Fourier transforms are shown to stabilize the *local* Schwartz spaces. Local and global Fourier inversion can be proved without direct mention of the self-duality of local fields k_v and adeles $\mathbb{A}$. Fourier inversion for non-archimedean local fields is much easier than for $\mathbb{R}$.

One should certify the absolute convergence in Re $s > 1$ of the global zeta integrals

$$Z(s,\chi,f) \;=\; \int_{\mathbb{J}} |x|^s\,\chi(x)\,f(x)\,d^\times x \qquad\qquad (\text{for } f\in\mathscr{S}(\mathbb{A}),\ s\in\mathbb{C},\ \text{Re } s>1)$$

The good-prime finite-prime part of any of Hecke's L-functions looks like

$$L^S(s,\chi) \;=\; \prod_{v\notin S} \frac{1}{1-q_v^{-(s+it_v)}}$$

where S is a finite set of places, including archimedean ones, to be excluded, and the real number t_v is determined by χ_v. It is relatively straightforward to produce these local factors as local zeta integrals. However, the global zeta integrals inevitably contain bad-prime factors, and, even when f is chosen so that for simple reasons $Z(s,\chi,f)$ is well behaved at bad primes, the adelic Fourier transform $\widehat{f}$ usually frustrates a similar trivial analysis. Thus, local zeta integrals

$$Z_v(s,\chi_v,f_v) \;=\; \int_{k_v^\times} |x|_v^s\,\chi_v(x)\;f_v(x)\;d_v^\times x$$

with *arbitrary* data f_v must be proven meromorphic, or else meromorphic continuation of $L^S(s,\chi)$ does not follow! We do such a computation in the next section.

Poisson summation is not trivial. Indeed, the *classical* form of Poisson summation depends on *pointwise* convergence of (classical) Fourier series. Nevertheless, the adelic form, its consequence for functional equations of theta functions, and consequences for functional equations of zeta integrals, provides a viewpoint that completely avoids concerns over congruence conditions and ideal classes.

Fujisaki's compactness lemma is non-trivial, and all the more mysterious since its proof is unexpected.

In the proof of analytic continuation (and functional equation), one should verify that the *half-zeta* integrals, that is, over ideles of norm ≥ 1, really *are* nicely convergent for all $s\in\mathbb{C}$, *and* that this entails entire-ness. Factoring the elementary integrals (for trivial χ) over the product of $\mathbb{J}^1/k^\times$ and the ray $\mathbb{R}^+$ is less serious.

32. *Local functional equations*

The first point of *local functional equations* is to prove that local zeta integrals with any Schwartz data whatsoever are meromorphic functions, granting that any given (non-zero) local zeta integral at v is meromorphic.

Let f be a Schwartz function on a *local* field k, ψ a non-trivial additive character on k. Fix an additive Haar measure dx on k, and define the local Fourier transform

$$\widehat{f}(\xi) \;=\; \int_k f(x)\,\psi(x\xi)\,dx$$

Suppose that his additive Haar measure is normalized so that Fourier inversion holds:

$$\widehat{\widehat{f}}\,(x) \;=\; f(-x)$$

Let $d^\times x$ be multiplicative Haar measure on $k^\times$. For a complex number s, define the simplest class of **local zeta integral** by

$$Z(s,f) \;=\; \int_{k^\times} |x|^s\, f(x)\; d^\times x$$

[32.1] Theorem: *(Local functional equation)* For Schwartz functions f, g on the local field k, the local zeta integral $Z(s,f)$ is absolutely convergent for $\mathrm{Re}\,(s) > 0$, has a meromorphic continuation to $s \in \mathbb{C}$, and

$$Z(s,f)\,Z(1-s,\widehat{g}) \;=\; Z(1-s,\widehat{f})\,Z(s,g)$$

Equivalently,

$$\frac{Z(s,f)}{Z(1-s,\widehat{f})} \;=\; \frac{Z(s,g)}{Z(1-s,\widehat{g})}$$

Proof: Since Schwartz functions are integrable, so the only issue in convergence of local zeta integrals occurs at 0, due to the potential blow-up of $|x|^s \cdot d^\times x$ there. Since Schwartz functions are locally constant near 0, it suffices to observe the finiteness of

$$\int_{\mathrm{ord} x \ge 0} |x|^{\mathrm{Re}\,(s)}\, d^\times x \;=\; \mathrm{const}\cdot \sum_{\ell\ge 0} q^{-\ell\cdot \mathrm{Re}\,(s)} \;<\; \infty \qquad\qquad (\text{for } \mathrm{Re}\,(s) > 0)$$

where q is the residue class field cardinality.

For the functional equation, take $0 < \mathrm{Re}\,(s) < 1$, so that the integrals for both $Z(s,f)$ and $Z(1-s,\widehat{g})$ are absolutely convergent. Then the local functional equation is a direct computation, as follows. Fubini is invoked throughout to change orders of integration. Some reflection may indicate that the crucial step is to expand the definition and replace y by yx/η:

$$\begin{aligned}
Z(s,f)\,Z(1-s,\widehat{g}) \;&=\; \int_{k^\times}\int_{k^\times} |x|^s\, f(x)\; |y|^{1-s}\, \widehat{g}(y)\; d^\times x\; d^\times y \\
&=\; \int_k \int_{k^\times}\int_{k^\times} \overline{\psi}(y\eta)\, |x|^s\, f(x)\; |y|^{1-s}\, g(\eta)\; d^\times y d^\times x\;\; d\eta \\
&=\; \int_k \int_{k^\times}\int_{k^\times} \overline{\psi}(yx)\, |x|^s\, f(x)\; |yx/\eta|^{1-s}\, g(\eta)\; d^\times y\; d^\times x\; d\eta \\
&=\; \int_k \int_{k^\times}\int_{k^\times} \overline{\psi}(yx)\, |x|^1\, f(x)\; |y|^{1-s}\; |\eta|^{s-1}\, g(\eta)\; d^\times y\; d^\times x\; d\eta
\end{aligned}$$

All that's left is to simplify and re-pack the integrals: the measure $|x|\cdot d^\times x$ is a constant multiple of the additive Haar measure dx. The precise constant is irrelevant, since it cancels itself in the necessary rearrangement:

$$|x|\,|\eta|^{-1}\,d^\times x\,d\eta \;=\; dx\,d^\times\eta$$

Also, it is convenient that for local fields k and $k^\times$ differ by a single point, of additive measure 0. Thus, continuing the previous computation,

$$\begin{aligned} Z(s,f)\,Z(1-s,\widehat{g}) &= \int_{k^\times}\int_k\int_{k^\times} \overline{\psi}(yx)\,f(x)\,|y|^{1-s}\,|\eta|^s\,g(\eta)\,d^\times y\,dx\,d^\times\eta \\ &= \int_{k^\times}\int_{k^\times} \widehat{f}(y)\,|y|^{1-s}\,|\eta|^s\,g(\eta)\,d^\times y\,d^\times\eta \\ &= Z(1-s,\widehat{f})\,Z(s,g) \end{aligned}$$

This proves the local functional equation in the region $0 < \mathrm{Re}(s) < 1$, so the general assertion follows from the Identity Principle from complex analysis. ///

[32.2] Remark: The local functional equations *locally everywhere* do not yield the *global* functional equation. Rather, the point of the local functional equations is to prove the *irrelevance* of the choice of local data f, g, as well as the *meromorphic continuation* of local zeta integrals for arbitrary data.

33. *The elementary global integral*

The poles and residues of zeta integrals are multiples of an elementary integral over $\mathbb{J}^+/k^\times$, which we claim is

$$\int_{\mathbb{J}^+/k^\times} |x|^{1-s}\,d^\times x = \frac{|\mathbb{J}^1/k^\times|}{s-1}$$

Multiplicative measures on $\mathbb{J}$ and $k_v^\times$ are completely determined by giving local units $\mathfrak{o}_v^\times$ measure 1 at *all* finite places, and $d^\times x = \frac{d^+x}{|x|_v}$ at archimedean places. Keep in mind that the product-formula norm $|\cdot|_\mathbb{C}$ is

$$|x|_\mathbb{C} \;=\; |N^\mathbb{C}_\mathbb{R}(x)|_\mathbb{R} \;=\; |x\,\overline{x}|_\mathbb{R} \;=\; \text{square of usual complex norm}$$

That is, the usual complex norm *extends* the norm on $\mathbb{R}$, but for zeta-integrals we must *compose* with the Galois norm.

For *abelian* (hence, *unimodular*) topological groups, the general riff

$$\int_G f(g)\,dg \;=\; \int_{H\backslash G}\Big(\int_H f(h\dot{g})\,dh\Big)\,d\dot{g}$$

applies: fixing any two of the three measures uniquely specifies the normalizing constant for the third so that the equation holds.

Our locally-everywhere normalization of measures on $k_v^\times$ specifies the measure on $\mathbb{J}$. Counting measure on $k^\times$ uniquely specifies the measure on $\mathbb{J}/k^\times$ by *one* instance of the above identity (with the sum being a type of integral, of course)

$$\int_\mathbb{J} f(g)\,dg \;=\; \int_{\mathbb{J}/k^\times}\sum_{h\in k^\times} f(h\dot{g})\,d\dot{g}$$

The subgroup $\mathbb{J}^1/k^\times$ of $\mathbb{J}/k^\times$ is *compact*, by Fujisaki, but we do not try to specify its measure directly. Instead, since $\mathbb{J}^1$ is the kernel of $|\cdot|$, $\mathbb{J}^1/k^\times$ fits into an exact sequence

$$1 \longrightarrow \mathbb{J}^1/k^\times \longrightarrow \mathbb{J}/k^\times \longrightarrow \mathbb{R}^+ \longrightarrow 1 \qquad (\mathbb{R}^+ = (0,+\infty))$$

Thus, the usual measure $\frac{dx}{x}$ on $\mathbb{R}^+$ and the measure on $\mathbb{J}/k^\times$ uniquely determine the measure on $\mathbb{J}^1/k^\times$ by

$$\int_{\mathbb{J}/k^\times} f(g)\,dg \;=\; \int_{(\mathbb{J}/k^\times)/(\mathbb{J}^1/k^\times)} \Big(\int_{\mathbb{J}^1/k^\times} f(h\dot{g})\,dh\Big)\,d\dot{g} \;=\; \int_{\mathbb{R}^+} \Big(\int_{\mathbb{J}^1/k^\times} f(h\dot{g})\,dh\Big)\,d\dot{g}$$

It is not absolutely necessary, but it is easy to identify a *section* $\sigma:\mathbb{R}^+\to\mathbb{J}$ having the property $|\sigma(t)|=t$. For $k=\mathbb{Q}$, just map $t\to(t,1,1,\ldots)$, the idele with trivial entries except at $\mathbb{Q}_\infty^\times\approx\mathbb{R}^\times$, where the entry is t. For general number fields k, with r_1,r_2 real-and-complex completions, let

$$\sigma(t) \;=\; (t^{\frac{1}{r_1+r_2}},\ldots,t^{\frac{1}{r_1+r_2}},1,1,1,1,\ldots)$$

with non-trivial entries at archimedean places.

With f the product of $|\cdot|^{1-s}$ and the characteristic function of $\mathbb{J}^+/k^\times$, this gives

$$\int_{\mathbb{J}^+/k^\times} |g|^{1-s}\,dg \;=\; \int_{(\mathbb{J}^+/k^\times)/(\mathbb{J}^1/k^\times)} \Big(\int_{\mathbb{J}^1/k^\times} |gh|^{1-s}\,dh\Big)\,d\dot{g} \;=\; \int_{(\mathbb{J}^+/k^\times)/(\mathbb{J}^1/k^\times)} \Big(\int_{\mathbb{J}^1/k^\times} |g|^{1-s}\,dh\Big)\,d\dot{g}$$

$$= \int_{[1,+\infty)} |\dot{g}|^{1-s}\Big(\int_{\mathbb{J}^1/k^\times} 1\,dh\Big)\,d\dot{g} \;=\; |\mathbb{J}^1/k^\times|\cdot\int_1^\infty t^{1-s}\,\frac{dt}{t}$$

$$= |\mathbb{J}^1/k^\times|\cdot\int_1^\infty t^{-s}\,dt \;=\; |\mathbb{J}^1/k^\times|\cdot\Big[\frac{t^{1-s}}{1-s}\Big]_1^\infty \;=\; \frac{|\mathbb{J}^1/k^\times|}{s-1} \qquad ///$$

[33.1] Remark: A little later, we do the non-elementary computation that

$$|\mathbb{J}^1/k^\times| \;=\; \frac{2^{r_1}\,(2\pi)^{r_2}\,h\,R}{D_k^{\frac{1}{2}}\,w}$$

34. *Vanishing of ramified elementary global integrals*

A character χ_v on $k_v^\times$ is *unramified* if it factors through the *norm*, that is, is of the form $x\to|x|_v^{s_v}$ for some $s_v\in\mathbb{C}$.

For non-archimedean k_v, for χ_v on $k_v^\times$ to be *ramified* means that it is non-trivial on $\mathfrak{o}_v^\times$ for finite places. For $k_v\approx\mathbb{R}$, a ramified character depends on *sign*. For $k_v\approx\mathbb{C}$, a ramified character depends on *argument*.

A character χ on $\mathbb{J}$ is *ramified* if it is ramified on some $k_v^\times$. Ramification is equivalent to *not* being $\mathbb{J}^1$-invariant. The same terminology applies to characters on $\mathbb{J}/k^\times$.

[34.1] Claim: For *ramified* χ, the elementary global integral vanishes:

$$\int_{J^+/k^\times} |x|^s\,\chi(x)\,d^\times x \;\;=\;\; 0 \qquad\qquad (\text{for } \chi \text{ ramified})$$

Thus, the residues of global zeta integrals $Z(s,\chi,f)$ at $s=0,1$ are 0 for ramified χ, so such global zeta integrals are *entire*.

Proof: For lighter notation, absorb the $|x|^s$ into χ. Use the integration riff

$$\int_G f(g)\,dg \;=\; \int_{H\backslash G} \Big(\int_H f(h\dot{g})\,dh\Big)\,d\dot{g}$$

to obtain

$$\int_{\mathbb{J}^+/k^\times} \chi(g)\,dg \;=\; \int_{(\mathbb{J}^+/k^\times)/(\mathbb{J}^1/k^\times)} \Big(\int_{\mathbb{J}^1/k^\times} \chi(\dot{g}h)\,dh\Big)\,dg$$

This invites a variant of the cancellation lemma: to be clear, we give the very slightly modified argument... let $h_o \in \mathbb{J}^1$ be such that $\chi(h_o) \neq 1$. Then, replacing h by hh_o,

$$\int_{\mathbb{J}^1/k^\times} \chi(\dot{g}h)\,dh \;=\; \int_{\mathbb{J}^1/k^\times} \chi(\dot{g}hh_o)\,dh \;=\; \chi(h_o)\cdot \int_{\mathbb{J}^1/k^\times} \chi(\dot{g}h)\,dh$$

Thus, the inner integral cancels, so the whole integral is 0. ///

35. *Good finite-prime local zeta integrals*

Good includes the assertion that the local Schwartz function f_v in the local zeta integral expression

$$Z_v(s,f_v) \;=\; \int_{k_v^\times} |x|_v^s\, f_v(x)\; d^\times x$$

is the *characteristic function* of the local integers $\mathfrak{o}_v$. The *good prime* assumption also includes less obvious, important points. By convention, *archimedean* primes are *never* good.

The good prime assumption includes the assertion that k_v is *absolutely unramified*, meaning k_v is unramified over the corresponding completion $\mathbb{Q}_p$, meaning p *stays prime* in $\mathfrak{o}_v$.

We will show that unramifiedness entails that the natural measure is $|\mathfrak{o}_v| = 1$, and the Fourier transform of the characteristic function of $\mathfrak{o}_v$ is *itself*. But these points do not affect the local *multiplicative* computation.

First, at finite primes, *always* normalize the multiplicative Haar measure so that $|\mathfrak{o}_v^\times| = 1$. Then the usual

$$\int_G f(g)\,dg \;=\; \int_{G/H}\int_H f(\dot{g}h)\;dh\;\;dg$$

with f the product of $|\cdot|_v^s$ and the characteristic function of $\mathfrak{o}_v$ gives

$$\int_{k_v^\times} f(g)\,dg \;=\; \int_{k_v^\times/\mathfrak{o}_v^\times}\int_{\mathfrak{o}_v^\times} f(\dot{g}h)\;dh\;\;dg \;=\; \int_{(k_v^\times\cap\mathfrak{o}_v)/\mathfrak{o}_v^\times}\int_{\mathfrak{o}_v^\times} |\dot{g}h|_v^s\;dh\;\;dg \;=\; \int_{(k_v^\times\cap\mathfrak{o}_v)/\mathfrak{o}_v^\times} |\dot{g}|_v^s\Big(\int_{\mathfrak{o}_v^\times} 1\;dh\Big)\,dg$$

$$=\; \int_{(k_v^\times\cap\mathfrak{o}_v)/\mathfrak{o}_v^\times} |\dot{g}|_v^s\;dg \;=\; \sum_{n=0}^{\infty} |p^n|_v^s \;=\; \frac{1}{1-|p|_v^{-s}} \;=\; \frac{1}{1-q_v^{-s}}$$

where $q_v \;=\; |p|_v^{-1}$ is the residue field cardinality. ///

The same computation applies to the *seemingly* more general

$$Z_v(s,\chi_v,f_v) \;=\; \int_{k_v^\times} |x|_v^s\,\chi_v(x)\,f_v(x)\;d^\times x$$

with f_v the characteristic function of $\mathfrak{o}_v$ and χ_v *unramified*, meaning that χ_v is trivial on $\mathfrak{o}_v^\times$. That is, the group homomorphism χ_v is $\mathfrak{o}_v$-invariant, so is inescapably of the form

$$\chi_v(x) \;=\; |x|_v^{it_\chi} \qquad\qquad \text{(for some } t_\chi \in \mathbb{R} \text{ depending on } \chi_v\text{)}$$

Then the unramified non-archimedean local zeta factor is

$$Z_v(s,\chi_v,f_v) \;=\; \int_{k_v^\times} |x|_v^s\,\chi_v(x)\,f_v(x)\,d^\times x \;=\; \int_{k_v^\times} |x|_v^{s+it_\chi}\,f_v(x)\,d^\times x \;=\; \frac{1}{1-q_v^{-s-it_\chi}}$$

This shifting of the exponent occurs for all kinds of L-functions.

For example, for groundfield $k=\mathbb{Q}$, for Dirichlet L-functions $L(s,\chi)$ the good-prime factors are

$$\frac{1}{1-\dfrac{\chi(p)}{p^s}} \;=\; \frac{1}{1-p^{-s+\frac{i\theta}{\log p}}} \qquad\qquad (\text{where } \chi(p)=e^{i\theta})$$

That is, here the local characters at unramified $p\sim v$ are

$$\chi_v(x) \;=\; |x|_v^{-\frac{i\theta}{\log p}}$$

with $e^{i\theta}$ a root of unity.

For an *ideal class character* χ, for number field k, for local parameter ϖ_v in k_v,

$$\chi_v(\varpi_v)^h \;=\; 1 \qquad\qquad (\text{with } h=h(\mathfrak{o}))$$

so $\chi_v(x_v)=|x|_v^{\frac{2\pi i\ell}{h\log q_v}}$ for some $\ell\in\mathbb{Z}$. For general *großencharakteren* there is no connection to roots of unity.

36. *Archimedean local zeta integrals*

Although archimedean places are never *good*, they are tractable.

[36.1] Real local zeta integrals The standard *unramified* local integral for $v\approx\mathbb{R}$ uses the Gaussian $f(x)=e^{-\pi x^2}$:

$$Z_{\mathbb{R}}(s,e^{-\pi x^2}) \;=\; \int_{\mathbb{R}^\times} |y|^s\,e^{-\pi y^2}\,\frac{dy}{|y|} \;=\; 2\int_0^\infty |y|^s\,e^{-\pi y^2}\,\frac{dy}{y} \;=\; \int_0^\infty |y|^{\frac{s}{2}}\,e^{-\pi y}\,\frac{dy}{y} \qquad (\text{replacing } y \text{ by } \sqrt{y})$$

$$=\; \pi^{-\frac{s}{2}}\int_0^\infty |y|^{\frac{s}{2}}\,e^{-y}\,\frac{dy}{y} \;=\; \pi^{-\frac{s}{2}}\cdot\Gamma\big(\frac{s}{2}\big)$$

[36.2] Remark: This recovers Riemann's gamma factor, despite the integral starting out with a different-looking normalization than Riemann's integral representation

$$\int_0^\infty y^{\frac{s}{2}}\,\frac{\theta(iy)-1}{2}\,\frac{dy}{y}$$

The only *ramified* character on $\mathbb{R}^\times$ is $y\to\operatorname{sgn}(y)|y|^s$. The standard *ramified* local integral for $v\approx\mathbb{R}$ uses $f(x)=xe^{-\pi x^2}$:

$$Z_{\mathbb{R}}(s,\operatorname{sgn},xe^{-\pi x^2}) \;=\; \int_{\mathbb{R}^\times} |y|^s\,\operatorname{sgn}(y)\cdot ye^{-\pi y^2}\,\frac{dy}{|y|} \;=\; \int_{\mathbb{R}^\times} |y|^s\cdot|y|\cdot e^{-\pi y^2}\,\frac{dy}{|y|} \;=\; 2\int_0^\infty |y|^{s+1}\,e^{-\pi y^2}\,\frac{dy}{y}$$

$$=\; \int_0^\infty |y|^{\frac{s+1}{2}}\,e^{-\pi y}\,\frac{dy}{y} \;=\; \pi^{-\frac{s+1}{2}}\int_0^\infty |y|^{\frac{s+1}{2}}\,e^{-y}\,\frac{dy}{y} \;=\; \pi^{-\frac{s+1}{2}}\,\Gamma\big(\frac{s+1}{2}\big)$$

This recovers the gamma factor for *odd* Dirichlet character L-functions $L(s,\chi)$, for example.

[36.3] Complex local zeta integrals

The correct normalization of measure, norm, and Fourier transform on $k_v \approx \mathbb{C}$ require some attention. This is typical of non-archimedean extensions $k_v/\mathbb{Q}_p$, too, but we have less prejudice about computations there than on $\mathbb{C}$.

Again, the product formula requires

$$|z|_{\mathbb{C}} \;=\; |N^{\mathbb{C}}_{\mathbb{R}}(z)|_{\mathbb{R}} \;=\; |z|^2 \qquad\qquad (\text{the latter the } \textit{usual} \text{ norm})$$

That is, our *usual* norm is the *extension* from $\mathbb{R}$ to $\mathbb{C}$, while the product formula demands something else, namely, *composition with Galois norm.*

Similarly, the *additive character* $\psi_{\mathbb{C}}(z)$ is

$$\psi_{\mathbb{C}}(z) \;=\; \psi_{\mathbb{R}}(\mathrm{tr}^{\mathbb{C}}_{\mathbb{R}}(z)) \;=\; e^{2\pi i(z+\overline{z})} \;=\; e^{4\pi i \mathrm{Re}\,(z)}$$

Since we cannot talke about *ramification of primes*, nor local or global *differents* $\mathfrak{d}_v, \mathfrak{d}$ as for non-archimedean places, suitable normalization of measure on $k_v \approx \mathbb{C}$ is determined by choice of character and the requirement that *Fourier inversion* hold with the same measure on both copies of $\mathbb{C}$, the original as well as the spectral side.

That is, determine a measure constant c by requiring, for all $f \in \mathscr{S}(\mathbb{C})$,

$$f(z) \;=\; \int_{\mathbb{C}}\int_{\mathbb{C}} \psi_{\mathbb{C}}(zw)\; \psi_{\mathbb{C}}(-w\zeta)\; f(\zeta)\; c\, d\zeta\; c\, dw$$

That is, letting $z = x+iy$, $w = u+iv$, and $\zeta = \xi + i\eta$,

$$f(z) \;=\; c^2 \cdot \int_{\mathbb{C}}\int_{\mathbb{C}} e^{2\pi i \mathrm{tr}(w(z-\zeta))}\; f(\zeta)\; d\zeta\; dw \;=\; c^2 \cdot \int_{\mathbb{C}}\int_{\mathbb{C}} e^{2\pi i((2u)(x-\xi)+(-2v)(y-\eta))}\; f(\zeta)\; d\zeta\; dw$$

We know Fourier inversion holds with the *usual* measure on $\mathbb{C}$, and with character $e^{2\pi i(ux+vy)}$. To compare to this, in the integral above replace u by $u/2$ and v by $-v/2$, giving

$$\frac{c^2}{2^2} \cdot \int_{\mathbb{C}}\int_{\mathbb{C}} e^{2\pi i(u(x-\xi)+v(y-\eta))}\; f(\zeta)\; d\zeta\; dw \;=\; \frac{c^2}{2^2} \cdot f(z)$$

Thus, the proper normalization of measure on $\mathbb{C}$ for Iwasawa-Tate is

$$d_{\mathbb{C}}(z) \;=\; 2 \cdot d_{\mathrm{usual}}(z)$$

Next, determine a Gaussian $e^{-c(x^2+y^2)}$ which is its own Fourier transform.

$$2 \cdot \int_{\mathbb{C}} e^{-4\pi i(ux-vy)}\; e^{-c(x^2+y^2)}\; dx\, dy \;=\; \frac{2\pi}{c} \cdot \int_{\mathbb{C}} e^{-2\pi i((2u)x-(2v)y)}\; e^{-\pi(x^2+y^2)}\; dx\, dy \;=\; \frac{2\pi}{c} \cdot e^{-\frac{4\pi^2}{c}(u^2+v^2)}$$

Thus, two reasons for $c = 2\pi$, so $f(w) = e^{-2\pi w\overline{w}}$.

Try taking corresponding multiplicative measure $2\,dz/|z|_{\mathbb{C}}$. Thus, the standard *unramified* complex zeta integral is

$$\int_{\mathbb{C}} |z|^s_{\mathbb{C}}\; e^{-2\pi z\overline{z}}\; \frac{2\,dz}{|z|_{\mathbb{C}}} \;=\; 4\pi \int_0^\infty r^{2s}\; e^{-2\pi r^2}\; r\, \frac{dr}{r^2}$$

$$=\; 4\pi \int_0^\infty r^{2s}\; e^{-2\pi r^2}\; \frac{dr}{r} \;=\; 2\pi \int_0^\infty r^s\; e^{-2\pi r}\; \frac{dr}{r} \;=\; 2\pi \cdot (2\pi)^{-s}\, \Gamma(s)$$

The extra constant 2π in front (*not* the $(2\pi)^{-s}$) suggests renormalizing the multiplicative measure by dividing through by 2π. Some sources do this, others leave the extra 2π.

The *ramified* unitary characters of $\mathbb{C}^\times$ are

$$\chi_\ell(re^{i\theta})|re^{i\theta}|^s_{\mathbb{C}} \;=\; e^{i\ell\theta}\cdot r^{2s} \qquad\qquad (\text{for } 0\neq\ell\in\mathbb{Z})$$

The standard choice of Schwartz function for the complex zeta integral depends on the sign of $\ell\in\mathbb{Z}$. For $\ell>0$, it is

$$\int_{\mathbb{C}} |z|^s_{\mathbb{C}}\;\chi_\ell(z)\;\overline{z}^\ell\;\;e^{-2\pi z\overline{z}}\;\frac{2\,dz}{|z|_{\mathbb{C}}} \;=\; \int_0^{2\pi}\int_0^\infty r^{2s}\;e^{i\ell\theta}\;(re^{-i\theta})^\ell\;e^{-2\pi z\overline{z}}\;\frac{2\,dz}{|z|_{\mathbb{C}}} \;=\; 4\pi\int_0^\infty r^{2s+\ell}\;e^{-2\pi r^2}\;r\,\frac{dr}{r^2}$$

$$=\;4\pi\int_0^\infty r^{2s+\ell}\;e^{-2\pi r^2}\;\frac{dr}{r} \;=\; 2\pi\int_0^\infty r^{s+\frac{\ell}{2}}\;e^{-2\pi r}\;\frac{dr}{r} \;=\; 2\pi\cdot(2\pi)^{-(s+\frac{\ell}{2})}\int_0^\infty r^{s+\frac{\ell}{2}}\;e^{-r}\;\frac{dr}{r}$$

$$=\;2\pi\cdot(2\pi)^{-(s+\frac{\ell}{2})}\,\Gamma\big(s+\frac{\ell}{2}\big) \qquad\qquad (\text{for } 0<\ell\in\mathbb{Z})$$

For $\ell<0$, the standard ramified complex local zeta integral is

$$\int_{\mathbb{C}} |z|^s_{\mathbb{C}}\;\chi_\ell(z)\;\;z^{|\ell|}\;\;e^{-2\pi z\overline{z}}\;\frac{2\,dz}{|z|_{\mathbb{C}}} \;=\; \int_0^{2\pi}\int_0^\infty r^{2s}\;e^{i\ell\theta}\;(re^{i\theta})^{-\ell}\;e^{-2\pi z\overline{z}}\;\frac{2\,dz}{|z|_{\mathbb{C}}} \;=\; 4\pi\int_0^\infty r^{2s-\ell}\;e^{-2\pi r^2}\;r\,\frac{dr}{r^2}$$

$$=\;4\pi\int_0^\infty r^{2s-\ell}\;e^{-2\pi r^2}\;\frac{dr}{r} \;=\; 2\pi\int_0^\infty r^{s-\frac{\ell}{2}}\;e^{-2\pi r}\;\frac{dr}{r} \;=\; 2\pi\cdot(2\pi)^{-(s-\frac{\ell}{2})}\int_0^\infty r^{s-\frac{\ell}{2}}\;e^{-r}\;\frac{dr}{r}$$

$$=\;2\pi\cdot(2\pi)^{-(s-\frac{\ell}{2})}\,\Gamma\big(s-\frac{\ell}{2}\big) \qquad\qquad (\text{for } \ell\leq 0)$$

Thus, for *both* $\ell>0$ and $\ell<0$, the local zeta integral is

$$2\pi\cdot(2\pi)^{-(s+\frac{|\ell|}{2})}\,\Gamma\big(s+\frac{|\ell|}{2}\big) \qquad\qquad (\text{for both } \ell\geq 0 \text{ and } \ell\leq 0)$$

---

37. *Convergence of local zeta integrals*

As usual, suppose χ_v is *unitary* meaning $|\chi_v|=1$, since any non-unitary part could be absorbed into $|\cdot|^s$. Use the standard notation $\sigma=\mathrm{Re}(s)$.

Treat the non-archimedean case first. Since $f_v\in\mathscr{S}(k_v)$, for some n the support of f is contained in $\varpi^{-n}\mathfrak{o}_v$. Since f is locally constant and compactly supported, it has a finite bound C. Then

$$|Z_v(s,\chi_v,f_v)| \;\leq\; \int_{k_v^\times} |x|^\sigma\,|\chi(x)|\,|f(x)|\,dx \;\leq\; C\cdot\int_{k_v^\times\cap\varpi^{-n}\mathfrak{o}_v} |x|^\sigma\,dx$$

$$=\;C\cdot\int_{(k_v^\times\cap\varpi^{-n}\mathfrak{o}_v)/\mathfrak{o}_v^\times} |x|^\sigma\Big(\int_{\mathfrak{o}_v^\times}1\Big)\,dx \;=\; C\cdot\sum_{\ell=-n}^\infty |\varpi^\ell|_v^\sigma \;=\; C\cdot\frac{q_v^{n\sigma}}{1-q_v^{-\sigma}} \;<\;\infty \qquad\qquad (\text{for } \sigma=\mathrm{Re}(s)>0)$$

For $k_v\approx\mathbb{R}$, given $f\in\mathscr{S}(\mathbb{R})$ for each N that

$$|f(x)|\;\;\ll_N\;\;(1+|x|^2)^{-N}$$

With $\sigma = \mathrm{Re}(s) > 0$, the local zeta integral is

$$|Z_v(s,\chi_v,f_v)| \ll_N \int_{\mathbb{R}^\times} |x|^\sigma\, |\chi_v(x)|\,(1+x^2)^{-N}\,\frac{dx}{|x|} \;\ll\; \int_0^\infty |x|^{\sigma-1}\,(1+x^2)^{-N}\,dx$$

$$\ll \int_0^1 |x|^{\sigma-1}\,dx \;+\; \int_1^\infty |x|^{\sigma-1-2N}\,dx$$

Given $\sigma > 0$, take N large enough so that $\sigma - 1 - 2N < -1$ gives convergence.

Convergence of the complex integrals is similar. ///

[37.1] Fourier transform eigenfunctions Whenever possible, we want local Schwartz functions f_v which are eigenfunctions for Fourier transform, preferably unchanged, so that in the *global* functional equation $Z(s,\chi,f) = Z(1-s,\overline{\chi},\widehat{f})$ as many local factors as possible are the same on both sides, apart from $s \leftrightarrow 1-s$ and $\chi \leftrightarrow \overline{\chi}$.

For absolutely unramified $k_v/\mathbb{Q}_p$, the characteristic function of the local integers $\mathfrak{o}_v$ is its own Fourier transform. For χ_v unramified at v, this gives the desired symmetry.

On $\mathbb{R}$, the Gaussian $e^{-\pi x^2}$ is its own Fourier transform.

On $\mathbb{R}$, for ramified $\chi_\mathbb{R}$, that is, for $\mathrm{sgn}(x)\,|x|^s$, the function $f_v(x) = xe^{-\pi x^2}$ is multiplied by $-i$ under Fourier transform, by contour-shifting:

$$\widehat{f_v}(\xi) \;=\; \int_\mathbb{R} e^{-2\pi i\xi x}\; x\,e^{-\pi x^2}\;dx \;=\; \int_\mathbb{R} e^{-2\pi i\xi(x-i\xi)}\;(x-i\xi)\,e^{-\pi(x-i\xi)^2}\;dx$$

$$=\; e^{-\pi\xi^2}\int_\mathbb{R}(x-i\xi)\,e^{-\pi x^2}\;dx \;=\; e^{-\pi\xi^2}\cdot\big(0-i\xi\big) \;=\; -i\xi e^{-\pi\xi^2}$$

Fourier transforms of Schwartz functions for ramified characters on $k_v \approx \mathbb{C}$ are the critical sub-case of *Hecke's identity*.

[37.2] Claim: The Schwartz function $(x \pm iy)^\ell\, e^{-\pi(x^2+y^2)}$ is an eigenfunction for Fourier transform, with eigenvalue $i^{-\ell}$.

Proof: Just do the case $(x+iy)^\ell\, e^{-\pi(x^2+y^2)}$. Rewrite this as $z^\ell e^{-\pi z\overline{z}}$, and rewrite the Fourier transform as

$$\int_\mathbb{C} e^{-\pi i(z\overline{w}+\overline{z}w)}\,z^\ell\,e^{-\pi z\overline{z}}\;dz \;=\; (-\pi i)^{-\ell}\Big(\frac{\partial}{\partial\overline{w}}\Big)^\ell\!\int_\mathbb{C} e^{-\pi i(z\overline{w}+\overline{z}w)}\,e^{-\pi z\overline{z}}\;dz \;=\; (-\pi i)^{-\ell}\Big(\frac{\partial}{\partial\overline{w}}\Big)^\ell e^{-\pi w\overline{w}}$$

$$=\; (-\pi i)^{-\ell}(-\pi w)^\ell\,e^{-\pi w\overline{w}} \;=\; i^{-\ell}\cdot w^\ell\,e^{-\pi w\overline{w}}$$

This presumes $\partial/\partial\overline{w}$ works as expected, which it does. ///

[37.3] Remark: Since $f^{\widehat{}\,\widehat{}}(x) = f(-x)$, necessarily $f^{\widehat{}\,\widehat{}\,\widehat{}\,\widehat{}} = f$, for all f. Thus, the only possible eigenvalues of Fourier transform are $\pm1, \pm i$. Further, the corresponding components are easy to pick out: with $\varepsilon \in \{\pm1,\pm i\}$, the ε^{th} component of f is

$$f \;+\; \varepsilon^{-1}\widehat{f} \;+\; \varepsilon^{-2}f^{\widehat{}\,\widehat{}} \;+\; \varepsilon^{-3}f^{\widehat{}\,\widehat{}\,\widehat{}}$$

38. *Convergence of global half-zeta integrals*

The point is to genuinely prove convergence of the half-zeta integrals

$$\int_{|y|\geq 1} |y|^s\, f(y)\, dy$$

with f a Schwartz function on the adeles, for *all* $s \in \mathbb{C}$.

Since f is at worst a *finite* sum of monomials $\otimes_v f_v$, without loss of generality we take it to be such a monomial, with f_v Schwartz on k_v. Since f is Schwartz, for all N there is a constant C_N (depending on f) such that

$$|f(x)| \;\leq\; C_N \cdot \prod_v \sup(|x_v|_v, 1)^{-2N} \qquad\qquad \text{(for adele } x = \{x_v\}\text{)}$$

For an *idele* y define the **gauge**[9]

$$\nu(y) \;=\; \prod_v \sup\{|y_v|_v,\, |\frac{1}{y_v}|_v\}$$

Almost all factors on the right-hand side are 1, so there is no issue of convergence. Further, note that

$$\big(\sup\{a,\, 1\}\big)^2 \;=\; \sup\{a^2,\, 1\} \;=\; a\cdot \sup\{a,\, \frac{1}{a}\} \qquad\qquad \text{(for } a > 0\text{)}$$

Applying the latter equality to every factor,

$$\prod_v \sup(|y_v|_v, 1)^{-2N} \;=\; |y|^{-N} \prod_v \sup(|y_v|_v,\, \frac{1}{|y_v|_v})^{-N} \;=\; |y|^{-N}\nu(y)^{-N}$$

Thus, on the set of ideles $\{|y| \geq 1\}$,

$$\prod_v \sup(|y_v|_v, 1)^{-2N} \;=\; |y|^{-N}\nu(y)^{-N} \;\leq\; \nu(y)^{-N} \qquad\qquad \text{(when } |y|\geq 1,\ N \geq 0\text{)}$$

Thus, with $\sigma = \mathrm{Re}\, s$, for every $N \geq 0$

$$\Big|\int_{|y|\geq 1} |y|^s\, f(y)\, dy\Big| \;\ll\; \int_{|y|\geq 1} |y|^\sigma\, \nu(y)^{-N}\, dy \;\ll\; \int_{\mathbb{J}} |y|^\sigma\, \nu(y)^{-N}\, dy \;=\; \prod_v \Big(\int_{k_v^\times} |y|^\sigma\, \sup(|y|,\, \frac{1}{|y|})^{-N}\, dy\Big)$$

For $N > |\sigma|$, the non-archimedean local integrals are absolutely convergent:

$$\int_{k_v^\times} |y|^\sigma\, \sup(|y|,\, \frac{1}{|y|})^{-N}\, dy \;=\; \sum_{\ell=0}^\infty q_v^{-\sigma-N} \;+\; \sum_{\ell=1}^\infty q_v^{\sigma-N}$$

$$=\; \frac{1}{1-q^{-\sigma-N}} + \frac{q^{\sigma-N}}{1-q^{\sigma-N}} \;=\; \frac{1-q^{-2N}}{(1-q^{-\sigma-N})\,(1-q^{\sigma-N})}$$

The archimedean integrals are convergent for similarly over-whelming reasons. For $2N > 1$ and $N > |\sigma|+1$, the product over places is dominated by the Euler product for the completed zeta functions $\xi_k(N+\sigma)\xi_k(N-\sigma)/\xi_k(2N)$, which converges absolutely. ///

[9] Such a gauge is often called a *group norm*. The latter terminology is mildly unfortunate, since it is not a norm in the vector space sense. Nevertheless, the terminology is standard.

[38.1] Lemma: For all N, a Schwartz function f on $\mathbb{A}$ satisfies

$$|f(x)| \ll_{f,N} \prod_v \sup(|x_v|_v, 1)^{-2N} \qquad \text{(for } x \in \mathbb{A})$$

Proof: By definition, $f \in \mathscr{S}(\mathbb{A})$ is a finite sum of *monomials* $f = \bigotimes_v f_v$. Thus, it suffices to consider monomial f, and to prove the *local* assertion that for $f_v \in \mathscr{S}(k_v)$

$$|f_v(x)| \ll_{N,f_v} \sup(|x_v|_v, 1)^{-2N} \qquad \text{(for } x \in k_v)$$

At archimedean places, the definition of the Schwartz space requires that

$$\sup_{x \in k_v} (1 + |x|_v)^N \cdot |f_v(x)| < \infty \qquad \text{(for archimedean } k_v, \text{ for all } N)$$

Thus, for archimedean k_v,

$$|f_v(x)| \ll_{f,N} (1 + |x|_v)^{-2N} \le \sup(|x|_v, 1)^{-2N}$$

Almost everywhere, f_v is the characteristic function of the local integers. At such places,

$$|f_v(x)| = \left\{ \begin{matrix} 1 & (\text{for } |x|_v \le 1) \\ \\ 0 & (\text{for } |x|_v > 1) \end{matrix} \right\} \le \sup(|x_v|_v, 1)^{-2N} \qquad \text{(for all } N)$$

At the remaining *bad* finite primes, $f_v \in \mathscr{S}(k_v)$ is compactly supported and locally compact. Then, similar to the *good* prime case,

$$|f_v(x)| \ll_{f_v} \left\{ \begin{matrix} 1 & (x \in \mathrm{spt} f_v) \\ \\ 0 & (x \notin \mathrm{spt} f_v) \end{matrix} \right\} \ll_{f_v,N} \sup(|x_v|_v, 1)^{-2N} \qquad \text{(for all } N)$$

This proves the lemma. ///

39. *Classfield Theory: semi-classical preview, examples*

In brief, *global* classfield theory describes *abelian* extensions of *number fields* and function fields. Takagi and Artin accomplished this, independently, about 1928.

In brief, *local* classfield theory does the analogous things for *local fields*: finite extensions of $\mathbb{Q}_p$ and of $\mathbb{F}_p((x))$.

Details of these classifications subsume all known (abelian) **reciprocity laws**.

Non-abelian classfield theory is an almost entirely *conjectural* extension of (genuine) classfield theory to $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Proofs are much harder than *statements*, and there are various levels of sophistication of the statements themselves.

Main Theorem of Global Classfield Theory (classical form): The abelian (Galois) extensions K of a number field k are in bijection with generalized ideal class groups, which are quotients of *ray class groups* of *conductor* (a non-zero ideal) $\mathfrak{f}$

$$I(\mathfrak{f})/P_{\mathfrak{f}}^{+} \;=\; \frac{\text{fractional ideals prime to } \mathfrak{f}}{\text{principal ideals with totally positive generators 1 mod } \mathfrak{f}}$$

Further, the bijection sends a given generalized ideal class group to the (abelian) *Galois group* of the extension, via the *Artin/Frobenius* map/symbols $\mathfrak{p} \to (\mathfrak{p}, K/k)$ [see below].

Main Theorem of Local Classfield Theory: The abelian (Galois) extensions K of a local field k are in bijection with the open, finite-index subgroups of $k^\times$, by

$$K/k \;\longleftrightarrow\; k^\times/N_k^K K^\times$$

This bijection is given by an isomorphism of the Galois group with $k^\times/N_k^K K^\times$ via Artin/Frobenius.

[39.1] Remark: Historically, local classfield theory was proven as a *corollary* of global classfield theory, using the idea that, given an abelian extension of a local field, there is an extension K/k of *number* fields and completions k_v of k and K_w of K such that K_w/k_v is the given extension of local fields.

Global classfield theory subsumes reciprocity laws: (at least ... *abelian* ones). This includes

Quadratic reciprocity over $\mathbb{Q}$ (Gauss, 1800) and over arbitrary number fields and function fields (Takagi, Artin, 1928, Iwasawa-Tate 1950, Weil 1964)

Equivalently, the zeta function of a quadratic extension of $\mathbb{Q}$ is the product of zeta of $\mathbb{Q}$ with a quadratic-character L-function.

Cubic and biquadratic reciprocity (Gauss, Jacobi, Eisenstein: 1820-44)

Factorization of zeta-functions of cyclotomic fields as products of Dirichlet L-functions over $\mathbb{Q}$ (Dirichlet, 1837).

Factorization of zeta-functions of abelian extensions of $\mathbb{Q}$ as products of Dirichlet L-functions over $\mathbb{Q}$.

One further aspect of classfield theory: One original technical motivation of further extensions of a given number field was to try to make non-principal ideals become principal.

The **Hauptidealsatz** (*Principal ideal theorem*) is the assertion that all ideals in $\mathfrak{o}_k$ become principal in the abelian extension of k corresponding to the *absolute* ideal class group. (Conjectured by Hilbert about 1897, proven by Furtwangler 1930). Examples had been known to Kummer and Kronecker.

The abelian extension corresponding to the absolute ideal class group is the *Hilbert classfield*, and is the *maximal unramified* abelian extension of the base: as part of global classfield theory, the only possible ramification is at primes dividing the conductor, for the absolute ideal class group just 1.

Golod and Shafarevich 1964 showed that there exist *infinite classfield towers*, meaning that it is futile to go to larger-and-larger fields hoping to find a PID.

Another technical aspect: norms in cyclic extensions A key point in (every version of) *proof* of global classfield theory is **Cyclic local-global principle for norms:** In a *cyclic* extension K/k of number fields, an element of k is a *global norm* if and only if it is a *local norm everywhere*. For $\alpha \in k$,

$$\alpha \in N_k^K(K^\times) \iff \alpha \in N_{k_v}^{K_w}(K_w^\times) \text{ for all } v, w$$

The most intelligible proof of *this* is probably Weil's 1967 rewrite of Noether's pre-1940 ideas, encapsulating some cohomological ideas in structure of semi-simple algebras, using *zeta functions* of simple algebras. The Artin-Tate notes from 1952 are more overtly cohomological.

To approach classfield theory, it is useful to progress from simple situations to complicated: *finite* fields, *local* fields, *number* fields.

Indeed, the simplest part of the Galois theory of local fields is described by the Galois theory of their residue fields. The same is true of number fields.

As a diagnostic, if we can't understand finite extensions of *finite* fields, most likely we'll not understand finite extensions of *local* fields and *number* fields.

Further, as below, all finite finite-field extensions are generated by *roots of unity*. Thus, extensions of local fields and number fields generated by roots of unity (*cyclotomic* extensions) are the first and canonical examples of abelian extensions. Extensions $k(\sqrt[n]{a})$ for k containing n^{th} roots of unity (*Kummer extensions*) are next.

In fact, over $\mathbb{Q}$ itself, classfield theory is provably the study of cyclotomic extensions (*Kronecker-Weber theorem*).

[39.2] Extensions of finite fields

Recall the classification of finite algebraic field extensions of $\mathbb{F}_p$:

[39.3] Claim: inside a fixed algebraic closure $\overline{\mathbb{F}}$ of $\mathbb{F}_p$, for each integer n there is a unique field extension K of degree n over $\mathbb{F}_p$. It is the collection of roots of $x^{p^n} - x = 0$ in the fixed algebraic closure.

Proof: On one hand, a finite multiplicative subgroup of a field is *cyclic*, else there'd be too many roots of unity of some order. A field extension of $\mathbb{F}_p$ of degree n is an n-dimensional $\mathbb{F}_p$-vectorspace, so has p^n elements. The non-zero elements form a cyclic group of order $p^n - 1$. These, together with 0, are roots of $x^{p^n} - x = 0$.

On the other hand, inside the algebraic closure there is a splitting field of $x^{p^n} - x$. ///

[39.4] Remark: The same proof works over arbitrary finite fields.

[39.5] Claim: The Galois group of $\mathbb{F}_{p^n}/\mathbb{F}_p$ is *cyclic*, generated by the Frobenius element $\alpha \to \alpha^p$.

Proof: The Frobenius element stabilizes $\mathbb{F}_{p^n}$, since $\alpha^{p^n} = \alpha$ implies

$$(\alpha^p)^{p^n} = \alpha^{p^{n+1}} = (\alpha^{p^n})^p = \alpha^p$$

On the other hand, the fixed points of the Frobenius in $\mathbb{F}_{p^n}$ are roots of $x^p - x = 0$, giving exactly $\mathbb{F}_p$. Similarly, the action of Frobenius on $\mathbb{F}_{p^n}$ really is of order n. Thus, by Galois theory, the Galois group of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$ is *cyclic* order n generated by Frobenius. ///

[39.6] Remark: The same proof works over arbitrary finite fields.

[39.7] Claim: The Galois norm $N : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is *surjective:*

Proof: The norm is

$$N\alpha \;=\; \alpha \cdot \alpha^p \cdot \ldots \cdot \alpha^{p^{n-1}} \;=\; \alpha^{1+p+p^2+\ldots+p^{n-1}} \;=\; \alpha^{\frac{p^n-1}{p-1}}$$

Note that the exponent divides $p^n - 1$. In a finite cyclic group of order ℓ, for every divisor k of ℓ, the map $g \to g^k$ surjects to the unique subgroup of order ℓ/k. Here, the Galois norm surjects to $\mathbb{F}_p^\times$. ///

[39.8] Remark: A similar result holds for extensions of arbitrary finite fields.

[39.9] Claim: The Galois trace tr $: \mathbb{F}_{p^n} \to \mathbb{F}_p$ is *surjective:*

Proof: The trace is

$$\mathrm{tr}\,\alpha \;=\; \alpha + \alpha^p + \ldots + \alpha^{p^{n-1}}$$

This is a linear combination (all coefficients 1) of field homomorphisms $\mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$. The desired assertion is a very special case of a sort of result already seen:

Linear independence of characters: Let $\chi_j : k \to \Omega$ be distinct field maps. For $c_j \in \Omega$, $\sum_j c_j\chi_j = 0$ as a map $k \to \Omega$ only for c_j all 0.

Proof: Let $\sum_j c_j\chi_j = 0$ be a shortest non-trivial relation, renumbering as convenient. Divide through by c_1, so

$$\chi_1 + c_2\chi_2 + \ldots \;=\; 0 \qquad\qquad (\text{with } c_2 \neq 0)$$

Let $0 \neq x \in k$ such that $\chi_1(x) \neq \chi_2(x)$. Then

$$0 \;=\; \chi_1(xy) + c_2\chi_2(xy) + \ldots \;=\; \chi_1(x) \cdot \Big(\chi_1(y) + c_2\frac{\chi_2(x)}{\chi_1(x)}\chi_2(y) + \ldots\Big)$$

Dividing by $\chi_1(x)$ and subtracting gives a shorter relation, contradiction. ///

Returning to the proof of the claim: the Galois maps of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$ are linearly independent, are $\mathbb{F}_p$-linear, so trace is a *not-identically-zero* $\mathbb{F}_p$-linear map $\mathbb{F}_{p^n} \to \mathbb{F}_p$. Since $\mathbb{F}_p$ is one-dimensional over itself, this is surjective. ///

[39.10] Remark: A similar result holds for extensions of arbitrary finite fields, in fact, of finite separable extensions.

[39.11] Unramified extensions of $\mathbb{Q}_p$ Inside a fixed algebraic closure of $\mathbb{Q}_p$, for each positive integer n there is a unique *unramified* extension k of $\mathbb{Q}_p$ of degree n over $\mathbb{Q}_p$. It is generated by a primitive $p^n - 1$ root of unity.

Proof: Recall that the local ramification degree e and residue class field extension degree f satisfy $ef = n$. The unramified-ness is $e = 1$, so $f = n$. There is a primitive $p^n - 1$ root of unity in $\mathbb{F}_{p^n}$.

Let Φ be the $(p^n - 1)^{th}$ cyclotomic polynomial. It has no repeated roots mod p. We do not claim that Φ is irreducible over $\mathbb{Q}_p$. (It probably isn't.) Let $\zeta_1 \in \mathfrak{o}_k$ reduce to a primitive $p^n - 1$ root mod p, so $\Phi(\zeta_1) = 0 \bmod p$ and $\Phi'(\zeta_1) \neq 0 \bmod p$. Hensel. ///

[39.12] Remark: The same proof works over arbitrary local fields.

Frobenius elements in Galois groups over $\mathbb{Q}_p$ In $k/\mathbb{Q}_p$, unramified or ramified, there is certainly a unique prime $\mathfrak{p}$ over p. Thus, the *decomposition group* $G_\mathfrak{p} = \{g \in \mathrm{Gal}(k/\mathbb{Q}_p) : g\mathfrak{p} = \mathfrak{p}\}$ is the whole Galois group $\mathrm{Gal}(k/\mathbb{Q}_p)$. Recall that $G_\mathfrak{p}$ *surjects* to the residue field Galois group, which is cyclic order n, generated by Frobenius.

In general, the kernel of the map of $G_\mathfrak{p}$ to the residue field Galois group is the inertia subgroup. Here, there cannot be a non-trivial kernel, since the residue field extension degree is equal to that of the local field extension degree.

Thus, $\mathrm{Gal}(k/\mathbb{Q}_p) = G_\mathfrak{p}$ is cyclic order n, with canonical generator also called *Frobenius*, characterized by reducing mod p to the finite-field Frobenius.

[39.13] Remark: The same proof works for unramified extensions of arbitrary local fields.

[39.14] Claim: The Galois norm $N : k \to \mathbb{Q}_p$ gives a *surjection* $\mathfrak{o}_k^\times \to \mathbb{Z}_p^\times$.

Proof: Surjectivity of finite-field norm and trace, and completeness. Frobenius $\varphi \in \mathrm{Gal}(k/\mathbb{Q}_p)$ satisfies $\varphi(\alpha) = \alpha^p \bmod p\mathfrak{o}$, so, mod $p\mathfrak{o}$

$$N\alpha \;=\; \alpha\,\alpha^p \ldots \alpha^{p^{n-1}} \;=\; \alpha^{1+p+p^2+\ldots+p^{n-1}} \;=\; \alpha^{\frac{p^n-1}{p-1}} \qquad (\mathrm{mod}\; p\mathfrak{o})$$

This reduces the question to proving surjectivity to $1+p\mathbb{Z}_p$. By surjectivity of trace on finite fields, $\mathrm{tr}^k_{\mathbb{Q}_p}\mathfrak{o}_k = \mathbb{Z}_p$. Thus, given $1+p\alpha$ with $\alpha \in \mathbb{Z}_p$, there is $\beta \in \mathfrak{o}$ with $\mathrm{tr}(\beta) = \alpha$. Thus, $N(1+p\beta) = 1+p\alpha \bmod p^2$. This reduces the question to proving surjectivity to $1+p^2\mathbb{Z}_p$. Continuing, using completeness, the sequence of cumulative adjustments converges. ///

[39.15] Remark: The same proof works for unramified extensions of arbitrary local fields.

[39.16] A very special sub-case: *unramified* local classfield theory:

(Mock) Theorem: The unramified extensions k of $\mathbb{Q}_p$ are in bijection with finite-index subgroups of $\mathbb{Q}_p^\times$ containing $\mathbb{Z}_p^\times$, by

$$\text{finite-index subgroup } H \supset \mathbb{Z}_p^\times \quad\longleftrightarrow\quad N^k_{\mathbb{Q}_p}(k^\times)$$

The Galois group is $\mathrm{Gal}(k/\mathbb{Q}_p) \approx \mathbb{Q}_p^\times/N^k_{\mathbb{Q}_p}(k^\times)$, via the map to Artin/Frobenius:

$$\big(\text{Frobenius } x \to x^p\big) \quad\longleftarrow\quad p$$

[39.17] Remark: The analogous result holds for all local fields.

Proof: We have shown that an unramified extension k of $\mathbb{Q}_p$ of degree n is cyclic Galois, obtained by adjoining a primitive $(p^n-1)^{th}$ root of unity ω, and the map from $\mathrm{Gal}(k/\mathbb{Q}_p)$ to the Galois group of residue fields is an isomorphism. Thus, the Frobenius generates $\mathrm{Gal}(k/\mathbb{Q}_p)$, and is order n.

Since the norm $N^k_{\mathbb{Q}_p}$ is surjective $\mathfrak{o}_k^\times \to \mathbb{Z}_p^\times$, $N^k_{\mathbb{Q}_p}(k^\times)$ is *open*. Also, $N^k_{\mathbb{Q}_p}(p) = p^n$. Thus, $\mathbb{Q}_p^\times/N^k_{\mathbb{Q}_p}(k^\times) \approx p^{\mathbb{Z}}/p^{n\mathbb{Z}}$, which gives the Galois group, by the map to Frobenius.

On the other hand, for $H \supset \mathbb{Z}_p^\times$ of finite index n, since $\mathbb{Q}_p^\times/\mathbb{Z}_p^\times \approx p^{\mathbb{Z}}$, necessarily $H = p^{n\mathbb{Z}} \cdot \mathbb{Z}_p^\times$. Adjoining a primitive $(p^n-1)^{th}$ root of unity produces an unramified degree n extension k such that $N^k_{\mathbb{Q}_p}(k^\times) = H$. ///

[39.18] Remark: This formulation of the classification of unramified extensions of local fields is not terribly useful, but illustrates the type of formulation *necessary* for more general abelian extensions, in local classfield theory.

[39.19] Another special case: quadratic extensions of $\mathbb{Q}_p$, $p \neq 2$:

(Mock) Theorem: Let $p > 2$. The quadratic extensions K of $\mathbb{Q}_p$ are in bijection with the subgroups H of index 2 in $\mathbb{Q}_p^\times$, by

$$K \longleftrightarrow \mathbb{Q}_p^\times / N^K_{\mathbb{Q}_p}(K^\times)$$

The extension $K/\mathbb{Q}_p$ is unramified if and only if $N^K_{\mathbb{Q}_p}(K^\times) \supset \mathbb{Z}_p^\times$.

[39.20] Remark: Since every field contains ± 1, and ± 1 are *distinct* in characteristic not 2, the theory of quadratic extensions is a special case of *Kummer theory*, which more generally discusses cyclic extensions of order n over ground fields of characteristic not dividing n and containing n^{th} roots of unity.

Proof: The unramified quadratic case is included in the general discussion of unramified extensions, of course. But the immediate issue is to understand the Kummer-theory quotient $k^\times/(k^\times)^2$.

Recall that the exponential map $x \to e^x = \sum_{n=0}^\infty \frac{x^n}{n!}$ converges p-adically for $\mathrm{ord}_p x > \frac{1}{p-1}$, since

$$\mathrm{ord}_p\, n! \;<\; \frac{n}{p} + \frac{n}{p^2} + \ldots \;=\; \frac{n/p}{1-\frac{1}{p}} \;=\; n \cdot \frac{1}{p-1}$$

This also applies to ord_p and/or $|\cdot|_p$ *extended* to field extensions K of $\mathbb{Q}_p$. Not *composed* with Galois norm, but, rather, *extended*. Similarly, $-\log(1-x) = \sum_{n\geq 1} \frac{x^n}{n}$ converges for $\mathrm{ord}_p x > 0$, since

$$\mathrm{ord}_p\, n \;\leq\; \log_p\, n \;\ll_\varepsilon\; n^\varepsilon \qquad\qquad (\text{for all } \varepsilon > 0)$$

The immediate point of considering these functions is to give the isomorphism of the subgroup of units $1 + p\mathbb{Z}_p \subset \mathbb{Z}_p^\times$ to $p\mathbb{Z}_p$. In particular, *everything* in $1 + p\mathbb{Z}_p$ is a *square* for $p > 2$, since $2 \in \mathbb{Z}_p^\times$.

(This, or some equivalent, is the most technical part of this discussion.) Next, to understand squares in $\mathbb{Z}_p^\times$, consider

$$1 \longrightarrow 1 + p\mathbb{Z}_p^\times \longrightarrow \mathbb{Z}_p^\times \longrightarrow (\mathbb{Z}/p)^\times \longrightarrow 1$$

Since everything in $1 + p\mathbb{Z}_p$ is a square, an element of $\mathbb{Z}_p^\times$ is a square if and only if its image in $(\mathbb{Z}/p)^\times$ is a square. The latter group is cyclic of order $p-1$, so the squares are of index 2.

To understand squares in $\mathbb{Q}_p^\times$, choice of the usual local parameter p gives a splitting $\mathbb{Q}_p^\times \approx \mathbb{Z}_p^\times \times p^{\mathbb{Z}}$, and

$$\begin{tikzcd}
1 \arrow[r] & (\mathbb{Z}_p^\times)^2 \times (p^2)^{\mathbb{Z}} \arrow[r] \arrow[d, equal] & \mathbb{Z}_p^\times \times p^{\mathbb{Z}} \arrow[r] \arrow[d, equal] & \{1,\varepsilon\} \times \{1,p\} \arrow[r] & 1 \\
& (\mathbb{Q}_p^\times)^2 & \mathbb{Q}_p^\times & &
\end{tikzcd}$$

where ε is a non-square unit (modulo squares of units). Thus, $\mathbb{Q}_p^\times$ modulo squares is a $2,2$ group, with representatives $1, \varepsilon, p, \varepsilon p$. Since $\mathbb{Q}_p(\sqrt{p})$ and $\mathbb{Q}_p(\sqrt{\varepsilon p})$ are visibly ramified: the square root is a uniformizer in the extension, and has $\mathrm{ord}_p = \frac{1}{2}$. Equally visibly, $\mathbb{Q}_p(\sqrt{\varepsilon})$ is the unique unramified quadratic extension. (This all uses $p > 2$!)

To make this a special case of local classfield theory, examine the norms from each of the three quadratic extensions for $p > 2$.

In the unramified extension, local units are norms, and the norm of $p^{\mathbb{Z}}$ hits $p^{2\mathbb{Z}}$, so the norm index is 2, and p is not a norm.

For the ramified quadratic extensions K, the norm is

$$N(a + b\sqrt{\varepsilon p}) \;=\; a^2 - \varepsilon p b^2$$

Certainly $-\varepsilon p$ is a norm, and is a local parameter, so $\mathbb{Q}_p^\times/N(K^\times)$ has representatives among *units*. From the norm expression, unit norms are squares mod p. Thus, the index is *at least* 2.

Thus, it suffices to show that $1+p\mathbb{Z}_p$ is hit by norms. Since $N(1+px)=(1+px)^2$ for $x\in\mathbb{Q}_p$, and $1+p\mathbb{Z}_p$ consists entirely of squares for $p>2$, the index inside the units is *exactly* 2 for ramified quadratic extensions. ///

[39.21] General Kummer theory: Recall that cyclic extensions K of degree dividing n of a field k of characteristic not dividing n and containing n^{th} roots of unity are in bijection with cyclic subgroups of $k^\times/(k^\times)^n$, by $K=k(\sqrt[n]{\alpha})\longleftrightarrow\langle\alpha\rangle \bmod (k^\times)^n$.

Proof: On one hand, certainly $k(\sqrt[n]{\alpha})=k(\sqrt[n]{\alpha\beta^n})$.

In one direction, in $K=k(\sqrt[n]{a})$, any $g\in\mathrm{Gal}(K/k)$ sends $\alpha=\sqrt[n]{a}$ to another n^{th} root of a, which is $\omega_g\cdot\alpha$ for some n^{th} root of unity ω_g. The map $g\to\omega_g$ is a group homomorphism, and is injective because the effect of g is determined by its effect on α, so G is cyclic of order dividing n.

On another hand, let G be the Galois group of cyclic K over k. Since k contains n^{th} roots of unity, the commuting k-linear endomorphisms of K given by G are *simultaneously diagonalizable.* Since this assertion is central to this proof of the theorem of Kummer theory, we give details.

To get an idea how to proceed, observe that the minimal polynomial $P(x)=\prod_\zeta(x-\zeta)$ of a generator g of G has roots n^{th} roots of unity. For each root ζ, with $Q_\zeta(x)=P(x)/(x-\zeta)$, $Q_\zeta(g)$ is not the 0 endomorphism of K, so there is $\alpha\in K$ such that $Q_\zeta(g)(\alpha)\neq 0$. Nevertheless, $(g-\zeta)Q_\zeta(g)(\alpha)=P(g)(\alpha)=0$. Thus, $Q_\zeta(g)(\alpha)$ is a (non-zero) ζ-eigenvector for g.

Since $g^n=1$, the minimal polynomial of g divides x^n-1, which has no repeated roots when the characteristic does not divide n. Thus, g is *diagonalizable*, meaning that K is the direct sum of g's eigenspaces. Indeed, as ζ runs over roots of $P(x)=0$, the quotients $Q_\zeta(x)=P(x)/(x-\zeta)$ have collective common factor 1. Thus, there are monic $R_\zeta(x)\in k[x]$ such that

$$1 \;=\; \sum_\zeta R_\zeta(x)\cdot Q_\zeta(x) \qquad\text{and}\qquad 1\;=\;\sum_\zeta R_\zeta(g)\cdot Q_\zeta(g)$$

Thus, $K=\bigoplus_\zeta\Big(R_\zeta(g)\cdot Q_\zeta(g)\Big)(K)$ and the ζ^{th} summand $\big(R_\zeta(g)\cdot Q_\zeta(g)\big)(K)$ is the ζ-eigenspace, proving diagonalizability.

For g of order exactly m, with $m|n$, let ζ be a primitive m^{th} root of unity, and $v\in K$ a ζ-eigenvector. Then $g(v^m)=(gv)^m=(\zeta v)^m=v^m$, so v^m is in k, while v itself is fixed by no proper subgroup of G. By Galois theory $K=k(\sqrt[m]{v^m})=k(\sqrt[n]{v^n})$. ///

[39.22] Remark: The example of Kummer theory is continued in the following section.

40. *Classfield Theory: semi-modern preview, examples*

[40.1] Theorem: *(Main theorem of global classfield theory)* The Galois groups of finite abelian extensions K of a number field k are the finite quotients of the idele class group $\mathbb{J}_k/k^\times$, namely

$$(\mathbb{J}_k/k^\times)/N_k^K(\mathbb{J}_K/K^\times) \quad \longleftrightarrow \quad K/k$$

The maps of quotients of idele class groups to Galois groups are *natural*, in the sense that, for finite abelian extensions $L \supset K \supset k$ there is a commutative diagram

$$\begin{tikzcd}
\mathbb{J}_k/k^\times)/N_k^L(\mathbb{J}_L/L^\times) \arrow[r, "\alpha_{L/k}"] \arrow[d, "\text{quot}"'] & \mathrm{Gal}(L/k) \arrow[d, "\text{quot}"] \\
\mathbb{J}_k/k^\times)/N_k^K(\mathbb{J}_K/K^\times) \arrow[r, "\alpha_{K/k}"'] & \mathrm{Gal}(K/k)
\end{tikzcd}$$

The maps $\alpha_{*/k}$ are **Artin maps** or **reciprocity law maps**

[40.2] Theorem: *(Main Theorem of Local Classfield Theory)* The Galois groups of finite abelian extensions K of a *local* field k are the quotients

$$k^\times/N_k^K(K^\times) \quad \longleftrightarrow \quad K/k$$

The maps to Galois groups are *natural*, in the sense that, for finite abelian extensions $L \supset K \supset k$ there is a commutative diagram

$$\begin{tikzcd}
k^\times/N_k^L(L^\times) \arrow[r, "\alpha_{L/k}"] \arrow[d, "\text{quot}"'] & \mathrm{Gal}(L/k) \arrow[d, "\text{quot}"] \\
k^\times/N_k^K(K^\times) \arrow[r, "\alpha_{K/k}"'] & \mathrm{Gal}(K/k)
\end{tikzcd}$$

The maps $\alpha_{*/k}$ are **local Artin** or **local reciprocity law** maps.

[40.3] Remark: We'd want a precise connection between local and global, too.

Note that the adelic rewrite of global classfield theory shows the connection to *norms*.

In *cyclic* extensions, the connection between global and local norms is clear:

[40.4] Theorem: *(Cyclic local-global principle for norms)* In a *cyclic* extension K/k of number fields, an element of k is a *global norm* if and only if it is a *local norm everywhere*. That is, for $\alpha \in k$,

$$\alpha \in N_k^K(K^\times) \quad \Longleftrightarrow \quad \alpha \in N_{k_v}^{K_w}(K_w^\times) \text{ for all } v, w$$

Proof by analytic properties of *zeta functions of simple algebras*.

Norm index inequalities play a central role in proofs of classfield theory.

For *unramified extensions* $L \supset K \supset k$ of a local field k, we do have the commutative compatibility diagram

$$\begin{tikzcd}
k^\times/N_k^L(L^\times) \arrow[r, "\alpha_{L/k}"] \arrow[d, "\text{quot}"'] & \mathrm{Gal}(L/k) \arrow[d, "\text{quot}"] & & L \arrow[d, dash] \\
k^\times/N_k^K(K^\times) \arrow[r, "\alpha_{K/k}"'] & \mathrm{Gal}(K/k) & \text{for unramified} & K \arrow[d, dash] \\
 & & & k
\end{tikzcd}$$

[40.5] Remark: Again, the maps $\alpha_{K/k}$ are *Artin maps* or *reciprocity law maps.* It is typically not obvious how to recover classical reciprocity laws.

[40.6] More on Kummer theory *Interaction* of the various extensions of k by n^{th} roots: Fix $2 \le \ell \in \mathbb{Z}$, k a field of characteristic not dividing ℓ, containing a primitive ℓ^{th} root of unity. Let $a_1, \ldots, a_n \in k^\times$, and $\alpha_j = \sqrt[\ell]{a_j}$ in a fixed finite Galois extension K of k.

Suppose that, for any pair of indices $i \neq j$, there is $\sigma \in \mathrm{Gal}(K/k)$ such that $\sigma(\alpha_i)/\alpha_i \neq \sigma(\alpha_j)/\alpha_j$.

[40.7] Remark: Since $\sigma(\alpha_i) = \omega_i \cdot \alpha_i$ for some ℓ^{th} root of unity ω_i (depending on σ), the hypothesis is equivalent to a_i/a_j *not* being an n^{th} power in k.

That is, the hypothesis is that the one-dimensional representations of $\mathrm{Gal}(K/k)$ on the lines $k \cdot \alpha_j$ are pairwise non-isomorphic. This description of the situation correctly suggests the proof of the following proposition.

[40.8] Remark: Historical and bibliographic pointers for the following proposition were gleaned from [Dubuque 2011], e.g., [Bergstrom 1953]'s reference to [Hasse 1933]. [Robinson 2011] proves the quadratic case, and suggests extensions. Unsurprisingly, such questions were addressed decades ago.

[40.9] Proposition: The α_j's are *linearly independent* over k.

Proof: Let $\sum_j c_j \cdot \alpha_j = 0$ be a shortest non-trivial linear relation with $c_j \in k$. For indices $i \neq j$ appearing in this relation, take $\sigma \in \mathrm{Gal}(K/k)$ such that $\sigma(\alpha_i)/\alpha_i \neq \sigma(\alpha_j)/\alpha_j$. Then

$$0 \;=\; \frac{\sigma(\alpha_i)}{\alpha_i} \cdot 0 - \sigma(0) \;=\; \frac{\sigma(\alpha_i)}{\alpha_i} \sum_t c_t \cdot \alpha_t - \sigma\Big(\sum_t c_t \cdot \alpha_t\Big)$$

$$= \sum_t c_t \cdot \alpha_t \cdot \big(\frac{\sigma(\alpha_i)}{\alpha_i} - \frac{\sigma(\alpha_t)}{\alpha_t}\big)$$

The coefficient of α_i is 0, while the coefficient of α_j is non-zero, by arrangement. This would contradict the assumption that the relation is shortest. Thus, there is no non-trivial relation. ///

[40.10] Remark: The argument reproves the impossibility of mapping a sum of mutually non-isomorphic irreducibles of $\mathrm{Gal}(K/k)$ non-trivially to the trivial representation. The argument resembles the argument for *linear independence of characters.*

[40.11] Corollary: For *(pairwise) relatively prime* square-free integers $a_1, \ldots, a_n$, the 2^n algebraic numbers $\sqrt{a_{i_1} \ldots a_{i_k}}$ with $i_1 < \ldots < i_k$ and $0 \le k \le n$ are linearly independent over $\mathbb{Q}$, so are a $\mathbb{Q}$-basis for $\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_n})$. In particular, the degree of that field over $\mathbb{Q}$ is the maximum possible, 2^n.

Proof: The ratios $(a_{i_1} \ldots a_{i_k})/(a_{j_1} \ldots a_{j_\ell})$ have some prime appearing in the numerator or denominator, not both, and to first power, so is not a square, by unique factorization. ///

The following is a *numerical* form of a reciprocity:

[40.12] Corollary: Let k be a field containing n^{th} roots of unity, with characteristic not dividing n. For a subgroup Θ of $k^\times$ containing $(k^\times)^n$ and with $\Theta/(k^\times)^n$ *finite*,

$$[k\Big(n^{th} \text{ roots of } a \in \Theta\Big) : k] \quad = \quad \#\, \Theta/(k^\times)^n$$

Proof: We really adjoin only n^{th} roots of *representatives* for $\Theta/(k^\times)^n$. Let K be the finite abelian extension obtained by adjoining all these roots. Given a, b in Θ but distinct mod $(k^\times)^n$, let $\alpha = \sqrt[n]{a}$ and $\beta = \sqrt[n]{b}$.

Necessarily there is $g \in \mathrm{Gal}(K/k)$ such that $g\alpha/\alpha \neq g\beta/\beta$, or else α/β is fixed by $\mathrm{Gal}(K/k)$, and then $a/b = (\alpha/\beta)^n \in (k^\times)^n$, contradiction.

Thus, by the proposition, the n^{th} roots of representatives are linearly independent over k. This computes the degree of the field extension. ///

For a field k containing n^{th} roots of unity, with characteristic not dividing n, fix a subgroup Θ of $k^\times$ containing $(k^\times)^n$ and with $\Theta/(k^\times)^n$ *finite*. Let

$$K \;=\; k\Big(n^{th} \text{ roots of } \theta \in \Theta/(k^\times)^n\Big)$$

For $\sigma \in \mathrm{Gal}(K/k)$ and $\theta \in \Theta$, for an n^{th} root $\sqrt[n]{\theta}$,

$$\sigma(\sqrt[n]{\theta}\,) \;=\; \omega_\theta(\sigma)\cdot\sqrt[n]{\theta} \qquad\qquad (\text{with } \omega_\theta(\sigma)^n = 1)$$

As for any collection of eigenvalues for a simultaneous eigenvector, $\sigma \to \omega_\theta(\sigma)$ is a *group homomorphism* for each $\sqrt[n]{\theta}$, using the fact that $\sigma, \tau \in \mathrm{Gal}(K/k)$ are k-linear and k contains n^{th} roots of unity:

$$\omega_\theta(\sigma\tau)\cdot\sqrt[n]{\theta} \;=\; (\sigma\tau)(\sqrt[n]{\theta}) \;=\; \sigma\big(\tau(\sqrt[n]{\theta})\big)$$

$$=\; \sigma\Big(\omega_\theta(\tau)\cdot\sqrt[n]{\theta}\Big) \;=\; \omega_\theta(\tau)\cdot\sigma(\sqrt[n]{\theta}) \;=\; \omega_\theta(\tau)\omega_\theta(\sigma)\cdot\sqrt[n]{\theta}$$

Also, $\sigma \times \theta \to \omega_\theta(\sigma)$ is a group homomorphism in θ: the ambiguity of choice(s) of n^{th} roots has no impact: with $\sqrt[n]{\theta\theta'} = \omega\cdot\sqrt[n]{\theta}\cdot\sqrt[n]{\theta'}$ for whatever n^{th} root of unity ω,

$$\omega_{\theta\theta'}(\sigma)\cdot\sqrt[n]{\theta\theta'} \;=\; \sigma(\sqrt[n]{\theta\theta'}) \;=\; \sigma(\omega\cdot\sqrt[n]{\theta}\cdot\sqrt[n]{\theta'})$$

$$=\; \omega\cdot\sigma(\sqrt[n]{\theta})\cdot\sigma(\sqrt[n]{\theta'}) \;=\; \omega\cdot\omega_\theta(\sigma)\cdot\sqrt[n]{\theta}\cdot\omega_{\theta'}(\sigma)\cdot\sqrt[n]{\theta'}$$

$$=\; \omega_\theta(\sigma)\omega_{\theta'}(\sigma)\big(\omega\cdot\sqrt[n]{\theta}\cdot\sqrt[n]{\theta'}\big) \;=\; \omega_\theta(\sigma)\omega_{\theta'}(\sigma)\,\sqrt[n]{\theta\theta'}$$

Certainly $(k^\times)^n$ maps to 1. Thus, we have

[40.13] Theorem: There is a canonical group homomorphism

$$\mathrm{Gal}(K/k) \;\times\; \Theta/(k^\times)^n \;\longrightarrow\; (n^{th} \text{ roots of unity})$$

and both groups are abelian, torsion of exponent dividing n. This gives a *duality* between the Galois group and $\Theta/(k^\times)^n$, rather than an *isomorphism.* ///

[40.14] Remark: Yes, a finite abelian group A is *non-canonically* isomorphic to its dual

$$A^\vee \;=\; \mathrm{Hom}_{\mathbb{Z}}(A,\, \mathbb{Q}/\mathbb{Z})$$

The popular identification

$$\mathbb{Q}/\mathbb{Z} \;\approx\; \{\text{roots of unity}\} \qquad \text{by} \qquad t \;\to\; e^{2\pi i t} \in \mathbb{C}^\times$$

is *not* canonical, and is not relevant to consideration of abstract fields k, because it depends on complex numbers to distinguish roots of unity.

In fact, in abstract Kummer theory, it is reasonable to obtain a duality rather than an isomorphism, because in this abstraction we have no device producing a map from $k^\times$ to the Galois group.

In contrast, for example, a choice of *generator* γ for a cyclic group of order n gives an isomorphism to its dual, by

$$\gamma^s \quad \longrightarrow \quad (\gamma^t \longrightarrow \frac{st}{n})$$

---

41. *Classfield theory: Hilbert's theorem* 90

In one regard, classfield theory is the discussion of abelian extensions without corresponding roots of unity in the ground-field.

[41.1] Example: global cyclotomic fields Cyclotomic field extensions of $\mathbb{Q}$ provide an elementary example of understandable structure results for abelian Galois extensions of order n without necessarily having any or all n^{th} roots of unity in the base field.

Let $K = \mathbb{Q}(\zeta)$ for ζ a primitive n^{th} root of unity. Grant that the ring of integers $\mathfrak{o}$ is $\mathbb{Z}[\zeta]$.

We know $[K : \mathbb{Q}] = \varphi(n)$ with the Euler totient function $\varphi(p_1^{e_1} \ldots) = (p_1 - 1)p^{e_1 - 1} \ldots$ and the Galois group is isomorphic to $(\mathbb{Z}/n)^\times$, by

$$(\mathbb{Z}/n)^\times \ \ni \ \ell \qquad \longrightarrow \qquad \sigma_\ell : \zeta \to \zeta^\ell$$

For prime p, σ_p *is the* p^{th} *Frobenius/Artin element:* since p divides the inner binomial coefficients $\binom{p}{j}$ with $0 < j < p$, and since $c_i^p = c_i \bmod p$ for $c_i \in \mathbb{Z}$,

$$\sigma_p\big(\sum_i c_i\, \zeta^i\big) \ = \ \sum_i c_i\, \zeta^{ip} \ = \ \Big(\sum_i c_i\, \zeta^i\Big)^p \bmod p\mathfrak{o}$$

$(\mathbb{Z}/n)^\times$ *is* the generalized ideal class group with conductor n.

[41.2] Hilbert's theorem number 90 in [Hilbert 1897] is

[41.3] Theorem: In a field extension K/k of degree n with cyclic Galois group generated by σ, the elements in K of norm 1 are exactly those of the form $\sigma\alpha/\alpha$ for $\alpha \in K$.

Proof: On one hand, for *any* finite Galois extension K/k, for $\sigma \in \mathrm{Gal}(K/k)$ and $\alpha \in K$,

$$N_k^K\big(\frac{\sigma\alpha}{\alpha}\big) \ = \ \prod_{\tau \in \mathrm{Gal}(K/k)} \tau\big(\frac{\sigma\alpha}{\alpha}\big) \ = \ \frac{\prod_\tau \tau\sigma\alpha}{\prod_\tau \tau\alpha} \ = \ \frac{\prod_\tau \tau\alpha}{\prod_\tau \tau\alpha} \ = \ 1$$

by changing variables in the numerator. This is the easy direction. The other direction uses the cyclic-ness. Let $\beta \in K$ with $N_k^K(\beta) = 1$. *Linear independence of characters* implies that the map $\varphi : K \to K$ by $\varphi = 1_K + \beta\sigma + \beta\beta^\sigma\sigma^2 + \ldots + \beta^{1+\sigma+\ldots+\sigma^{n-2}}\sigma^{n-1}$ is not identically 0. The not-identical-vanishing assures that there is $\gamma \in K$ such that

$$0 \ \neq \ \alpha \ = \ \varphi(\gamma) \ = \ \gamma + \beta\gamma^\sigma + \beta\beta^\sigma\gamma^{\sigma^2} + \ldots + \beta^{1+\sigma+\ldots+\sigma^{n-2}}\gamma^{\sigma^{n-1}}$$

Then $\beta\alpha^\sigma = \alpha$, and $\beta = \alpha/\sigma\alpha$. ///

Hilbert' Theorem 90 gives another proof of

[41.4] Corollary: A cyclic degree n extension K/k of k containing n^{th} roots of unity is obtained by adjoining an n^{th} root.

Proof: For primitive n^{th} root of unity ζ, since $N_k^K(\zeta) = \zeta^n = 1$, by Hilbert's Theorem 90 there is $\alpha \in K$ such that $\zeta = \sigma\alpha/\alpha$. That is, $\sigma\alpha = \zeta \cdot \alpha$ and $\sigma(\alpha^n) = \alpha^n$, so $\alpha^n \in k$. ///

Additive version of Theorem 90: Let K/k be cyclic of degree n with Galois group generated by σ. Then $\mathrm{tr}_k^K(\beta) = 0$ if and only if there is $\alpha \in K$ such that $\beta = \alpha - \alpha^\sigma$.

Proof: The traces of elements $\alpha - \sigma\alpha$ are easily 0, again. *Linear independence of characters* shows that trace is not identically 0, so there is γ with non-zero trace. With

$$\alpha \;=\; \frac{1}{\mathrm{tr}_k^K(\gamma)}\Big(\beta\gamma^\sigma + (\beta+\beta^\sigma)\gamma^{\sigma^2} + \ldots + (\beta+\beta^\sigma+\ldots+\beta^{\sigma^{n-2}})\gamma^{\sigma^{n-1}}\Big)$$

we have $\beta = \alpha - \alpha^\sigma$. ///

[41.5] Corollary: *(Artin-Schreier extensions)* Let K/k be cyclic of order p in characteristic p. Then there is $K = k(\alpha)$ with α satisfying an equation $x^p - x + a = 0$ with $a \in k$.

Proof: Since $\mathrm{tr}_k^K(-1) = p\cdot(-1) = -p = 0$, by additive Theorem 90 there is α such that $\alpha - \alpha^\sigma = -1$, which is $\alpha^\sigma = \alpha + 1$... ///

42. *Classfield theory: connecting local and global*

For $\mathfrak{p}$ in $\mathfrak{o}_k$ and $\mathfrak{P}|\mathfrak{p}$ in $\mathfrak{o}_K$ unramified in an abelian extension K/k of number fields, the inertia subgroup of the decomposition group $G_\mathfrak{p} \subset \mathrm{Gal}(K/k)$ is trivial, $G_\mathfrak{p}$ is generated by the Artin element $(\mathfrak{p}, K/k)$.

The corresponding unramified extension of completions K_w/k_v is *cyclic* with Galois group generated by the local Artin element $(\mathfrak{m}_v, K_w/k_v)$ with $\mathfrak{m}_v$ the unique non-zero prime in $\mathfrak{o}_v$. The local Artin/reciprocity map $\alpha_{w/v} : k_v^\times \to \mathrm{Gal}(K_w/k_v)$ is

$$\alpha_{w/v}(x) \;=\; (\mathfrak{m}_v, K_w/k_v)^{\mathrm{ord}_v x} \qquad\qquad (\text{unramified } K_w/k_v)$$

Identifying the two cyclic groups $\mathrm{Gal}(K_w/k_v) \approx G_\mathfrak{p}$ by identifying their corresponding Artin elements $(\mathfrak{m}_v, K_w/k_v) \longleftrightarrow (\mathfrak{p}, K/k)$, we can consider the local Artin map as mapping to $G_\mathfrak{p}$, and

$$\alpha_{w/v} \;:\; k_v^\times \;\longrightarrow\; \mathrm{Gal}(K_w/k_v) \;\approx\; G_\mathfrak{p} \;\subset\; \mathrm{Gal}(K/k)$$

With the identification $\mathrm{Gal}(K_w/k_v) \approx G_\mathfrak{p} \subset \mathrm{Gal}(K/k)$ at unramified places, define the *global* Artin/reciprocity map $\alpha_{K/k} : \mathbb{J} \longrightarrow \mathrm{Gal}(K/k)$ by

$$\alpha_{K/k}(x) \;=\; \prod_v \prod_{w|v} \alpha_{w/v}(x_v) \qquad\qquad (\text{for } x = \{x_v\} \in \mathbb{J}_k)$$

For the moment, we seem not to know how to define local Artin/reciprocity maps at *ramified* primes.

[42.1] Remark: Local norms at unramified K_w/k_v are *surjective* to local units, so the product is *finite.*

[42.2] Remark: The *critical* part of the assertion of global classfield theory is that the global $\alpha_{K/k}$ *factors through* the idele class group $\mathbb{J}_k/k^\times$.

It is a *local* fact that $\alpha_{w/v} : k_v^\times \to \mathrm{Gal}(K_w/k_v)$ factors through $k_v^\times/N_{k_v}^{K_w} K_w^\times$ and gives an *isomorphism* $\alpha_{w/v} : k_v^\times/N_{k_v}^{K_w} K_w^\times \to \mathrm{Gal}(K_w/k_v)$. Thus, $\alpha_{K/k}$ factors similarly. And $\alpha_{K/k} : \mathbb{J}_k/k^\times N_k^K \mathbb{J}_K \longrightarrow \mathrm{Gal}(K/k)$ is an *isomorphism.*

[42.3] Significance of factoring through $\mathbb{J}/k^\times$ and $\mathbb{J}/k^\times N_k^K \mathbb{J}_K$ Since norms in unramified extensions of non-archimedean fields are *surjective* to local units, and norms on archimedean fields are open maps, the image $N_k^K \mathbb{J}_K$ is *open* in $\mathbb{J}_k$. Thus, the local and global Artin maps are *continuous.*

The latter open-ness/continuity reformulates *part* of the classical assertion that the Artin map *has a conductor*. The difficult part is $k^\times$-invariance.

By Fujisaki's Lemma, since the norms at archimedean places include *the ray* $\{(t^{1/N},\ldots,t^{1/N},1,1,\ldots) : t>0\}$ with $N = r_1+r_2$, the quotient $\mathbb{J}_k/k^\times N_k^K \mathbb{J}_K$ is *finite*, in any case.

Recall how factoring of the quadratic *norm residue* symbol through $\mathbb{J}_k/k^\times$ proves reciprocity for the quadratic Hilbert symbol, and then more classical forms of quadratic reciprocity: for global field k with *completions* k_v of k, for K a *quadratic* extension of k, put

$$K_v \;=\; K\otimes_k k_v$$

The *local norm residue symbol* $\nu_v : k_v^\times \to \{\pm 1\}$ is

$$\nu_v(\alpha) \;=\; \begin{cases} +1 & (\text{for } \alpha\in N(K_v^\times)) \\ \\ -1 & (\text{for } \alpha\notin N(K_v^\times)) \end{cases}$$

For $k_v = \mathbb{Q}_p$ with odd p, we have proven the small *local*

[42.4] Theorem:

$$[k_v^\times : N(K_v^\times)] \;=\; \begin{cases} 2 & (\text{when } K_v \text{ is a field}) \\ \\ 1 & (\text{when } K_v\approx k_v\times k_v) \end{cases}$$

[42.5] Corollary: ν_v is a group homomorphism $k_v^\times \to \{\pm 1\}$. ///

We grant ourselves

[42.6] Theorem: the quadratic norm-residue map ν is $k^\times$-invariant: it *factors through* $\mathbb{J}/k^\times$.

We recall how this form of a *reciprocity law* entails more classical-looking reciprocity laws:

Quadratic Hilbert symbols: For $a,b\in k_v$ the (quadratic) Hilbert symbol is

$$(a,b)_v \;=\; \begin{cases} 1 & (\text{if } ax^2+by^2=z^2 \text{ has non-trivial solution in } k_v) \\ \\ -1 & (\text{otherwise}) \end{cases}$$

[42.7] Corollary: For $a,b\in k^\times$, $\Pi_v\;(a,b)_v \;=\; 1$.

Proof: For b a non-square in $k^\times$, $(a,b)_v$ is $\nu_v(a)$ for the field extension $k(\sqrt{b})$, and reciprocity for the norm residue symbol gives the result for the Hilbert symbol. ///

Next, traditional-looking quadratic reciprocity laws follow from reciprocity for the quadratic Hilbert symbol. Define

$$\Big(\frac{x}{v}\Big)_2 \;=\; \begin{cases} 1 & (\text{for } x \text{ a non-zero square mod } v) \\ \\ 0 & (\text{for } x = 0 \bmod v) \\ \\ -1 & (\text{for } x \text{ a non-square mod } v) \end{cases}$$

Quadratic Reciprocity ('main part'): For π and ϖ two elements of $\mathfrak{o}$ generating distinct odd prime ideals,

$$\Big(\frac{\varpi}{\pi}\Big)_2 \Big(\frac{\pi}{\varpi}\Big)_2 \;=\; \Pi_v\,(\pi,\varpi)_v$$

where v runs over all *even or infinite* primes, and $(,)_v$ is the (quadratic) Hilbert symbol.

Proof: Claim that, since $\pi\mathfrak{o}$ and $\varpi\mathfrak{o}$ are odd primes,

$$(\pi,\varpi)_v \;=\; \begin{cases} \left(\frac{\varpi}{\pi}\right)_2 & \text{for } v = \pi\mathfrak{o} \\ \left(\frac{\pi}{\varpi}\right)_2 & \text{for } v = \varpi\mathfrak{o} \\ 1 & \text{for } v \text{ odd and } v \neq \pi\mathfrak{o}, \varpi\mathfrak{o} \end{cases}$$

Let $v = \pi\mathfrak{o}$. Suppose that there is a solution x, y, z in k_v to

$$\pi x^2 + \varpi y^2 \;=\; z^2$$

Via the ultrametric property, $\mathrm{ord}_v y$ and $\mathrm{ord}_v z$ are identical, and less than $\mathrm{ord}_v x$, since ϖ is a v-unit and $\mathrm{ord}_v \pi x^2$ is *odd*. Multiply through by π^{2n} so that $\pi^n y$ and $\pi^n z$ are v-units. Then ϖ must be a square modulo v.

On the other hand, when ϖ is a square modulo v, use Hensel's lemma to infer that ϖ is a square in k_v. Then $\varpi y^2 = z^2$ certainly has a non-trivial solution.

For v an odd prime distinct from $\pi\mathfrak{o}$ and $\varpi\mathfrak{o}$, π and ϖ are v-units. When ϖ is a square in k_v, $\varpi = z^2$ has a solution, so the Hilbert symbol is 1. For unit ϖ not a square in k_v, the quadratic field extension $k_v(\sqrt{\varpi})$ has the property that the norm map is *surjective* to units in k_v. Thus, there are $y, z \in k_v$ so that

$$\pi \;=\; N(z + y\sqrt{\varpi}) \;=\; z^2 - \varpi y^2$$

Thus, all but even-prime and infinite-prime quadratic Hilbert symbols are quadratic symbols. ///

Simplest example: For two (positive) odd prime numbers p, q, we prove that Gauss' quadratic reciprocity

$$\left(\frac{q}{p}\right)_2 \left(\frac{p}{q}\right)_2 \;=\; (-1)^{(p-1)(q-1)/4}$$

From quadratic Hilbert reciprocity,

$$\left(\frac{q}{p}\right)_2 \left(\frac{p}{q}\right)_2 \;=\; (p,q)_2 (p,q)_\infty$$

Indeed, since both p, q are positive, the equation

$$px^2 + qy^2 \;=\; z^2$$

has non-trivial *real* solutions x, y, z. That is, the $\mathbb{Q}_\infty$ Hilbert symbol $(p,q)_\infty$ is 1. Therefore, only the 2-adic Hilbert symbol contributes to the right-hand side of Gauss' formula:

$$\left(\frac{q}{p}\right)_2 \left(\frac{p}{q}\right)_2 \;=\; (p,q)_2$$

Hensel's lemma shows that the solvability of this equation, for p, q both 2-adic units, depends only upon their residue classes mod 8.

The usual formula $(-1)^{(p-1)(q-1)/4}$ is just one way of interpolating the 2-adic Hilbert symbol by elementary-looking formulas. ///

[42.8] Remark: Anticipating that general classfield theory is couched in terms of *norms*, we should expect analogous recovery of other reciprocity laws.

43. *Proof of quadratic norm-residue symbol reciprocity*

We show that over global fields k (characteristic not 2) the *quadratic norm residue symbol* is a *Hecke character*, that is, a $k^\times$-invariant continuous character on the ideles of k.

The role of certain quadratic exponential functions as tempered distributions is striking. The archimedean prototype is

$$S_x(z) \;=\; e^{\pi i x|z|^2} \qquad\qquad (x \in \mathbb{R}^\times \text{ and } z \in \mathbb{C})$$

This argument is suggested by, and essential to, a careful treatment of *Segal-Shale-Weil/oscillator representations*, and subsequent proof that *theta series are automorphic forms.*

[43.1] Standard set-up and Poisson summation

Let k be a global field of characteristic not 2. On each completion k_v of k fix a non-trivial additive unitary character ψ_v, so that, for all but finitely-many v,

$$\psi_v(xy) \;=\; 1 \;\text{ for all } y \in \mathfrak{o}_v \;\;\Leftrightarrow\;\; x \in \mathfrak{o}_v \qquad\qquad (\mathfrak{o}_v \text{ the local ring of integers})$$

Further, choose the family of characters so that the global character

$$\psi \;=\; \bigotimes_v \psi_v$$

is *trivial* on $k \subset k_{\mathbb{A}}$. For a character and (additive) Haar measure on k_v the local Fourier transform is

$$Ff(x) \;=\; \hat{f}(x) \;=\; \int_{k_v} f(y)\,\overline{\psi}_v(xy)\,dy$$

Take the Haar measure so that Fourier inversion holds:

$$f^{\frown\frown}(x) \;=\; f(-x)$$

The aggregate of local measures should make the total measure of the quotient $\mathbb{A}_k/k$ be 1.

Let K be either a quadratic field extension of k or isomorphic to $k \times k$. In either case let σ be the non-trivial k-algebra automorphism of K. Define a k-valued k-bilinear form $\langle,\rangle$ on K by

$$\langle \alpha, \beta\rangle \;=\; \mathrm{tr}_{K/k}(\alpha\beta^\sigma) \qquad\qquad (\text{with } \mathrm{tr}_{K/k}(\alpha) = \alpha + \alpha^\sigma)$$

Extend this k_v-linearly to a k_v-valued k_v-bilinear form $\langle,\rangle$ on

$$K_v \;=\; K \otimes_k k_v$$

Give the spaces K_v additive compatible Haar measures, such that Fourier Inversion holds locally everywhere, with respect to the pairing

$$a \times b \;\longrightarrow\; \psi\langle a, b\rangle$$

Locally and globally the convolution on Schwartz-Bruhat functions is

$$(f * \varphi)(a) \;=\; \int f(a-b)\,\varphi(b)\,db$$

The groups are abelian, so convolution is commutative:

$$f * \varphi \;=\; \varphi * f$$

For a Schwartz-Bruhat function f on $K_{\mathbb{A}}$, Poisson summation is

$$\sum_{x\in K} f(x) \;=\; \sum_{x\in K} \widehat{f}(x)$$

[43.2] Lemma: *(p-adic version)* For Schwartz-Bruhat f on K_v and smooth φ on K_v,

$$F(\varphi f) \;=\; F\varphi * Ff$$

where $F\varphi$ is the Fourier transform of the tempered distribution φ.

[43.3] Note: In the lemma, *smooth* means *locally constant.* The analogue of the lemma in the archimedean case is more delicate, since in that case Schwartz-Bruhat and test functions differ, and the notion of *moderate growth* is needed in addition to smoothness.

Proof: (p-adic case) The proof is a reduction to the corresponding property for Schwartz-Bruhat functions. Let L_b be the (left regular representation) operator on Schwartz-Bruhat functions by

$$L_b f(a) \;=\; f(a-b)$$

For a function h on K_v, let

$$\theta h(x) \;=\; h(-x)$$

The convolution of a distribution u and a test function f is

$$(u*f)(a) \;=\; u(L_a\theta f)$$

When the distribution u is integration against a *function* S, convolution is the usual convolution of functions.

WIth ch_X be the characteristic function of a (large) compact open subgroup X of K_v

$$\mathrm{ch}_X\varphi \longrightarrow \varphi \qquad\qquad \text{(in the topology of tempered distributions)}$$

Indeed, for large enough X depending upon the Schwartz-Bruhat function f,

$$\int_X \varphi(a)\, f(a)\, da \;=\; \int_{K_v} \varphi(a)\, f(a)\, da$$

since in the p-adic case f has compact support. Likewise, since the Fourier transform is a topological automorphism of Schwartz-Bruhat functions,

$$\lim_X F(\mathrm{ch}_X u) \;=\; Fu$$

Thus,

$$(F\varphi * Ff)(a) \;=\; (F\varphi)(L_a\theta Ff) \;=\; \lim_X\,(F(\mathrm{ch}_X\varphi))(L_a\theta Ff)$$
$$=\; \lim_X\,(F(\mathrm{ch}_X\varphi) * Ff)(a) \;=\; \lim_X\, F(\mathrm{ch}_X\varphi f)(a) \;=\; F(\varphi f)(a)$$

using the identity

$$F(\alpha*\beta) \;=\; F\alpha * F\beta$$

for Schwartz-Bruhat functions. ///

[43.4] Weil's quadratic exponential distributions are tempered distributions. The first two lemmas contain the germ of the reciprocity law.

For $x \in k_v^\times$ define

$$S_x(a) \;=\; \psi_v(\frac{x}{2}\langle a,a\rangle)$$

View this as a tempered distribution, as usual, by identifying it with the integration-against functional

$$f \longrightarrow \int_{K_v} S_x(a)\, f(a)\, da$$

[43.5] Lemma: *(p-adic case)*

$$FS_x \;=\; \gamma(x)\, S_{-x^{-1}}$$

where

$$\gamma(x) \;=\; \lim_X \int_X \psi_v(\frac{x}{2}\langle a,a\rangle)\, da$$

as X ranges over larger and larger compact open subgroups of K_v. In fact, there is a large-enough compact open subgroup Y of K so that the limit is reached for any $X \supset Y$.

[43.6] Lemma: Let f be a Schwartz-Bruhat function on K_v. For $x \in k_v^\times$ and $a \in K_v$

$$(S_x * f)(a) \;=\; S_x(a)\, F(S_x f)(xa)$$

Proof: (of first lemma) In the course of the proof, we show that the limit exists in the stronger sense indicated. By the usual definition of Fourier transform of a tempered distribution,

$$FS_x(f) \;=\; S_x(Ff) \;=\; \int_{K_v} S_x(a)\, Ff(a)\, da$$

Since Ff is also a Schwartz-Bruhat function, the characteristic function ch_X of any sufficiently large compact open set X can be inserted into the integral without affecting its value. Thus,

$$FS_x(f) \;=\; \int_{K_v} S_x(a)\, \mathrm{ch}_X(a)\, Ff(a)\, da$$

Then $S_x\mathrm{ch}_X$ is itself a Schwartz-Bruhat function, so apply the identity

$$\int_{K_v} f_1(a)\, Ff_2(a)\, da \;=\; \int_{K_v} Ff_1(a)\, f_2(a)\, da$$

Thus,

$$FS_x(f) \;=\; \int_{K_v} F(S_x\mathrm{ch}_X)(a)\, f(a)\, da$$

Since generally

$$\psi_v\langle a,b\rangle \;=\; \psi_v(\langle a,b\rangle^\sigma) \;=\; \psi_v\langle b,a\rangle$$

given $a \in K_v$,

$$F(S_x\mathrm{ch}_X)(a) \;=\; \int_X S_x(b)\, \overline{\psi}_v\langle a,b\rangle\, db \;=\; \int_X \psi_v(\frac{x}{2}\langle b,b\rangle - \langle a,b\rangle)\, db$$

$$= \int_X \psi_v(\frac{x}{2}\langle b,b\rangle - \tfrac{1}{2}\langle a,b\rangle - \tfrac{1}{2}\langle b,a\rangle)\, db \;=\; \int_X \psi_v(\frac{x}{2}\langle b - x^{-1}a, b - x^{-1}a\rangle - x^{-1}\langle a,a\rangle)\, db$$

For X large enough (depending upon a), replace b by $b + x^{-1}a$ to obtain

$$F(S_x\mathrm{ch}_X)(a) \;=\; S_{-x^{-1}}\langle a,a\rangle \int_X \psi_v(\frac{x}{2}\langle b,b\rangle)\, db$$

Thus,

$$FS_x \;=\; S_{-x^{-1}} \lim_X \int_X \psi_v(\frac{x}{2}\langle b,b\rangle)\,db$$

as claimed. ///

Proof: (of second lemma) From the definitions, and from

$$\psi\langle a,b\rangle \;=\; \psi\langle b,a\rangle$$

we have

$$(f*S_x)(a) \;=\; (S_x*f)(a) \;=\; \int_K S_x(a-b)\,f(b)\,db \;=\; \int_K \psi\big(\frac{x}{2}\langle a,a\rangle - \frac{x}{2}\langle a,b\rangle - \frac{x}{2}\langle b,a\rangle + \frac{x}{2}\langle b,b\rangle\big)\,f(b)\,db$$

$$=\; \int_K S_x(a)\,\overline{\psi}\langle xa,b\rangle\,S_x(b)\,f(b)\,db \;=\; S_x(a)\int_K \overline{\psi}\langle xa,b\rangle\,S_x(b)\,f(b)\,db \;=\; S_x(a)\,F(S_x f)(xa)$$

as desired. ///

[43.7] Quadratic norm residue symbols and local integrals

The *local norm residue symbol*

$$\nu_v : k_v^\times \longrightarrow \{\pm 1\}$$

attached to the 'separable quadratic extension' K_v/k_v is as follows. For $K_v = K\otimes_k k_v$ not a field, put $\nu_v(x) = 1$ for all $x\in k_v^\times$. For K_v is a field, put $\nu_v(x)=1$ if x is a norm from K_v, otherwise $\nu_v(x) = -1$.

It is non-trivial, but by now we know, that *the norms from K_v are of index two in $k_v^\times$ for K_v a separable quadratic field extension of $k_v^\times$*. We invoke this to know that ν_v is a group homomorphism.

As above, let

$$\gamma(x) \;=\; \gamma_v(x) \;=\; \lim_X \int_X S_x(a)\,da$$

where X ranges over larger and larger compact open subgroups of K_v, and $x\in k_v^\times$.

[43.8] Lemma: *(p-adic case)*

$$\gamma_v(x) \;=\; \nu_v(x)|x|_{k_v}^{-1}\,\gamma_v(1) \qquad\qquad (\text{for } x\in k_v^\times)$$

Proof: From the definition,

$$\gamma(x) \;=\; \lim_X \int_X \psi(xaa^\sigma)\,da$$

and *the limit is reached for sufficiently large X*. For $x\in k_v^\times$ of the form $x = bb^\sigma$, replacing a by ab^{-1} in the integral gives

$$\gamma(x) \;=\; |b|_{K_v}^{-1} \lim_X \int_{bX} \psi(aa^\sigma)\,da$$

We are using the local norms making the product formula hold, so

$$|x|_{k_v} \;=\; |bb^\sigma|_{k_v} \;=\; |b|_{K_v}$$

Thus, we have the desired formula when x is a local norm.

When x is not a local norm, then it must be that K_v is a field, otherwise the local norm map is onto. Let Θ be the subgroup of $K_v^\times$ of elements of norm 1; it is *compact.* Letting X vary over Θ-*stable* compact open subgroups,

$$\gamma(x) \;=\; \lim_X \int_X \psi(xaa^\sigma)\,da \;=\; \lim_X \int_{\Theta\backslash X}\int_\Theta \psi(xa\theta\theta^\sigma a^\sigma)\,d\theta\,da \;=\; \lim_X \int_{\Theta\backslash X} \psi(xaa^\sigma)\,da$$

giving Θ total measure 1. Taking the quotient of $K_v^\times$ by the kernel Θ of the norm,

$$\varphi \;:\; \Theta\backslash K_v^\times \;\longrightarrow\; k_v^\times \qquad\qquad (\text{by } \alpha \to \alpha\alpha^\sigma)$$

is an isomorphism to its image. Note that

$$d^\times\alpha \;=\; |\alpha|_{K_v}^{-1} d\alpha \qquad\qquad d^\times y \;=\; |y|_{k_v}^{-1} dy$$

are multiplicative Haar measures on $K_v^\times$ and $k_v^\times$, respectively. The (topological) isomorphism just above yields

$$\gamma(x) \;=\; \lim_X \int_{\Theta\backslash X} \psi(xaa^\sigma)\,da \;=\; \lim_{X'} \int_{\Theta\backslash X'} \psi(x\alpha\alpha^\sigma)\,|\alpha|_{K_v}\,d^\times\alpha \;=\; \lim_Y \int_Y \psi(xy)\,|y|_{k_v}\,d^\times y$$

where $y = \alpha\alpha^\sigma$, $X' = X - 0$, and Y is the image of X' under the norm map. (Here we choose *some* compatible normalizations of the measures: it doesn't matter *which.*)

Since in this quadratic field extension the norms are of index 2,

$$\lim_Y \int_Y \psi(xy)\,d^\times y \;=\; \lim_Z \int_Z \psi(xy)\,\frac{1}{2}(1 + \mathrm{ord}_v(y))\,|y|_{k_v}\,d^\times y$$

where Z runs over larger and larger compact open additive subgroups of k_v (ignoring the point $0 \in k_v^\times$). A typical elementary cancellation argument shows

$$\lim_Z \int_Z \psi(xy)\,|y|_{k_v}\,d^\times y \;=\; 0 \qquad\qquad (\text{for } x \neq 0)$$

Then

$$\gamma(x) \;=\; \lim_Z \int_Z \psi(xy)\,\frac{1}{2}\mathrm{ord}_v(y)\,|y|_{k_v}\,d^\times y$$

Replace y by yx^{-1} to obtain the desired identity. ///

[43.9] Reciprocity law for quadratic norm residue symbols

[43.10] Theorem: The (quadratic) *global norm residue symbols*

$$x \;\longrightarrow\; \nu_{K/k}(x) \;=\; \Pi_v\,\nu_v(x) \qquad\qquad (\text{with } x \text{ an idele of } k)$$

are *Hecke characters*, that is, are *trivial on* $k^\times$. Continuity is clear.

Proof: This *global* assertion needs a global *source*: Poisson summation. For f an *adelic* Schwartz-Bruhat function, $x \in k^\times$, and an adele $a = \{a_v\}$, write

$$S_x(a) \;=\; \Pi_v\,S_x^v(a_v)$$

where

$$S_x^v(a) \;=\; \psi_v(\frac{x}{2}a_v a_v^\sigma)$$

Since S_x is 1 on K,

$$\sum_{a\in K} f(a) \;=\; \sum_{a\in K} S_x(a)\, f(a)$$

By Poisson summation,

$$\sum_{a\in K} F(S_x f)(a) \;=\; \sum_{a\in K} (FS_x * Ff)(a) \;=\; \gamma(x) \sum_{a\in K} (S_{-x^{-1}} * Ff)(a)$$

by the first lemma, which computed the Fourier transform of S_x as tempered distribution. By the second lemma, which computed $S_x * f$, this is

$$\gamma(x) \sum_{a\in K} S_{-x^{-1}}(a)\, F(S_{-x^{-1}} Ff)(xa) \;=\; \gamma(x) \sum_{a\in K} F(S_{-x^{-1}} Ff)(xa)$$

since $S_{-x^{-1}} = 1$ on K. Change variables in the sum, replacing a by ax^{-1}, to obtain (so far)

$$\sum_{a\in K} f(a) \;=\; \gamma(x) \sum_{a\in K} F(S_{-x^{-1}} Ff)(a) \;=\; \gamma(x) \sum_{a\in K} S_{-x^{-1}}(a)\, Ff(a)$$

the latter by Poisson summation, and this is

$$=\; \gamma(x) \sum_{a\in K} Ff(a) \;=\; \gamma(x) \sum_{a\in K} f(a)$$

since $S_{-x^{-1}}(a) = 1$, and again applying Poisson summation. Taking any f so that

$$\sum_{a\in K} f(a) \;\neq\; 0$$

necessarily

$$\gamma(x) \;=\; 1 \qquad\qquad \text{(for all } x \in k^\times\text{)}$$

Then

$$1 \;=\; \gamma(x) \;=\; \Pi_v\, \gamma_v(x) \;=\; \Pi_v\, |x|_{k_v}^{-1} \nu_v(x)\gamma_v(x) \;=\; \Pi_v\, \nu_v(x)\gamma_v(1) \;=\; \nu(x)\gamma(1)$$

from the product formula and from the earlier result that

$$\gamma_v(x) \;=\; \nu_v(x)\gamma_v(1)$$

Thus, ν is a Hecke character. ///

44. *Herbrand quotients, topological antecedents*

[44.1] Herbrand quotients: veiled homological ideas Homological algebra includes computational devices extending linear algebra and counting procedures. Motivations also come from (algebraic) topology, defining and *counting holes.*

It is easy enough to *define* the *Herbrand quotient*, although explaining its significance requires more effort:

Let A be an abelian group, with maps $f : A \to A$ and $g : A \to A$, such that $f \circ g = 0$ and $g \circ f = 0$.

$$q(A) \;=\; q_{f,g}(A) \;=\; \text{Herbrand quotient of } A, f, g \;=\; \frac{[\ker f : \mathrm{im} g]}{[\ker g : \mathrm{im} f]}$$

(Inscrutable) Herbrand Quotient Lemma: For finite A, $q(A) = 1$. For f-stable, g-stable subgroup $A \subset B$ with $f, g : B \to B$, we have $q(B) = q(A) \cdot q(B/A)$, in the usual sense that if two are finite, so is the third, and the relation holds:

$$\frac{[\ker f|_B : \mathrm{im} g|_B]}{[\ker g|_B : \mathrm{im} f|_B]} \;=\; q(B) \;=\; q(A) \cdot q(B/A) \;=\; \frac{[\ker f|_A : \mathrm{im} g|_A]}{[\ker g|_A : \mathrm{im} f|_A]} \cdot \frac{[\ker f|_{B/A} : \mathrm{im} g|_{B/A}]}{[\ker g|_{B/A} : \mathrm{im} f|_{B/A}]}$$

We will see that this lemma is about *Euler-Poincaré characteristics* of the short exact sequence of *complexes*

$$\begin{tikzcd}
 & \vdots \arrow[d, "f"'] & \vdots \arrow[d, "f"'] & \vdots \arrow[d, "f"'] & \\
0 \arrow[r] & A \arrow[r] \arrow[d, "g"'] & B \arrow[r] \arrow[d, "g"'] & B/A \arrow[r] \arrow[d, "g"'] & 0 \\
0 \arrow[r] & A \arrow[r] \arrow[d, "f"'] & B \arrow[r] \arrow[d, "f"'] & B/A \arrow[r] \arrow[d, "f"'] & 0 \\
0 \arrow[r] & A \arrow[r] \arrow[d, "g"'] & B \arrow[r] \arrow[d, "g"'] & B/A \arrow[r] \arrow[d, "g"'] & 0 \\
 & \vdots & \vdots & \vdots &
\end{tikzcd}$$

The best-known *Euler characteristic* refers to the numbers of vertices V, edges E, and F faces of a polyhedron, and *Euler's theorem* is that, for *convex* polyhedra,

$$V - E + F \;=\; 2 \qquad\qquad \text{(Euler char of convex polyhedron)}$$

In a purely algebraic setting, with definitions stripped of origins, motivation, or purpose: A *complex* of abelian groups A_i is a family of homomorphisms

$$\ldots \longrightarrow A_i \xrightarrow{f_i} A_{i-1} \xrightarrow{f_{i-1}} \ldots$$

with the *composition of any two consecutive maps* equal 0, that is, with $f_{i-1} \circ f_i \;=\; 0$, for all i. The **(co)homology**, with superscript or subscript depending on context and numbering conventions, is

$$H_i(\text{the complex}) \;=\; H^i(\text{the complex}) \;=\; \frac{\ker f_i}{\mathrm{im} f_{i\pm 1}}$$

The utility of this requires explanation. Indeed, the history of the interaction of linear algebra and algebraic topology (as *counting holes*) is tangled.

[44.2] Recollection of topological antecedents:

counting holes. An n-dimensional triangle is an n-*simplex.* A *simplicial complex* [different use of the word!] X is a topological space made by sticking together simplices *in a reasonable way.*

An *orientation* of a simplex is an ordering of its vertices: an oriented n-simplex is a list $\sigma = [v_o, v_1, \ldots, v_n]$ of $n+1$ vertices v_j, with ordering specified modulo even permutations.

The *boundary* $\partial\sigma$ is an alternating sum, in the free group generated by the simplices in X:

$$\begin{aligned}\partial\sigma \;&=\; [v_1,\ldots,v_n] - [v_o,v_2,\ldots,v_n] + \ldots + (-1)^n[v_o,v_1,\ldots,v_{n-1}] \\ &=\; \sum_{j=0}^{n}(-1)^j[v_o,\ldots,\widehat{v_j},\ldots,v_n] \qquad\qquad \text{(hat denoting omission)}\end{aligned}$$

Permuting the vertices in a simplex multiplies it by the sign of the permutation:

$$[v_{\pi(0)}, v_{\pi(1)}, \ldots, v_{\pi(n)}] \;=\; \text{sign}(\pi)\cdot[v_0, v_1, \ldots, v_n]$$

Such symbol-patterns occur in many places.

The abelian group C_n of *n-chains* in X is the free group on oriented n-dimensional simplices in X, and $\partial = \partial_n$ maps $C_n \to C_{n-1}$. A little work shows that $\partial_{n-1}\circ\partial_n = 0$ as a map $C_n \to C_{n-2}$, so we have a *chain complex*

$$\begin{tikzcd} \ldots \arrow[r] & C_i \arrow[r, "\partial_i"] & C_{i-1} \arrow[r, "\partial_{i-1}"] & \ldots \arrow[r, "\partial_2"] & C_1 \arrow[r, "\partial_1"] & C_0 \end{tikzcd}$$

with *homology*

$$H_i(X) \;=\; \frac{\ker\partial_i}{\text{im}\partial_{i+1}} \;=\; \frac{i\text{-dimensional } \textit{cycles}}{i\text{-dimensional } \textit{boundaries}}$$

It is not obvious, but *the rank of the free part of $H_i(X)$ is the number of i-dimensional holes in X*, in the following sense.

Basic theorem: The n-sphere S^n has $H_i(S^n) = 0$ for $0 < i \neq n$, and $H_n(S^n) = \mathbb{Z}$. ///

[44.3] Example:

First, check that $\partial_1\partial_2 = 0$:

$$\partial_1\partial_2[v_0,v_1,v_2] \;=\; \partial_1\Big([v_1,v_2]-[v_0,v_2]+[v_0,v_1]\Big) \;=\; \big([v_2]-[v_1]\big)-\big([v_2]-[v_0]\big)+\big([v_1]-[v_0]\big) \;=\; 0$$

Second: make a circle S^1 as a hollow triangle X by sticking together three line segments $[v_0,v_1]$, $[v_1,v_2]$, $[v_2,v_0]$. The whole chain complex is not very big:

$$\begin{tikzcd} 0 \arrow[r, "\partial_2"] & C_1 \arrow[r, "\partial_1"] & C_0 \end{tikzcd}$$

with C_1 free of rank 3 made from the three line segments $[v_i,v_j]$, and C_0 of rank 3, made from the three vertices.

$$H_1(X) \;=\; \frac{\ker\partial_1}{\text{im}\partial_2} \;=\; \ker\partial_1 \;=\; \mathbb{Z}\cdot\Big([v_0,v_1]+[v_1,v_2]+[v_2,v_0]\Big)$$

Thus, $H_1(X)$ is free, rank one, so this computes that *there is one one-dimensional hole in a circle.*

Another example computation: We can make a 2-sphere by sticking together four oriented triangles along their edges, forming a hollow tetrahedron X: $[v_0,v_1,v_2]$, $[v_1,v_2,v_3]$, $[v_2,v_3,v_0]$, and $[v_3,v_0,v_1]$. The whole chain complex is not very big:

$$\begin{tikzcd} 0 \arrow[r] & C_2 \arrow[r, "\partial_2"] & C_1 \arrow[r, "\partial_1"] & C_0 \end{tikzcd}$$

with C_2 free of rank 4 made from the four triangles, C_1 of rank 6 made from the six line segments $[v_i, v_j]$, and C_0 of rank 4, made from the four vertices. Note the patterns $\partial_1[v_a, v_b] \;=\; [v_a] - [v_b]$ and

$$\partial_2[v_a, v_b, v_c] \;=\; [v_b, v_c] - [v_a, v_c] + [v_a, v_b]$$

Linear algebra gives $H_1(X) \approx \{0\}$ and $H_2(X) \approx \mathbb{Z}$, confirming that there is *no* one-dimensional hole in a 2-sphere, but there is a *two-dimensional* hole.

Computational device: long exact sequence, Mayer-Vietoris sequence The homology of spheres S^n is best determined *not* by *direct* computation. Under mild hypotheses on topological spaces X, Y, there is a *long exact sequence* (Recall: $A \to B \to C$ is *exact* when $\mathrm{im}(A \to B) = \ker(B \to C)$...)

$$\begin{tikzcd}
 & & \ldots \arrow[dll] \\
\ldots H_i(X \cap Y) \arrow[r] & H_i(X) \oplus H_i(Y) \arrow[r] & H_i(X \cup Y) \arrow[dll] \\
H_{i-1}(X \cap Y) \arrow[r] & H_{i-1}(X) \oplus H_{i-1}(Y) \arrow[r] & H_{i-1}(X \cup Y) \arrow[dll] \\
\ldots & &
\end{tikzcd}$$

The long exact sequence is the basic computational device!

The long exact sequence allows computation of homology of spheres *by induction.* Suppose $H_i(S^{n-1}) = 0$ for $0 < i < n-1$ and $H_{n-1}(S^{n-1}) = \mathbb{Z}$. Also, $H_0(S^{n-1}) = \mathbb{Z}$, equivalent to *connectedness.* S^n is the union of upper hemi-sphere X and lower hemi-sphere Y, with intersection the equator S^{n-1}, setting up the induction. We grant ourselves that X, Y have no holes, in the sense that their only non-vanishing homology is $H_0(X) = H_0(Y) = \mathbb{Z}$. Thus, all the higher $H_i(X) \oplus H_i(Y)$'s are 0, and the long exact sequence becomes

$$\begin{tikzcd}
 & & \ldots \arrow[dll] \\
\ldots H_i(S^{n-1}) \arrow[r] & 0 \arrow[r] & H_i(S^n) \arrow[dll] \\
H_{i-1}(S^{n-1}) \arrow[r] & 0 \arrow[r] & H_{i-1}(S^n) \arrow[dll] \\
\ldots & &
\end{tikzcd}$$

That is, the long exact sequence in homology breaks up into smaller exact sequences

$$0 \longrightarrow H_i(S^n) \longrightarrow H_{i-1}(S^{n-1}) \longrightarrow 0 \qquad\qquad (\text{for } i > 1)$$

and, more fussily,

$$0 \to H_1(S^n) \to H_0(S^{n-1}) \to H_0(X) \oplus H_0(Y) \to H_0(S^n) \to 0$$

The *dimension-shifting* conclusion is $H_i(S^n) \approx H_{i-1}(S^{n-1})$, clear for $i > 1$.

For the fussy case $i = 1$, $0 \to H_1(S^n) \to \mathbb{Z} \to \mathbb{Z} \oplus \mathbb{Z} \to \mathbb{Z} \to 0$ gives $H_1(S^n) = 0$. ///

[44.4] Remark: This computation is an archetype.

45. *Homological paraphrase of Hilbert's Theorem 90*

The linear algebra that counts holes is useful for counting other things.

To introduce cohomology as saying useful things about familiar objects, rewrite Hilbert's theorem 90: for $G = \mathrm{Gal}(K/k) = \langle\sigma\rangle$ *cyclic*, letting $t = \sum_{g\in G} g \in \mathbb{Z}[G]$, the additive version of the theorem asserts

$$\frac{\ker t|_K}{\mathrm{im}(\sigma-1)|_K} \;=\; 0$$

The multiplicative version *has the same form*, once we realize that for $\beta \in K^\times$, $(\sigma-1)\beta = \sigma\beta/\beta$ and $t\cdot\beta = N_k^K(\beta)$.

An assertion ker/im = 0 is of the desired homological form. Homological algebra puts such quotients into a larger context. *The Artin/reciprocity map will have a natural homological sense.* The numerators in Hilbert's Theorem 90 are the kernels of the norm $N_k^K : K^\times \to k^\times$ and trace $\mathrm{tr}_k^K : K \to k$. $k^\times = (K^\times)^G$ and $k = K^G$ are the G-fixed submodules of $K^\times$ and K, by Galois theory.

Recall that, for a group G and $\mathbb{Z}$-module A with G acting, the *fixed* sub-module A^G is

$$A^G \;=\; \{a \in A \;:\; ga = a \,\text{for all}\, g\in G\}$$

This is the trivial-representation *isotype* in A. This is *characterized* as the *subobject* through which all G-maps from trivial G-modules N to A factor:

$$\begin{tikzcd}
A^G \arrow[r] & A \\
X \arrow[u, dashed, "\exists!"] \arrow[ur, "\forall"'] &
\end{tikzcd}$$

(G acting trivially on X)

The denominators in Theorem 90 are explained as follows. The *co-fixed* quotient module A_G of a G-module A is characterized as the *quotient* through which all G-maps from A to trivial G-modules X factor:

$$\begin{tikzcd}
A_G \arrow[d, dashed, "\exists!"'] & A \arrow[l] \arrow[dl, "\forall"] \\
X &
\end{tikzcd}$$

(G acting trivially on X)

This is A's trivial-representation *co-isotype*. It is provably *constructed* as

$$A_G \;=\; \frac{A}{I_G\cdot A}$$

where I_G is the *augmentation ideal*, the kernel of the *augmentation map* $\varepsilon : \mathbb{Z}[G] \to \mathbb{Z}$, defined by $\varepsilon g = 1$ for all $g \in G$. Therefore,

$$I_G \;=\; \text{ideal generated in } \mathbb{Z}[G] \text{ by } g-1 \text{ for } g \in G$$

$I_G \cdot A$ appears in Hilbert's theorem 90 for cyclic G.

For *cyclic* $G = \langle\sigma\rangle$ of order n, with $t = \sum_{g\in G} g$

$$(\sigma-1)\cdot t \;=\; t\cdot(\sigma-1) \;=\; (\sigma-1)\cdot(1+\sigma+\sigma^2+\ldots+\sigma^{n-1})$$

$$=\; \sigma^n - 1 \;=\; 0 \qquad\qquad (\text{in } \mathbb{Z}[G])$$

Thus, since the composite of any two successive maps is 0, by definition we have a two-sided *complex* fitting the hypotheses of the *Herbrand quotient* situation:

$$\begin{tikzcd}\dots \arrow[r, "t"] & A \arrow[r, "\sigma-1"] & A \arrow[r, "t"] & A \arrow[r, "\sigma-1"] & A \arrow[r, "t"] & \dots\end{tikzcd}$$

(Co-)homology quotients abstracting Theorem 90 are

$$\frac{\ker t|_A}{\mathrm{im}(\sigma-1)|_A} \qquad\qquad \frac{\ker(\sigma-1)|_A}{\mathrm{im} t|_A}$$

46. *Sample exact sequences*

[46.1] Euler-Poincaré characteristics We noted that the homology of spheres S^n is best computed *not* by expressing the spheres as simplicial complexes and using the definition, but by a *long exact sequence* in homology, obtained from the Mayer-Vietoris theorem.

That is, express S^n as the union of two hemispheres, each having trivial homology (no holes!), intersecting at the equator, isomorphic to S^{n-1}. In this example, the (Mayer-Vietoris) long exact sequence has many 0's, giving $H^i(S^n) \approx H^{i-1}(S^{n-1})$ for $2 \le i < n$. Induction on the dimension n of S^n essentially reduces to some low-dimensional and *edge* cases.

These edge cases are nicely explained via *Euler-Poincaré characteristics*, in an algebraic sense, rather than the naive geometric sense $V - E + F$.

The fussy edge cases in using Mayer-Vietoris to compute homology of spheres are

$$0 \to H_1(S^n) \to \mathbb{Z} \to \mathbb{Z} \oplus \mathbb{Z} \to \mathbb{Z} \to 0$$

and, at the bottom of the induction,

$$0 \to H_1(S^1) \to \mathbb{Z} \oplus \mathbb{Z} \to \mathbb{Z} \oplus \mathbb{Z} \to \mathbb{Z} \to 0$$

In both cases, the unknown object injects to a free $\mathbb{Z}$-module, so is free. Then the question is obviously its *rank*.

Claim *(about Euler characteristic)***:** In an exact sequence

$$0 \longrightarrow F_1 \longrightarrow F_2 \longrightarrow \dots \longrightarrow F_{n-1} \longrightarrow F_n \longrightarrow 0$$

of *free* modules F_i, we have $\sum_i (-1)^i \cdot \mathrm{rk} F_i = 0$.

Proof: For a *short* exact sequence $0 \to A \to B \to C \to 0$ of vector spaces over a field, the standard idea that any basis of A can be extended to a basis of B, with the (images of the) *new* elements forming a basis of $C \approx B/A$, proves the assertion in this case.

The general case is by induction: an exact sequence

$$\begin{tikzcd}0 \arrow[r] & F_1 \arrow[r] & \dots \arrow[r] & F_{n-1} \arrow[r] & F_{n-1} \arrow[r] & F_n \arrow[r] & 0\end{tikzcd}$$

with $n > 3$ can be broken into two smaller ones:

$$\begin{tikzcd}0 \arrow[r] & \dots \arrow[r] & F_{n-2} \arrow[rr] \arrow[dr] & & F_{n-1} \arrow[r] & F_n \arrow[r] & 0 \\ & & & X \arrow[ur] \arrow[dr] & & & \\ & & 0 \arrow[ur] & & 0 & & \end{tikzcd}$$

with X the image of F_{n-2} and the kernel of $F_{n-1} \to F_n$. Then the two equations

$$\dim F_1 - \dim F_2 + \dim F_3 - ... + (-1)^{n-1} \dim X \ = \ 0$$

$$\dim X - \dim F_{n-1} + \dim F_n \ = \ 0$$

give the assertion, by subtracting or adding. ///

[46.2] Remark: The same argument applies to exact sequences of *free modules* over a PID.

[46.3] Remark: The same argument proves a counting result, namely, for an exact sequence of *finite* abelian groups,

$$\begin{tikzcd} 0 \arrow[r] & M_1 \arrow[r] & \ldots \arrow[r] & M_{n-1} \arrow[r] & M_{n-1} \arrow[r] & M_n \arrow[r] & 0 \end{tikzcd}$$

$\prod_i |M_i|^{(-1)^i} = 1$, or, equivalently, $\sum_i (-1)^i \cdot \log |M_i| = 0$. This bears on Herbrand-quotient issues.

[46.4] Shortest long exact sequence A commutative diagram

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & A \arrow[r] \arrow[d, "f"'] & B \arrow[r] \arrow[d, "f"'] & C \arrow[r] \arrow[d, "f"'] & 0 \\
0 \arrow[r] & A' \arrow[r] \arrow[d] & B' \arrow[r] \arrow[d] & C' \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

with exact *rows* gives a long exact sequence

$$0 \to \ker f|_A \to \ker f|_B \to \ker f|_C \to \frac{A'}{fA} \to \frac{B'}{fB} \to \frac{C'}{fC} \to 0$$

The least obvious map is $\ker f|_C \longrightarrow A'/fA$. The diagram is a short exact sequence of the *complexes* $0 \to A \to A' \to 0$, $0 \to B \to B' \to 0$, and $0 \to C \to C' \to 0$.

Least obvious part of the proof: The *connecting homomorphism* $\delta : \ker f|_C \longrightarrow A'/fA$ is not obvious. Given $f(c) = 0$, take $b \to c$. Then $f(b) \to f(c) = 0$, so there is $a' \to f(b)$. Put $\delta(c) = a'$.

The rest of the proof is more natural. ///

[46.5] Remark: The previous description of the connecting homomorphism is the content of the *Snake Lemma.*

[46.6] Example: Powers in $\mathbb{Z}_p^\times$, $p > 2$. Let $f(x) = x^n$, and consider

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & 1 + p\mathbb{Z}_p \arrow[r] \arrow[d, "f"'] & \mathbb{Z}_p^\times \arrow[r] \arrow[d, "f"'] & \mathbb{Z}/p^\times \arrow[r] \arrow[d, "f"'] & 0 \\
0 \arrow[r] & 1 + p\mathbb{Z}_p \arrow[r] \arrow[d] & \mathbb{Z}_p^\times \arrow[r] \arrow[d] & \mathbb{Z}/p^\times \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

Let $\mu_n R$ be n^{th} roots of unity in R, and $U = 1 + p\mathbb{Z}_p$. The long exact sequence is (with multiplicative notation)

$$1 \to \mu_n U \to \mu_n \mathbb{Z}_p^\times \to \mu_n \mathbb{Z}/p^\times \to \frac{U}{U^n} \to \frac{\mathbb{Z}_p^\times}{(\mathbb{Z}_p^\times)^n} \to \frac{\mathbb{Z}/p^\times}{(\mathbb{Z}/p^\times)^n} \to 1$$

For $p \not| n$, and $p > 2$ we understand n^{th} powers in U and in $\mathbb{Z}/p^\times$: on U the n^{th} power map is an isomorphism. Thus, the previous diagram becomes

$$1 \to 1 \to \mu_n \mathbb{Z}_p^\times \to \mu_n \mathbb{Z}/p^\times \to 1 \to \frac{\mathbb{Z}_p^\times}{(\mathbb{Z}_p^\times)^n} \to \frac{\mathbb{Z}/p^\times}{(\mathbb{Z}/p^\times)^n} \to 1$$

The collapsing gives two *isomorphisms*: whatever n^{th} roots of unity are in $\mathbb{Z}/p^\times$ lift to $\mathbb{Z}_p^\times$, and $x \in \mathbb{Z}_p^\times$ is an n^{th} power *if and only if* it is an n^{th} power mod p.

[46.7] Remark: Obtaining n^{th} roots of unity in $\mathbb{Z}_p$ didn't seem to need Hensel's Lemma, only that $x \to x^n$ is an isomorphism on U.

47. *Herbrand quotients: less-bare definition*

An abelian group A with an ordered pair of maps $f : A \to A$ and $g : A \to A$, with $f \circ g = 0$ and $g \circ f = 0$ gives a periodic *complex*

$$\ldots \xrightarrow{f} A \xrightarrow{g} A \xrightarrow{f} A \xrightarrow{g} \ldots$$

This is an example of a *complex*

$$\ldots \xrightarrow{f_{i-1}} A_i \xrightarrow{f_i} A_{i+1} \xrightarrow{f_{i+1}} \ldots$$

where the essential requirement is that the composition $f_{i+1} \circ f_i$ of any two successive maps is 0, that is, that $\ker f_i \subset \mathrm{im} f_{i+1}$. The *(co-) homology* of the complex is the collection of quotients

$$H_i(\text{the complex}) \;=\; H^i(\text{the complex}) \;=\; \frac{\ker f_i|_{A_i}}{\mathrm{im} f_{i-1}|_{A_{i-1}}}$$

The periodic complex

$$\ldots \xrightarrow{f} A \xrightarrow{g} A \xrightarrow{f} A \xrightarrow{g} \ldots$$

has just two (co-) homology groups,

$$\frac{\ker f|_A}{\mathrm{im} g_A} \qquad \frac{\ker g|_A}{\mathrm{im} f_A}$$

and there is no natural indexing. The *Herbrand quotient* is the ratio of the orders of these groups:

$$\text{Herbrand quotient of } A, f, g \;=\; q_{f,g}(A) \;=\; \frac{[\ker f : \mathrm{im} g]}{[\ker g : \mathrm{im} f]}$$

Back to the

(Inscrutable) Herbrand Quotient Lemma: For finite A, $q(A) = 1$. For f-stable, g-stable subgroup $A \subset B$ with $f, g : B \to B$, we have $q(B) = q(A) \cdot q(B/A)$, in the usual sense that if two are finite, so is the third, and the relation holds. *(Proof below)*

In fact, letting $C = B/A$, the lemma refers to a situation

$$\begin{tikzcd}
& \cdots \arrow[d, "g"'] & \cdots \arrow[d, "g"'] & \cdots \arrow[d, "g"'] & \\
0 \arrow[r] & A \arrow[r] \arrow[d, "f"'] & B \arrow[r] \arrow[d, "f"'] & C \arrow[r] \arrow[d, "f"'] & 0 \\
0 \arrow[r] & A \arrow[r] \arrow[d, "g"'] & B \arrow[r] \arrow[d, "g"'] & C \arrow[r] \arrow[d, "g"'] & 0 \\
0 \arrow[r] & A \arrow[r] \arrow[d, "f"'] & B \arrow[r] \arrow[d, "f"'] & C \arrow[r] \arrow[d, "f"'] & 0 \\
& \cdots & \cdots & \cdots &
\end{tikzcd}$$

with columns *complexes* and rows *exact*, where again, $\ldots \xrightarrow{f} X \xrightarrow{g} \ldots$ *exact* means $\ker g = \mathrm{im} f$. Important special cases are that $0 \to A \to B$ implies $A \to B$ *injects*, and $B \to C \to 0$ implies $B \to C$ *surjects*. The latter diagram is *commutative*, in the sense that compositions of maps are independent of the route through the diagram.

In the Herbrand quotient diagram, a special case of the *long exact sequence in (co-) homology* will give a periodic long exact sequence

$$\ldots \to \frac{\ker f_A}{\mathrm{im} g_A} \to \frac{\ker f_B}{\mathrm{im} g_B} \to \frac{\ker f_C}{\mathrm{im} g_C} \to \frac{\ker g_A}{\mathrm{im} f_A} \to \frac{\ker g_B}{\mathrm{im} f_B} \to \frac{\ker g_C}{\mathrm{im} f_C} \to \ldots$$

The periodicity often is emphasized by writing the long exact sequence as

$$\begin{tikzcd}
& \frac{\ker f|_A}{\mathrm{im} g|_A} \arrow[r] & \frac{\ker f|_B}{\mathrm{im} g|_B} \arrow[dr] & \\
\frac{\ker g|_C}{\mathrm{im} f|_C} \arrow[ur] & & & \frac{\ker f|_C}{\mathrm{im} g|_C} \arrow[dl] \\
& \frac{\ker g|_B}{\mathrm{im} f|_B} \arrow[ul] & \frac{\ker g|_A}{\mathrm{im} f|_A} \arrow[l] &
\end{tikzcd}$$

The numerical assertion of the Herbrand lemma is extracted from this periodic exact sequence by *Euler-Poincaré characteristics.*

[47.1] Claim: (Recap) The *Euler characteristic* $\sum_i (-1)^i \dim F_i$ of an exact sequence

$$0 \longrightarrow V_1 \longrightarrow V_2 \longrightarrow \ldots \longrightarrow V_{n-1} \longrightarrow V_n \longrightarrow 0$$

of vector spaces over a field is $\sum_i (-1)^i \dim F_i = 0$. ///

[47.2] Corollary: The Euler-Poincaré characteristic $\dim V_1 - \dim V_2 + \dim V_3 - \dim V_4 + \dim V_5 - \dim V_6$ of a *periodic* exact diagram of vector spaces

$$\begin{tikzcd}
& V_1 \arrow[r] & V_2 \arrow[dr] & \\
V_6 \arrow[ur] & & & V_3 \arrow[dl] \\
& V_5 \arrow[ul] & V_4 \arrow[l] &
\end{tikzcd}$$

is 0.

Proof: Use the splicing trick, with

$$X \;=\; \ker(V_1 \to V_2) \;=\; \mathrm{im}(V_6 \to V_1)$$

to rewrite the periodic exact sequence as

$$\begin{tikzcd} 0 \arrow[r] & X \arrow[r] & V_1 \arrow[r] & \ldots \arrow[r] & V_6 \arrow[r] & X \arrow[r] & 0 \end{tikzcd}$$

The Euler-Poincaré characteristic of the un-spliced exact sequence is

$$0 \;=\; (-1)^1 \dim X - \Big(\sum_{i=1}^{6} (-1)^i \dim V_i\Big) + (-1)^8 \dim X \;=\; -\sum_{i=1}^{6} (-1)^i \dim V_i$$

giving the asserted vanishing. ///

[47.3] Remark: By the same arguments, for exact sequences of *finite* abelian groups

$$\begin{tikzcd} 0 \arrow[r] & A_1 \arrow[r] & \ldots \arrow[r] & A_{n-1} \arrow[r] & A_{n-1} \arrow[r] & A_n \arrow[r] & 0 \end{tikzcd}$$

we have

$$\frac{|A_1| \cdot |A_3| \cdot |A_5| \cdot \ldots}{|A_2| \cdot |A_4| \cdot |A_6| \ldots} \;=\; 1$$

and the analogous corollary: for periodic exact

$$\begin{tikzcd} & A_1 \arrow[r] & A_2 \arrow[dr] & \\ A_6 \arrow[ur] & & & A_3 \arrow[dl] \\ & A_5 \arrow[ul] & A_4 \arrow[l] & \end{tikzcd}$$

we have

$$\frac{|A_1| \cdot |A_3| \cdot |A_5|}{|A_2| \cdot |A_4| \cdot |A_6|} \;=\; 1$$

From the periodic exact sequence

$$\begin{tikzcd} & \dfrac{\ker f|_A}{\mathrm{img}|_A} \arrow[r] & \dfrac{\ker f|_B}{\mathrm{img}|_B} \arrow[dr] & \\ \dfrac{\ker g|_C}{\mathrm{im}f|_C} \arrow[ur] & & & \dfrac{\ker f|_C}{\mathrm{img}|_C} \arrow[dl] \\ & \dfrac{\ker g|_B}{\mathrm{im}f|_B} \arrow[ul] & \dfrac{\ker g|_A}{\mathrm{im}f|_A} \arrow[l] & \end{tikzcd}$$

we obtain the assertion of the *Herbrand Quotient Lemma*:

$$1 \;=\; \frac{|A_1|}{|A_4|} \cdot \frac{|A_5|}{|A_2|} \cdot \frac{|A_3|}{|A_6|} \;=\; \frac{[\ker f_A : \mathrm{img}_A]}{[\ker g_A : \mathrm{im}f_A]} \cdot \frac{[\ker g_B : \mathrm{im}f_B]}{[\ker f_B : \mathrm{img}_B]} \cdot \frac{[\ker f_C : \mathrm{img}_C]}{[\ker g_C : \mathrm{im}f_C]} \qquad ///$$

[47.4] Remark: The finiteness assertions were omitted, but it is clear that the Herbrand quotient lemma is a corollary of Euler-Poincaré characteristic ideas and the long exact sequence in homology.

We collect some further lemmas of a veiled homological nature:

[47.5] Lemma: For A finite, $\frac{[\ker f_A : \mathrm{im} g_A]}{[\ker g_A : \mathrm{im} f_A]} = 1$.

Proof: A similar but more elementary hexagonal picture is useful, with ascending lines inclusions:

$$\begin{tikzcd}
& A \arrow[dl, dash] \arrow[dr, dash] & \\
\ker f|_A \arrow[d, dash] & & \ker g|_A \arrow[d, dash] \\
\mathrm{im} g|_A \arrow[dr, dash] & & \mathrm{im} f|_A \arrow[dl, dash] \\
& 0 &
\end{tikzcd}$$

By the isomorphism theorem, $A/\ker f|_A \approx \mathrm{im} f|_A$ and $A/\ker g|_A \approx \mathrm{im} g|_A$, so opposite *slanted* sides have the same indices. By finiteness of A and multiplicativity of indices, the vertical indexes are identical. ///

[47.6] Lemma: For abelian groups $A \supset B$ with a group homomorphism $f : A \to A'$, writing f_A for $f|_A$ and similarly for B,

$$[A : B] \;=\; [\ker f_A : \ker f_B] \,\cdot\, [\mathrm{im} f_A : \mathrm{im} f_B]$$

in the sense that if two of the indices are *finite*, then the third is, also, and equality holds

Proof: Certainly $A \supset \ker f_A + B \supset B$, and

$$[A : B] = [A : \ker f_A + B] \cdot [\ker f_A + B : B]$$

By isomorphism theorems,

$$\frac{A}{\ker f_A + B} \;\approx\; \frac{\mathrm{im} f_A}{\mathrm{im} f_B}$$

and

$$\frac{\ker f_A + B}{B} \;\approx\; \frac{\ker f_A}{\ker f_A \cap B} \;=\; \frac{\ker f_A}{\ker f_B} \qquad ///$$

48. *The snake lemma and the Gamma function*

The *shortest long exact sequence* above has a surprising application in a different direction.

Euler's integral $\Gamma(s) = \int_0^\infty t^s\, e^{-t}\, \frac{dt}{t}$ converges for $\mathrm{Re}(s) > 0$. The usual way to see that $\Gamma(s)$ has an *meromorphic continuation* is to repeatedly integrate by parts.

However, the long exact sequence in homology shows that the values are completely determined from a suitable *characterization* of such integrals.

Rewrite the integral as an integral over the whole line, by replacing t by x^2:

$$\Gamma(s) \;=\; \int_0^\infty t^s\, e^{-t}\, \frac{dt}{t} \;=\; \int_{\mathbb{R}} |x|^{2s-1}\, e^{-x^2}\, dx$$

The Gaussian e^{-x^2} is in the Schwartz space $\mathscr{S}$ on $\mathbb{R}$, and for $\mathrm{Re}(\lambda) > 0$ the map $u_\lambda(\varphi) = \int_{\mathbb{R}} |x|^\lambda \, \varphi(x)\, dx$ is in the space $\mathscr{S}^*$ of continuous linear functionals on $\mathscr{S}$, that is, *tempered distributions*. While u_λ *can* be meromorphically continued as a tempered-distribution-valued function of λ, and this is indeed of interest, strikingly, *without* meromorphic continuation, u_λ is determined by the Snake Lemma, that is, by the long exact sequence in homology, as follows.

Observe that for $\mathrm{Re}(\lambda) \gg 1$, u_λ is differentiable, and $xu'_\lambda = \lambda \cdot u_\lambda$. That is, for such λ, u_λ is annihilated by

$$T_\lambda \;=\; x\frac{d}{dx} - \lambda$$

Let $\mathscr{S}_o$ be the space of Schwartz functions *vanishing to infinite order* at 0, and $\mathscr{S}_o^*$ its dual.

Let v_λ be u_λ restricted to $\mathscr{S}_o$, where the integral converges for *all* $\lambda \in \mathbb{C}$. That is, v_λ is *entire* as a function of λ.

We wish to *extend* v_λ from $\mathscr{S}_o$ to S, thus *continuing* u_λ outside the region of convergence of the integral.

Characterize u_λ and v_λ as being solutions of the equation $T_\lambda u = 0$.

Thus, in the surjection $\mathscr{S}^* \to \mathscr{S}_o^*$, we want $u_\lambda \in \mathscr{S}^*$ mapping to v_λ *and* $u_\lambda \in \ker T_\lambda$. Further, we hope that the extension u_λ is *unique*.

The space $X = \ker(\mathscr{S}^* \to \mathscr{S}_o^*)$ consists of distributions supported at 0. By the theory of Taylor-Maclaurin expansions, X is finite linear combinations of Dirac δ and its derivatives.

Consider the commutative diagram

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & X \arrow[r] \arrow[d, "T_\lambda"'] & \mathscr{S}^* \arrow[r] \arrow[d, "T_\lambda"'] & \mathscr{S}_o^* \arrow[r] \arrow[d, "T_\lambda"'] & 0 \\
0 \arrow[r] & X \arrow[r] \arrow[d] & \mathscr{S}^* \arrow[r] \arrow[d] & \mathscr{S}_o^* \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

We have $v_\lambda \in \ker T_\lambda\big|_{\mathscr{S}_o^*}$, and want *unique* $u_\lambda \in \ker T_\lambda\big|_{\mathscr{S}^*}$ surjecting to v_λ. The long exact sequence exactly gives the criterion: the not-so-long long exact sequence is

$$\begin{tikzcd}
0 \arrow[r] & \ker T_\lambda|_X \arrow[r] & \ker T_\lambda\big|_{\mathscr{S}_o^*} \arrow[r] & \ker T_\lambda\big|_{\mathscr{S}^*} \arrow[dll] & \\
 & \dfrac{X}{T_\lambda X} \arrow[r] & \dfrac{\mathscr{S}_o^*}{T_\lambda \mathscr{S}_o^*} \arrow[r] & \dfrac{\mathscr{S}^*}{T_\lambda \mathscr{S}^*} \arrow[r] & 0
\end{tikzcd}$$

The part of interest is

$$\begin{tikzcd}
0 \arrow[r] & \ker T_\lambda|_X \arrow[r] & \ker T_\lambda\big|_{\mathscr{S}_o^*} \arrow[r] & \ker T_\lambda\big|_{\mathscr{S}^*} \arrow[r] & \dfrac{X}{T_\lambda X}
\end{tikzcd}$$

Thus, $v_\lambda \in \ker T|_{\mathscr{S}_o^*}$ is assured to be in the image of $\ker T_\lambda|_{\mathscr{S}^*}$ when $X/T_\lambda X = 0$, and *uniquely* so when $\ker T_\lambda|_X = 0$.

[48.1] Remark: We reach these conclusions without knowing the details of the *connecting homomorphism*, or of the other (more elementary) maps.

Thus, the desired u_λ *exists* when $X/T_\lambda X = 0$, that is, when $T_\lambda X = X$, and is *unique* when $T_\lambda u = 0$ has no non-trivial solution in X.

For test function φ

$$(x\frac{d}{dx}\delta)(\varphi) \;=\; (\frac{d}{dx}\delta)(x\varphi) \;=\; -\delta(\frac{d}{dx}x\varphi)$$

$$=\; -x\Big|_{x=0}\cdot\varphi'(0) - \frac{dx}{dx}\Big|_{x=0}\cdot\varphi(0) \;=\; \varphi(0) \;=\; \delta(\varphi)$$

That is, $x\frac{d}{dx}\delta = -\delta$. By induction, $x\frac{d}{dx}\delta^{(n)} = -(n+1)\cdot\delta^{(n)}$.

Thus, u_λ exists and is unique for $\lambda \notin \{-1,-2,-3,\ldots\}$. Thus, $\Gamma(s) = u_{2s-1}(e^{-x^2})$ *certainly* exists for $s \notin \{0,-\frac{1}{2},-1,-\frac{3}{2},-2,\ldots\}$.

[48.2] Remark: This incorrectly indicates potential trouble at negative half-integers. To see that there is no such trouble, further information about the maps in the long exact sequence is needed.

49. *Local cyclic norm index theorem*

(Also, see Lang, p. 187 ff.)

[49.1] Theorem: For a cyclic extension K/k of degree n of local fields, with Galois group $G = \langle\sigma\rangle$ and ramification index e, integers $\mathfrak{o}\subset k$ and $\mathfrak{O}\subset K$, we have

$$[k^\times : N_k^K K^\times] \;=\; n \qquad [\mathfrak{o}^\times : N_k^K \mathfrak{O}^\times] \;=\; e$$

Proof: Apply the Herbrand quotient lemma to

$$0 \longrightarrow \mathfrak{O}^\times \longrightarrow K^\times \longrightarrow \mathbb{Z} \longrightarrow 0$$

where $\mathrm{ord} : K^\times \to \mathbb{Z}$. Since Galois preserves $|\cdot|_K$, the action of G on this copy of $\mathbb{Z}$ is *trivial.* Thus,

$$\ker t|_{\mathbb{Z}} \;=\; \{0\} \qquad \mathrm{im} t|_{\mathbb{Z}} \;=\; n\cdot\mathbb{Z}$$

and

$$\ker(\sigma-1)|_{\mathbb{Z}} \;=\; \mathbb{Z} \qquad \mathrm{im}(\sigma-1)|_{\mathbb{Z}} \;=\; 0$$

so

$$q_{\sigma-1,t}(\mathbb{Z}) \;=\; \frac{[\ker(\sigma-1)|_{\mathbb{Z}} : \mathrm{im} t|_{\mathbb{Z}}]}{[\ker t|_{\mathbb{Z}} : \mathrm{im}(\sigma-1)|_{\mathbb{Z}}]} \;=\; \frac{[\mathbb{Z} : n\cdot\mathbb{Z}]}{[\{0\} : \{0\}]} \;=\; n$$

Theorem 90 is $\ker t|_{K^\times} = \mathrm{im}(\sigma-1)|_{K^\times}$. Thus,

$$q_{\sigma-1,t}(K^\times) \;=\; \frac{[\ker(\sigma-1)|_{K^\times} : \mathrm{im} t|_{K^\times}]}{[\ker t|_{K^\times} : \mathrm{im}(\sigma-1)|_{K^\times}]}$$

$$=\; \frac{[k^\times : N_k^K K^\times]}{1} \;=\; [k^\times : N_k^K K^\times]$$

Thus, the Herbrand Lemma gives

$$n \;=\; q_{\sigma-1,t}(\mathbb{Z}) \;=\; \frac{q_{\sigma-1,t}(K^\times)}{q_{\sigma-1,t}(\mathfrak{O}^\times)} \;=\; \frac{[k^\times : N_k^K K^\times]}{q_{\sigma-1,t}(\mathfrak{O}^\times)}$$

We show that $q_{\sigma-1,t}(\mathfrak{O}^\times) = 1$.

There is a *normal basis* $x_1, \ldots, x_n$ for K/k, that is, G acts transitively on the x_i. Multiply every x_i by the same sufficiently high power of a local parameter in k to preserve the normal basis property, and to put all the x_i inside a sufficiently high power of the maximal ideal in $\mathfrak{O}$ such that the exponential map is defined on $V = \sum_i \mathfrak{o} x_i$, and inverse given by logarithm is defined on its image $U = \exp V$.

[49.2] Claim: $\ker(\sigma-1)|_V = \mathrm{im} t|_V$ and $\ker t|_V = \mathrm{im}(\sigma-1)|_V$.

Proof: (of claim) With $(\sigma-1)\sum_i c_i x_i = 0$ with $c_i \in k$, all coefficients are the same, by transitivity. On the other hand, if the coefficients are the same, certainly the element is in $\ker(\sigma-1)$. Application of t to $c_1 x_1$ produces all elements with identical coefficients. Thus, $\ker(\sigma-1)|_V = \mathrm{im} t|_V$. This is one equality.

For the other equality, index so that $x_i = \sigma^{i-1}(x_1)$. Vanishing $t \cdot \sum_i c_i x_i = 0$ is exactly $(\sum_i c_i)(\sum_i x_i) = 0$, which is $\sum_i c_i = 0$. Then

$$\sum_i c_i x_i \;=\; \sum_i c_i(x_i - x_1) \;=\; \sum_i c_i(\sigma^{i-1}-1)x_1 \;\in\; (\sigma-1)\sum_i \mathfrak{o} x_i$$

so $\ker t|_V = \mathrm{im}(\sigma-1)|_V$. ///

Since the Galois action is *continuous* on K, it commutes with exp and log where the series converge. Thus, $V = \exp U$ is a G-module with the same Herbrand-related quotients as U, namely

$$\ker(\sigma-1)|_U = \mathrm{im} t|_U \qquad \text{and} \qquad \ker t|_U = \mathrm{im}(\sigma-1)|_U$$

Since $[\mathfrak{O}^\times : U] < \infty$, by the Lemma $q_{\sigma-1,t}(\mathfrak{O}^\times/U) = 1$, and, again by the Herbrand Lemma,

$$1 \;=\; q_{\sigma-1,t}(V) \;=\; q_{\sigma-1,t}(U) \;=\; \frac{q_{\sigma-1,t}(\mathfrak{O}^\times)}{q_{\sigma-1,t}(\mathfrak{O}^\times/U)} \;=\; q_{\sigma-1,t}(\mathfrak{O}^\times)$$

From this,

$$1 \;=\; q_{\sigma-1,t}(\mathfrak{O}^\times) \;=\; \frac{[\mathfrak{o}^\times : N_k^K \mathfrak{O}^\times]}{[\ker t|_{\mathfrak{O}^\times} : \mathrm{im}(\sigma-1)|_{\mathfrak{O}^\times}]}$$

Since $|\sigma x/x| = 1$, by Theorem 90, $\ker t|_{\mathfrak{O}^\times} = \mathrm{im}(\sigma-1)|_{K^\times}$. Thus,

$$[\ker t|_{\mathfrak{O}^\times} : \mathrm{im}(\sigma-1)|_{\mathfrak{O}^\times}] \;=\; [\mathrm{im}(\sigma-1)|_{K^\times} : \mathrm{im}(\sigma-1)|_{\mathfrak{O}^\times}]$$

$$=\; [\mathrm{im}(\sigma-1)|_{K^\times} : \mathrm{im}(\sigma-1)|_{k^\times \mathfrak{O}^\times}]$$

Using $[A : B] = [\ker f|_A : \ker f|_B] \cdot [\mathrm{im} f|_A : \mathrm{im} f|_B]$ for $A \supset B$, this is

$$\frac{[K^\times : k^\times \mathfrak{O}^\times]}{[\ker(\sigma-1)|_{K^\times} : \ker(\sigma-1)|_{k^\times \mathfrak{O}^\times}]}$$

Essentially by definition, $[K^\times : k^\times \mathfrak{O}^\times] = e$, and

$$[\ker(\sigma-1)|_{K^\times} : \ker(\sigma-1)|_{k^\times \mathfrak{O}^\times}] \;=\; [k^\times : k^\times] \;=\; 1$$

so $[\ker t|_{\mathfrak{O}^\times} : \mathrm{im}(\sigma-1)|_{\mathfrak{O}^\times}] = e$.

Thus,

$$1 \;=\; \frac{[\mathfrak{o}^\times : N_k^K \mathfrak{O}^\times]}{[\ker t|_{\mathfrak{O}^\times} : \mathrm{im}(\sigma-1)|_{\mathfrak{O}^\times}]} \;=\; \frac{[\mathfrak{o}^\times : N_k^K \mathfrak{O}^\times]}{e}$$

and the cyclic local norm index theorem is done. ///

Elementary abelian group theory and induction give

[49.3] Corollary: *For finite abelian extension K/k of local fields,*

$$[k^\times : N_k^K K^\times] \le [K:k] \qquad \text{and} \qquad [\mathfrak{o}^\times : N_k^K \mathfrak{O}^\times] \le e \qquad ///$$

[49.4] Remark: Local classfield theory asserts *equalities* here for *all* finite abelian extensions, not only cyclic.

50. *More cohomology, statements of theorems*

In fact, we have not completed *any* proof of the main results of local or global classfield theory, although the Herbrand quotient discussion and discussion of long exact sequences from short exact sequences of *complexes* are essential for almost any sensible proof.

With considerable effort, we have proven $[K:k] = [k^\times : N_k^K K^\times]$ for *cyclic* local field extensions.

We will state some of the main theorems of classfield theory in modern form, and discuss them afterward, but proofs still will not be complete.

Write $G_{K/k} = \mathrm{Gal}(K/k)$. For an extension K/k of local fields with $[K:k] = n$, $H^2(G_{K/k}, K^\times)$ is *cyclic* of order n, and contains a unique generator, the **canonical class** $u_{K/k}$ which under the *Brauer invariant* map $H^2(G_{K/k}, K^\times) \to \mathbb{Q}/\mathbb{Z}$ maps to $1/n$.

[50.1] Theorem: *For $q \in \mathbb{Z}$, the cup-product $\alpha \to \alpha \cdot u_{K/k}$ on Tate cohomology $\widehat{H}^q(G_{K/k}, \mathbb{Z}) \to \widehat{H}^{q+2}(G_{K/k}, K^\times)$ is an isomorphism.*

In particular, for $q = -2$, $\widehat{H}^{-2}(G, \mathbb{Z})$ is ordinary group homology $H_1(G, \mathbb{Z})$, and $H_1(G, \mathbb{Z}) = G/G^{\mathrm{der}} = G^{\mathrm{ab}}$. Also, $\widehat{H}^0(G_{K/k}, K^\times) = k^\times / N_k^K K^\times$, so:

Corollary/Definition: the *inverse reciprocity map* or *inverse norm residue symbol* $\alpha_{K/k}^{-1} : \alpha \to \alpha \cdot u_{K/k}$ is an *isomorphism* $\mathrm{Gal}(K/k)^{\mathrm{ab}} \to k^\times / N_k^K K^\times$.

Local Existence Theorem: Given an open finite-index subgroup U of $k^\times$, there is a unique abelian K/k with $N_k^K K^\times = U$.

[50.2] Remark: Because the (inverse) reciprocity map is given by cup product with a canonical element, for $L \supset K \supset k$, some diagrams will obviously commute. Further, for *groundfields* $k \subset k' \subset K$,

$$\begin{tikzcd} k^\times \arrow[r, "\alpha_{K/k'}"] \arrow[d, "\mathrm{inc}"'] & \mathrm{Gal}(K/k)^{\mathrm{ab}} \arrow[d, "V"] \\ k'^\times \arrow[r, "\alpha_{K/k'}"] & \mathrm{Gal}(K/k')^{\mathrm{ab}} \end{tikzcd}$$

where V is the *Verlagerung*, or *transfer* (below...) In fact, this may provide a minor motivation to understand *transfer*.

Global:

[50.3] Lemma: *For all $w|v$ in K_w/k_v, the groups $H^q(G_{K_w/k_v}, K_w^\times)$ are canonically isomorphic to each other, so we identify them. Then*

$$\widehat{H}^q(G_{K/k}, \mathbb{J}_K) \approx \coprod_v \widehat{H}^q(G_{K_w/k_v}, K_w^\times)$$

[50.4] Corollary: $H^1(G_{K/k}, \mathbb{J}_K) = 0$ and

$$H^2(G_{K/k}, \mathbb{J}_K) \approx \coprod_v \frac{1}{n_v}\mathbb{Z}\Big/\mathbb{Z} \qquad\qquad (\text{with } n_v = [K_w : k_v])$$

[50.5] Proposition: $(\mathbb{J}_K/K^\times)^{\mathrm{Gal}(K/k)} = \mathbb{J}_k/k^\times$

[50.6] Theorem: With Herbrand quotient $q(G, A) = |H^2(A)|/|H^1(A)|$ of G-module A, for *cyclic* K/k, $q(G_{K/k}, \mathbb{J}_K/K^\times) = n$.

[50.7] Corollary: For K/k cyclic of degree n, $|\mathbb{J}_k/k^\times N_k^K \mathbb{J}_K| \geq n$.

[50.8] Remark: This was formerly the *second* inequality, but by 1960's became the *first* inequality.

[50.9] Corollary: For $N_k^K \mathbb{J}_K \subset U \subset \mathbb{J}_k$ and $k^\times U$ dense in $\mathbb{J}_k$, necessarily $K = k$.

[50.10] Corollary: (For finite abelian K/k), for S any finite set of primes containing ramified primes, $\mathrm{Gal}(K/k)$ is generated by Frobenius elements from primes *not* in S.

[50.11] Corollary: There are infinitely-many primes outside S which do *not* split completely.

[50.12] Theorem: *(second/other inequality)* the orders of $\widehat{H}^0(G_{K/k}, \mathbb{J}_K/K^\times)$ and $\widehat{H}^2(G_{K/k}, \mathbb{J}_K/K^\times)$ divide $[K : k]$, and $\widehat{H}^1(G_{K/k}, \mathbb{J}_K/K^\times) = 0$.

[50.13] Theorem: The global reciprocity law map is the product of the local ones (as earlier), so is a product of cup-product maps in cohomology.

[50.14] Some explanations... if not proofs...

Tate cohomology of finite groups: Fitting into the Herbrand quotient situation, a finite cyclic group $G = \langle\sigma\rangle$ with $t = \sum_{g\in G} g$ attaches to every G-module A a *periodic complex*

$$\begin{tikzcd} \ldots \arrow[r, "\sigma-1"] & A \arrow[r, "t"] & A \arrow[r, "\sigma-1"] & A \arrow[r, "t"] & \ldots \end{tikzcd}$$

with (co-)homology $\ker(\sigma-1)|_A/\mathrm{im}t|_A$ and $\ker t|_A/\mathrm{im}(\sigma-1)|_A$. Of course, $\ker(\sigma-1)|_A = A^G$. It is standard to define *Tate cohomology* for finite cyclic G by

$$\widehat{H}^n(G, A) \;=\; \begin{cases} \dfrac{A^G}{\mathrm{im}t|_A} & (n \text{ even}) \\[2ex] \dfrac{\ker t|_A}{\mathrm{im}(\sigma-1)|A} & (n \text{ odd}) \end{cases}$$

[50.15] Remark: Tate cohomology is defined for all $n \in \mathbb{Z}$. The hat does not mean *completion* or *dual*: it is merely a distinguishing mark.

More generally: for merely *finite* G and G-module A, for reasons that are not instantly clear, Tate cohomology is defined as follows. Let $t = \sum_{g\in G} g$ be the *trace/norm* element as before, and I_G the *augmentation ideal* in $\mathbb{Z}[G]$ generated by $g-1$ for all $g \in G$. Tate cohomology is

$$\widehat{H}^n(G,A) \;=\; \begin{cases} H^n(G,A) & (\text{for } n \ge 1) \\ \dfrac{A^G}{\mathrm{im} t|_A} & (n=0) \\ \dfrac{\ker t|_A}{I_G \cdot A} & (n=-1) \\ H_{1+|n|}(G,A) & (\text{for } n \le -2) \end{cases}$$

where (!?!) $H^n(G,A)$ with $n \ge 0$ is *group cohomology* and $H_n(G,A)$ with $n \ge 0$ is *group homology*, defined as follows.

To begin, the 0^{th} cohomology and homology are just *fixed* and *cofixed* vectors: $H^0(G,A) = A^G$ and $H_0(G,A) = A_G$.

The *functor* $A \rightsquigarrow A^G$ is *left-exact* in that, provably,

$$0 \to A \to B \to C \to 0 \;\text{ exact} \quad \Longrightarrow \quad 0 \to A^G \to B^G \to C^G \;\text{ exact}$$

Dually, the *functor* $A \rightsquigarrow A_G = A/I_G A$ is *right-exact*:

$$0 \to A \to B \to C \to 0 \;\text{ exact} \quad \Longrightarrow \quad A_G \to B_G \to C_G \to 0 \;\text{ exact}$$

These one-sided exactnesses can be proven directly, but are also corollaries of the *adjunction*

$$\mathrm{Hom}_G(A_G, B) \;\approx\; \mathrm{Hom}_G(A, B^G)$$

and the general fact that *left adjoints like $LA = A_G$ are right exact,* and *right adjoints like $RB = B^G$ are left exact.*

For fixed G, the higher cohomology and homology functors $A \rightsquigarrow H^n(A)$ and $A \rightsquigarrow H_n(A)$ are characterized as the *universal* things that from a short exact sequence $0 \to A \to B \to C \to 0$ produce one-sided *long exact sequences completing* $0 \to A^G \to B^G \to C^G$ and $A_G \to B_G \to C_G \to 0$

$$\begin{tikzcd}
0 \arrow[r] & A^G \arrow[r] & B^G \arrow[r] & C^G \arrow[r] & H^1(A) \arrow[dllll] \\
H^1(B) \arrow[r] & H^1(C) \arrow[r] & H^2(A) \arrow[r] & H^2(B) \arrow[r] & H^2(C) \arrow[dllll] \\
H^3(A) \arrow[r] & H^3(B) \arrow[r] & H^3(C) \arrow[r] & H^4(A) \arrow[r] & \ldots
\end{tikzcd}$$

in cohomology, and for homology going in the opposite direction:

$$\begin{tikzcd}
H^1(C) \arrow[r] & A_G \arrow[r] & B_G \arrow[r] & C_G \arrow[r] & 0 \\
H^2(A) \arrow[r] & H^2(B) \arrow[r] & H^2(C) \arrow[r] & H^1(A) \arrow[r] & H^1(B) \arrow[ullll] \\
\ldots \arrow[r] & H^4(C) \arrow[r] & H^3(A) \arrow[r] & H^3(B) \arrow[r] & H^3(C) \arrow[ullll]
\end{tikzcd}$$

In both cases, *naturality* is required, meaning that a map of *short exact sequences*

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] \arrow[d] & B \arrow[r] \arrow[d] & C \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & A' \arrow[r] & B' \arrow[r] & C' \arrow[r] & 0
\end{tikzcd}$$

gives a map of long-exact sequences:

In cohomology,

$$\begin{tikzcd}
0 \arrow[r] & A^G \arrow[r] \arrow[d] & B^G \arrow[r] \arrow[d] & C^G \arrow[r] \arrow[d] & H^1(A) \arrow[r] \arrow[d] & \ldots \\
0 \arrow[r] & A'^G \arrow[r] & B'^G \arrow[r] & C'^G \arrow[r] & H^1(A') \arrow[r] & \ldots
\end{tikzcd}$$

and for homology

$$\begin{tikzcd}
\ldots \arrow[r] & H^1(C) \arrow[r] \arrow[d] & A_G \arrow[r] \arrow[d] & B_G \arrow[r] \arrow[d] & C_G \arrow[r] \arrow[d] & 0 \\
\ldots \arrow[r] & H^1(C') \arrow[r] & A'_G \arrow[r] & B'_G \arrow[r] & C'_G \arrow[r] & 0
\end{tikzcd}$$

Any functors like H^n and H_n that fit into such diagrams are **δ-functors**.

Finally, the H^n's and H_n's are characterized as **universal** δ-functors extending $A \rightsquigarrow A^G$ and $A \rightsquigarrow A_G$: for any other collection T^n extending H^n or T_n extending H_n, there are unique $H^n(A) \to T^n(A)$ or $T_n(A) \to H_n(A)$ such that for all $0 \to A \to B \to C \to 0$, there are maps between long exact sequences, in cohomology

$$\begin{tikzcd}
\ldots \arrow[r] & H^n \arrow[r] \arrow[d] & H^n(B) \arrow[r] \arrow[d] & H^n(C) \arrow[r] \arrow[d] & \ldots \\
\ldots \arrow[r] & T^n \arrow[r] & T^n(B) \arrow[r] & T^n(C) \arrow[r] & \ldots
\end{tikzcd}$$

and in homology

$$\begin{tikzcd}
\ldots \arrow[r] & T_n \arrow[r] \arrow[d] & T_n(B) \arrow[r] \arrow[d] & T_n(C) \arrow[r] \arrow[d] & \ldots \\
\ldots \arrow[r] & H_n \arrow[r] & H_n(B) \arrow[r] & H_n(C) \arrow[r] & \ldots
\end{tikzcd}$$

... lots more remains to be said...

Bibliography

[Artin-Tate 1952/67] E. Artin, J. Tate, *Classfield theory*, 1952 seminar notes, Benjamin 1967, republished AMS-Chelsea 2008.

[Bergstrom 1953] H. Bergstrom, review of [Mordell 1953], Math. Reviews MR0058649.

[Besicovitch 1940] A.S. Besicovitch, *On the linear independence of fractional powers of integers*, J. Lond. Math. Soc. **15** (1940), 3-6.

[Cohen 2007] H. Cohen, *Number Theory: Volume I, Tools and Diophantine Equations*, ... *Volume II, Analytic and Modern Tools*, Springer-Verlag, 2007.

[Dedekind 1871] R. Dedekind, *Über die Theorie der ganzen algebraischen Zahlen. X*, supplement to P.G.L. Dirichlet's *Vorlesungen über Zahlentheorie*, 2nd ed., Vieweg, Braunschweig, 1871. Fourth edition 1894.

[Dubuque 2011] W. Dubuque's answer to math.stackexchange.com/questions/30687, retrieved 22 Dec 2011.

[Edwards 1974] H.M. Edwards, *Riemann's zeta function*, Academic Press, New York, 1974.

[Eisenstein 1850] G. Eisenstein, *Über en einfaches Mittel zur Auffindung der höheren Reciprocitätsgesetze und der mit ihnen zu verbindenden Ergänzungssätze*, J. reine angew. Math. **39** (1850), 351-364; *Mathematische Werke, II*, 623-636, Chelsea, New York, 1975.

[Gelfand-Graev-PS 1969] I. Gelfand, M. Graev, I. Piatetski-Shapiro, *Representation Theory and Automorphic Functions*, W.B. Saunders Co., Philadelphia, 1969.

[Godement Jacquet 1972] R. Godement, H. Jacquet, *Zeta functions of Simple Algebras*, Lecture Notes in Math. **260**, Springer-Verlag, 1972.

[Guinand 1947] A. P. Guinand, *Some Fourier transforms in prime-number theory*, Quart. J. Math., Oxford **18** (1947), 53-64.

[Hadamard 1893] J. Hadamard, *Étude sur les Propriétés des Fonctions Entières et en Particulier d'une Fonction Considérée par Riemann*, J. Math. Pures Appl. **9** (1893), 171-215.

[Hadamard 1896] J. Hadamard, *Sur la distribution des zéros de la fonction $\zeta(s)$ et ses conséquences arithmétiques*, Bull. Soc. Math. France **24** (1896), 199-220.

[Hasse 1933] H. Hasse, *Klassenkorpertheorie*, Marburg (1933), 187-195.

[HeathBrown-Patterson 1979] D.R. Heath-Brown, S.J. Patterson, *The distribution of Kummer sums at prime arguments*, J. reine und Angew. Math. **310** (1979), 111-130.

[Hecke 1918] E. Hecke, *Eine neue Art von Zetafunktionen und ihre Beziehungen der Verteilung der Primzahlen*, Math. Z. **1** no. 4 (1918), 357-376.

[Hecke 1920] E. Hecke, *Eine neue Art von Zetafunktionen und ihre Beziehungen der Verteilung der Primzahlen*, Math. Z. **6** no. 1-2 (1920), 11-51.

[Hilbert 1897] D. Hilbert, *Die theorie der algebraischen Zahlkörper*, Jahresbericht der Deutschen Math.-Vereinigung **4** (1897), 175-546.

[Iwasawa 1950/1952] K. Iwasawa, [brief announcement], in Proceedings of the 1950 International Congress of Mathematicians, Vol. 1, Cambridge, MA, 1950, 322, Amer. Math. Soc., Providence, RI, 1952.

[Iwasawa 1952/1992] K. Iwasawa, *Letter to J. Dieudonné*, dated April 8, 1952, in *Zeta Functions in Geometry*, editors N. Kurokawa and T. Sunada, Advanced Studies in Pure Mathematics **21** (1992), 445-450.

[Ivić 1985] A. Ivić, *The Riemann zeta function*, J. Wiley, New York, 1985.

[Iwaniec 2002] H. Iwaniec, *Spectral Methods of Automorphic Forms*, 2nd edition, AMS, Providence, 2002. [First edition, Revisto Mathematica Iberoamericana, 1995.]

[Jacquet-Langlands 1971] H. Jacquet and R. P. Langlands, *Automorphic forms on GL_2*, Lecture Notes in Mathematics **114**, Springer-Verlag, Berlin and New York, 1971.

[Jacquet-PS- Shalika 1979] H. Jacquet, I. Piatetski-Shapiro, and J. Shalika, *Automorphic forms on $GL(3)$*, Annals of Math. **109** (1979), 169-258.

[Koch 1997] H. Koch, *Number Theory: Algebraic Numbers and Functions*, AMS, 2000; translation by D. Kramer of *Zahlentheorie: Algebraische Zahlen und Funktionen*, F. Vieweg, Braunschweig/Wiesbaden, 1997.

[Kummer 1847] E. Kummer, *Über die Zerlegung der aus Wurzeln der Einheit gebildeten complexen Zahlen in ihtre Primfactoren*, J. reine angew. Math. **35** 91847), 327-367. *Collected Papers, I*, 211-251.

[Lagrange 1870] J. L. Lagrange, *Réflexions sur la résolution algébrique des équations*, 1770.

[Lang 1970] S. Lang, *Algebraic number theory*, Addison-Wesley, 1970.

[Lang 1978,80] S. Lang, *Cyclotomic Fields, I,II*, Springer-Verlag, 1978, 1980.

[vonMangoldt 1895] H. von Mangoldt, *Zu Riemann's Abhandlung 'Über die Anzahl der Primzahlen unter einer gegebenen Grösse'*, J. Reine Angew. Math. **114**, 255-305.

[Matchett 1946] M. Matchett, *On the Zeta Function for Ideles*, thesis, Indiana University, 1946.

[Mordell 1953] L.J. Mordell, *On the linear independence of algebraic numbers*, Pacific J. Math. **3** (1953), 625-630.

[O'Connor-Robertson 2001] J.J. O'Connor and E.F. Robertson, *Alexandre-Théophile Vandermonde*, http://www-history.mcs.st-and.ac.uk/Biographies/Vandermonde.html

[Patterson 1988] S. J. Patterson, *An introduction to the theory of the Riemann zeta function*, Cambridge University Press, 1988.

[de la Vallée-Poussin 1896] C.-L. de la Vallée-Poussin, *Recherches analytiques sur la théorie des nombres premiers*, Annales de la Société Scientifiques de Bruxelles 20B (1896), 183-256.

[Riemann 1859] B. Riemann, *Über die Anzahl der Primzahlen unter einer gegebenen Grösse*, Monats. Akad. Berlin (1859), 671-680.

[Stickelberger 1890] L. Stickelberger, *Über einer Verallgemeinerung der Kreistheilung*, Math. Ann. **37** (1890), 321-367.

[Tamagawa 1963] T. Tamagawa, *On the ζ-functions of a division algebra*, Ann. of Math. (2) **77** (1963), 387-405.

[Tate 1950/1967] J. Tate, *Fourier analysis in number fields and Hecke's zeta functions*, thesis, Princeton (1950), in *Algebraic Number Theory*, J. Cassels and J. Frölich, editors, Thompson Book Co., 1967.

[Titchmarsh 1951] E.C. Titchmarsh, *The theory of the Riemann zeta function*, Oxford University Press, 1951.

[Robinson 2011] G. Robinson's answer to math.stackexchange.com/questions/93453, retrieved 22 Dec 2011.

[Vandermonde 1771] A.-T. Vandermonde, *Memoire sur la resolution des équations*, Acad. Sci. Paris, 1771.

[Washington 1982], L. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, 1982.

[Weil 1940/1965] A. Weil, *L'intégration dans les groupes topologiques, et ses applications*, Hermann, Paris, 1940, second edition 1965.

[Weil 1952] A. Weil, *Sur les 'formules explicites' de la théorie des nombres premiers*, Comm. Lund (vol. dedié à Marcel Riesz) 252-265. (*Oeuvres sci.* [1952b], Vol. II, Springer, New York, 1979.)

[Weil 1972] A. Weil, *Sur les formules explicites de la théorie des nombres*, Izv. Akad. Nauk. (ser. Math.) **36** (1972), 3-18. (*Oeuvres sci.* [1972], Vol. III, Springer, New York, 1979.)