(*April 20, 2015*)

Euler, Raphson, Newton, Puiseux, Riemann, Hurwitz, Hensel

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

[This document is
http://www.math.umn.edu/~garrett/m/complex/notes_2014-15/12_ERNPRHH.pdf]

Just a draft!

1. Euler characteristic of triangulated surfaces
2. Riemann-Hurwitz theorem on ramified coverings
3. Locating ramified points
4. Newton polygons and ramification
5. Newton-Raphson/Hensel's lemma
6. Newton-Puiseux series and proofs

This is a sketch of some useful devices due to many, many people. [1]

A *Riemann surface* is a one-dimensional complex manifold. Here, we are interested only in *compact, connected* Riemann surfaces. The complex manifold structure implies (!) that these surfaces are *oriented*.

Riemann approximately proved that every compact, connected Riemann surface is a *projective algebraic curve*, but the *Dirichlet (minimum) principle* he invoked was literally incorrect. The literal falsity amounts to the fact that a convex, closed subset of a *Banach* space need not have a unique element of least norm: it may have none, or infinitely-many. This minimum principle is *true* in a *Hilbert* space, as was observed, in effect, by Beppo Levi in 1906, who also created a Hilbert space to capture some aspect of the differentiability of functions, a forerunner of Sobolev spaces.

The arguably most-natural spaces of continuous functions or k-fold differentiable functions on a compact space have natural structures of Banach spaces, so it is not surprising that these natural structures were thought to have the subtler properties needed for subtler applications. After Levi's 1906 work, we have understood the advantages of Hilbert-space re-constitution of more naive notions.

Granting Riemann's result, we consider *complex projective curves* X, that is, point sets in complex projective two-space $\mathbb{P}^2$ defined by a single *homogeneous* polynomial equation:

$$X \;=\; \{(x,y,z) \in \mathbb{P}^2 \;:\; P(x,y,z) \;=\; 0 \qquad (P \text{ homogeneous, irreducible in } \mathbb{C}[x,y,z])$$

Another latent problem is that such curves can have *singularities*, such as *self-intersections*, which are resolved by *blowing-up points* and creating non-singular curves in $\mathbb{P}^3$. But the complex-manifold property fails at a self-intersection point, so complex algebraic curves with self-intersections are not quite complex manifolds, and the Euler-characteristic computation can be harder to justify.

---

1. *Euler characteristics of surfaces*

Surface means a two-dimensional *topological* manifold, that is, every point has a neighborhood homeomorphic to an open in $\mathbb{R}^2$.

For a triangulated (connected, compact, oriented) surface with V vertices, E edges, and F faces, the *genus* (number of *handles*) is determined as an *Euler characteristic*

$$2 - 2g \;=\; V - E + F$$

[1] To name just a few: Leonard Euler, Joseph Raphson, Isaac Newton, Victor Puiseux, Bernard Riemann, Adolf Hurwitz, Kurt Hensel.

Euler approximately proved something in this direction. Making a precise assertion, and proving it, is non-trivial.

The classification of compact, connected, oriented surfaces by their *genus*, is non-trivial. The *idea* is that the surface is a *sphere with handles*, and the genus is the number of handles. It is not at all obvious that this is an adequate or correct description, although it is plausible, and was proven correct in the early 20th century.

For a compact, connected, oriented surface S, the genus is *half* the dimension of the first homology $H_1(S)$.

The Euler characteristic of a finite sequence of real vector spaces $V_0, V_1, V_2, \ldots$ is the alternative sum of dimensions:

$$\chi(V_0, V_1, V_2, \ldots) \;=\; \dim V_0 - \dim V_1 + \dim V_2 - \dim V_3 + \ldots$$

Letting V_i be the real vector space with basis consisting of i-dimensional simplices in a triangulation of a surface, we recover Euler's formula

$$\chi \;=\; \dim V_0 - \dim V_1 + \dim V_2 \;=\; V - E + F$$

However, one should reasonably worry that different triangulations could give different Euler characteristics. There is a re-expression of the Euler characteristic which is more reassuring that it is intrinsic:

The 0^{th} homology of a reasonable connected space is rank 1, as is the 2^{nd} homology of a compact, connected, oriented surface, and all higher homology is 0. This is not elementary, but granting this, the Euler characteristic of the sequence $H_0(S), H_1(S), H_2(S), \ldots$ can be rewritten as

$$\chi(H_0(S), H_1(S), H_2(S), \ldots) \;=\; \dim H_0(S) - \dim H_1(S) + \dim H_2(S) \;=\; 1 - 2g + 1 \;=\; 2 - 2g$$

---

2. *Riemann-Hurwitz theorem on ramified coverings*

For a degree-n *ramified cover* $\pi : Y \to X$ of compact, connected, Riemann surfaces, the genus g_Y of Y is related to the genus g_X of X by

$$2 - 2g_Y \;=\; n \cdot (2 - 2g_X) + \sum_{\text{ramified } y_o} (e_{y_o} - 1)$$

where the sum is over points $y \in Y$ *ramified* over X, and e_y is the ramification index of y over $\pi(y)$.

The idea of *ramification* is that, on a small-enough neighborhood of y_o, after a suitable change of coordinates, the map π is $\pi(y) = (y - y_o)^{e_{y_o}}$.

The easiest case is *hyper-elliptic* curves $y^2 = f(x)$ where f is a square-free polynomial in x. The square-free condition avoids *reducibility* of the curve. For example, $y^2 = x^2$ falls apart into two curves $y = x$ and $y = -x$. Further, these curves intersect at 0 and at ∞, so their union fails to be a manifold at those intersection points.

At x_o such that $f(x_o) \neq 0$, there are two *distinct* square roots $\pm y_o \neq 0$ of $f(x_o)$, and the derivative $\frac{\partial}{\partial y}(y^2 - f(x_o)) = 2y$ does not vanish at $y = y_o$. Thus, by the holomorphic inverse function theorem, there are two *holomorphic* square roots $\sqrt{f(x)}$ near $x = x_o$. In particular above x_o with $f(x_o) \neq 0$ there is *no ramification*.

At x_o with $f(x_o) = 0$, there is a unique y_o satisfying $y_o^2 = f(x_o)$, but this in itself is not quite proof of ramification, since we might have the misfortune of having a self-intersection. Fortunately, hyper-elliptic curves do not have self-intersections in the finite part $\mathbb{C}$ of $\mathbb{P}^1$, as we see:

Letting $f(x) = (x-x_1)\dots(x-x_n)$ with the x_j distinct, near x_1 the *other* factors *have* two distinct, holomorphic square roots. Thus, the equation can be rewritten

$$\Big(\frac{y}{\sqrt{(x-x_2)(x-x_3)\dots(x-x_n)}}\Big)^2 \;=\; x-x_1$$

which shows that there is ramification of index 2 above x_1.

Still looking at hyperelliptic $y^2 = f(x)$, to examing ramification at infinity, replace y by $1/y$ and x by $1/x$. For example, from $y^2 = x^5 - 1$ in coordinates at infinity, $(1/y)^2 = (1/x)^6 - 1$, which rearranges to $x^6 = y^2(1-x^6)$ or

$$y^2 \;=\; \frac{x^6}{1-x^6}$$

The right-hand side has two holomorphic square roots near $x = 0$, so there is *no ramification*. However, since both these local square root functions take value 0 at $x = 0$, there is a self-intersection of the curve.

In general, for $y^2 = f(x)$ with f square-free and *even* degree, there is no ramification at infinity, but there is self-intersection there. For f *odd* degree, there is ramification of index 2 at infinity. Thus,

[2.0.1] Corollary: For hyper-elliptic curves $\pi : Y \to \mathbb{P}^1$ given by $y^2 = f(x)$ with f a square-free polynomial of degree d in x, the Riemann-Hurwitz formula simplifies to

$$2-2g_Y \;=\; 2\cdot(2-2\cdot 0) - d - \begin{cases} 1 & (\text{for } d \text{ odd}) \\ 0 & (\text{for } d \text{ even}) \end{cases}$$

That is,

$$g_Y \;=\; \begin{cases} \dfrac{d-1}{2} & (\text{for } d \text{ odd}) \\ \dfrac{d-2}{2} & (\text{for } d \text{ even}) \end{cases}$$

---

3. *Locating ramified points*

The holomorphic inverse function theorem asserts that, for a polynomial $F(x,y)$ in two variables, at x_o, y_o satisfying $F(x_o,y_o) = 0$ and $\frac{\partial F}{\partial y}(x_o,y_o) \neq 0$, there is a holomorphic function $y = f(x)$ near x_o such that $f(x_o) = y_o$ and $F(x,f(x)) = 0$ for x sufficiently near x_o.

Determination of points x_o so that there is y_o satisfying $F(x_o,y_o) = 0$ and $\frac{\partial F}{\partial y}(x_o,y_o) = 0$ can be done systematically. View F as a polynomial $P(y) = F(x,y)$ in y with coefficients in the field of fractions $\mathbb{C}(x)$ of $\mathbb{C}[x]$. The ring $\mathbb{C}(x)[y]$ is a principal ideal domain, and in fact has a Euclidean algorithm, which produces a *greatest common divisor* $g(y) \in \mathbb{C}(x)[y]$ of $P(y), P'(y)$.

This *gcd* is of positive degree if and only if $P(y)$ has a repeated factor in $\mathbb{C}(x)[y]$, in which case $F(x,y) \in \mathbb{C}[x,y]$ is *reducible*, by Gauss' lemma. Then the curve defined by $F(x,y) = 0$ would be *reducible*, meaning that it is a proper union of two curves, which necessarily intersect, and we wish to exclude this case.

Thus, in all situations we wish to consider, the *gcd* is not identically $0 \in \mathbb{C}(x)$. Thus, it has finitely-many zeros in $\mathbb{C}$, and these are the only candidate points $x_o \in \mathbb{C}$ over which there may exist y_o satisfying $F(x_o,y_o) = 0$ but $\frac{\partial F}{\partial y}F(x_o,y_o) = 0$.

[3.0.1] Example: Consider $F(x,y) = y^3 + 3xy + x^3$. At $x = 0$ there is the obvious degeneration, but what else? Applying the Euclidean algorithm in $\mathbb{C}(x)[y]$ to $f(y) = F(x,y)$ and $f'(y) = 3y^2 + 3x$:

$$f(y) - \frac{y}{3}\cdot f'(y) \;=\; \Big(y^3+3xy+x^3\Big) - \frac{y}{3}\cdot\Big(3y^2+3x\Big) \;=\; 2xy + x^3$$

Division-with-remainder of $f'(y)$ by a linear (in y) polynomial $y-a$ produces a remainder equal to evaluation of $f'(a)$. Away from $x=0$, dividing by $2xy+x^3$ will produce the same remainder as dividing by $y+\frac{x^2}{2}$, namely, evaluation at $-x^2/2$:

$$\gcd(f(y), f'(y)) \;=\; f'(x^2/2) \;=\; 3\cdot((-x^2/2)^2+x) \;=\; \frac{3}{4}\cdot x\cdot(x^3+4)$$

Thus, in this example, in addition to $x=0$, the other points over which some ramification occurs are the cube roots of -4.

If we remember the symmetric-function computation determining the *discriminant* of a cubic y^3+by+c with roots α,β,γ

$$(\alpha-\beta)^2(\beta-\gamma)^2(\gamma-\alpha)^2 \;=\; -4b^3-27c^2$$

then we can check the outcome of the *gcd* computation: for $y^3+3xy+x^3$ the discriminant formula gives

$$\text{discriminant } y^3+3xy+x^3 \;=\; -4(3x)^3-27(x^3)^2 \;=\; -27x^3(4+x^3)$$

For x a cube root $-\sqrt[3]{4}$ of -4, the equation become $y^3-3\sqrt[3]{4}y-4=0$. In fact, the Euclidean algorithm above shows that when x is a cube root of -4, the linear (in y) factor $2xy+x^3=2x\cdot(y+\frac{x^2}{2})$ is the common factor of both $f(y)$ and $f'(y)$, meaning that $f(y)$ has a repeated root $y=-x^2/2$, appearing with multiplicity exactly 2. This computation also checks that the root is *not* of multiplicity 3, unlike the situation at $x=0$, where the equation degenerates into $y^3=0$.

Thus, there are two points y_1, y_2 lying over x_o a cube root of -4, and one of the two has ramification index 2, while the other is unramified.

---

4. *Newton polygons and ramification*

Newton polygons, described below, subsume *Eisenstein's criterion* for irreducibility as a very special case. More important for our purposes is the information they give about ramification.

To gain information about the ramification of $\pi: Y\to X$ described by a polynomial relation $F(x,y)=0$ at a point $\pi:(x_o,y_o)\to x_o$, first rewrite the relation as a monic polynomial in $y-y_o$, with coefficients in $\mathbb{C}(x)$:

$$(y-y_o)^n + c_{n-1}(x)(y-y_o)^{n_1} + \ldots + c_2(x)(y-y_o)^2 + c_1(x)(y-y_o) + c_o(x) \qquad (\text{with } c_j(x)\in\mathbb{C}(x))$$

Let $\text{ord}_{x-x_o} f(x)$ be the order of vanishing of a rational function $f(x)$, including the possibility that $f(x)$ has a pole, so the order can be negative.

Consider data points (i,j) with $j=j(i)\text{ord}_{x-x_o}\, c_{n-i}(x)$, putting $j=j(i)=+\infty$ if $c_{n-i}=0$. Consider piecewise-linear convex (bending upward) functions P on the interval $[0,n]$ such that for each integer i

$$P(i) \;\le\; j(i)$$

Let N be the *maximum* among these, and let $i_1<\ldots<i_m$ be the integer indices where *equality* occurs:

$$N(i_k) \;=\; \text{ord}\; c_{n-(i+k)}(x)$$

The line segements

$$\ell_k \;=\; \text{line segment connecting } N(i_k) \text{ and } N(i_{k+1})$$

form the *Newton polygon* attached to f.

Adjacent segments with the same slope are considered to be parts of a single segment.

For example, at $x_o = 0 = y_o$, the polynomial $y^5 + x^2y^3 + x(x+1)y + x^2$ has data points $(0,0)$, $(1,+\infty)$, $(2,+\infty)$, $(3,2)$, $(4,1)$, and $(5,2)$. Thus, the Newton polygon has vertices $(0,0)$, $(4,1)$, and $(5,2)$. The two points with second coordinate $+\infty$ certainly lie strictly above the Newton polygon, but also the point $(3,2)$ lies above it.

The precise content of the Newton polygon attached to a polynomial $f(x,y)$ will be discussed below. Here, we note some special corollaries in which the Newton polygon gives complete information about ramification. The first is parallel to the situation of Eisenstein's criterion, already generalizing it somewhat:

[4.0.1] Corollary: If the Newton polygon at x_o consists of a single segment with *rise* (change in vertical coordinate) and *run* (change in horizontal) *relatively prime*, then the covering is *totally ramified* over x_o, of degree equal to the horizontal length. (Proof below.)

For example, $y^5 + x^3y + x^2 = 0$ at $x = 0$ has a Newton polygon of slope $2/5$, so the ramification is *total*, the index is 5.

[4.0.2] Corollary: Every length-1 segment having *integer slope* indicates an *unramified* point (x_o, y_o) lying over x_o. That is, for each such segment, there is a holomorphic function y of x near x_o such that $y(x_o) = y_o$. (Proof below.)

For example, $y^5 + xy^2 + x^2y + x^4 = 0$ at $x = 0$ has a Newton polygon with three segments, one of length 3 and slope $1/3$, another of length 1 and slope 1, and another of length 1 and slope 2, so from the latter we see that there are two unramified points over $x = 0$.

[4.0.3] Corollary: Every segment whose *rise* n and *run* m are *relatively prime* indicates a point (x_o, y_o) ramified with index m over x_o. (Proof below.)

Thus, continuing with the previous example, in addition to the two unramified points over $x_o = 0$, there is exactly one other point, and it has ramification index 3.

When the rise and run of a segment are *not* relatively prime, there is ambiguity in the conclusion. For example, for $y^5 + xy^2 + x^3$ at $x = 0$, there is one segment of length 3 and slope $2/3$, indicating a point with ramification index 3, but the other segment has rise 2 and slope 2. Without further effort, we cannot tell whether there are two unramified points lying over x_o, or a further single point with ramification index 2. Via *Hensel's lemma*, below, we can determine that there are two unramified points in addition to the point with ramification index 3. That is, there are two distinct holomorphic functions y of x near x_o satisfying the equation.

---

5. *Newton-Raphson/Hensel's lemma*

The Newton-Raphson method, in the better form due to Raphson, approximates real roots of polynomials f in $\mathbb{R}[x]$ by iteratively sliding down the tangent from the value $f(x_n)$ at x_n to (what we hope is) an improved approximation

$$x_{n+1} \;=\; x_n - \frac{f(x_n)}{f'(x_n)}$$

In good situations, $\lim_n x_n$ is a root of $f(x) = 0$. In this incarnation, there is no advance assurance that a root *exists*, and even if a root is known to exist, there can be complications due to very small non-zero values, for example.

In contrast, the analogue for p-adic numbers, *Hensel's Lemma*, works much better! Here, we want an instance of an abstracted version of Hensel's Lemma, applicable to solving equations $F(x,y) = 0$ as above. Although these ideas admit further abstraction, for tangibility we consider a specific setting.

Namely, we consider the ring $\mathbb{C}[[x]]$ of *formal power series* in x. Formal power series are not *formal* in the pejorative sense of allegedly having no genuine meaning, or in any sense of asserted contentless-ness, despite

some sources' treatment of them as such. In terms of *notation*, a formal power series in $\mathbb{C}[[x]]$ is of the form

$$a_o + a_1 x + a_2 x^2 + a_3 x^3 + \dots \qquad \text{(with } a_j \in \mathbb{C}\text{)}$$

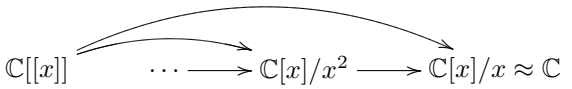
with no conditions on the growth of the coefficients a_j. The notational sense is clear, but the content or meaning is not adequately conveyed by a superficial appraisal of the notation.

One relatively elementary, concrete description of the formal power series ring $\mathbb{C}[[x]]$ as a genuine object is as the *completion* of the polynomial ring $\mathbb{C}[x]$ with respect to the x-adic metric, $|\cdot|_x$, defined by

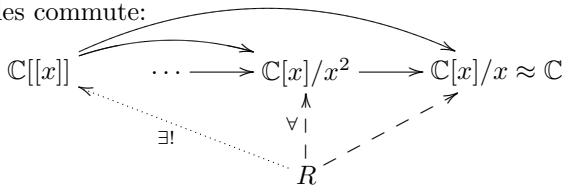
$$|x^n \cdot f(x)|_x \;=\; 2^{-n} \qquad \text{(for } f(x) \in \mathbb{C}[x] \text{ prime to } x\text{)}$$

Any other constant > 1 will do in place of the 2. That is, polynomials highly divisible by x are small.

A slightly less elementary characterization, more useful in the long run, is that $\mathbb{C}[[x]]$ is the (projective) *limit* of the quotient rings $\mathbb{C}[x]/x^n \cdot \mathbb{C}[x]$. That is, first, there are commutative ring homomorphisms $\mathbb{C}[[x]] \to \mathbb{C}[x]/x^n$ for all n, sending 1 to 1, and *compatible* in the sense that all triangles commute:



Second, for all *compatible* families of commutative ring homomorphisms $R \to \mathbb{C}[x]/n$ there is a unique $R \to \mathbb{C}[[x]]$ making all triangles commute:



These two descriptions produce the same object $\mathbb{C}[[x]]$.

The field of fractions of $\mathbb{C}[[x]]$, denoted $\mathbb{C}((x))$, is (provably) the ring of *finite-nosed* formal Laurent expansions. In fact, there is only one ring element needing an inverse, x, so

$$\mathbb{C}((x)) \;=\; \mathbb{C}[[x]][\frac{1}{x}]$$

Analogously the ring of p-adic integers $\mathbb{Z}_p$ is a metric completion of $\mathbb{Z}$ with respect to the p-adic metric $|p^n \cdot \frac{a}{b}|_p = p^{-n}$ with a, b prime to p. Also, $\mathbb{Z}_p$ is the limit of quotients $\mathbb{Z}/p^n$. The field of fractions $\mathbb{Q}_p$ is $\mathbb{Z}_p[1/p]$, since p is the only non-unit.

[5.0.1] Claim: *(Simplest Hensel's lemma)* For monic $f(Y) \in \mathbb{C}[[x]][Y]$, if $y_o \in \mathbb{C}[[x]]$ is such that $f(y_o) = 0 \bmod x$ but $f'(y_o) \neq 0 \bmod x$, then the recursion

$$y_{n+1} \;=\; y_n - \frac{f(y_n)}{f'(y_n)}$$

converges in $\mathbb{C}[[x]]$ to a solution y of $f(y) = 0$, and $y = y_o \bmod x$.

Proof:

///

[5.0.2] Claim: *(Next-simplest Hensel's lemma)* For monic $f(Y) \in \mathbb{C}[[x]][Y]$, if $y_o \in \mathbb{C}[[x]]$ is such that the x-adic norm $|f(y_o)/f'(y_o)^2|_x$ (note that the denominator is squared!) satisfies $|f(y_o)/f'(y_o)^2|_x$, then the recursion

$$y_{n+1} \;=\; y_n - \frac{f(y_n)}{f'(y_n)}$$

converges in $\mathbb{C}[[x]]$ to a solution y of $f(y) = 0$, and $y = y_o \bmod x$.

Proof:

///

[5.0.3] Claim: *(Another Hensel's lemma)* For monic $f(Y) \in \mathbb{C}[[x]][Y]$, if $f(Y) = g_o(Y) \cdot h_o(Y) \bmod x$ for *relatively prime*, monic $g_o(Y), h_o(Y) \in \mathbb{C}[Y]$, then there is a recursion to obtain relatively prime, monic $g(Y), h(Y) \in \mathbb{C}[[x]](Y)$ such that $g(Y) = g_o(Y) \bmod x$, $h(Y) = h_o(Y) \bmod x$, and $f(Y) = g(Y) \cdot h(Y)$

Proof:

///

[5.1] Mild pathology

$$y^2(y-1)^2 + xy + x \;=\; 0$$

has no roots y in $\mathbb{C}[[x]]$, because mod x it is

$$y^2(y-1)^2 \;=\; 0 \qquad\qquad (\bmod\ x)$$

Mod x^2, trying $y = ax$, it gives an impossible equation

$$x \;=\; 0 \qquad\qquad (\bmod\ x^2)$$

and similarly for $y = 1 + ax$. If we try to use the simplest form of Hensel's lemma, starting with $y_o = 0$,

$$y_o$$

---

6. *Newton polygons*

[6.0.1] Corollary: Let m_j be the slope of ℓ_j, and let p_j be the length of the projection of ℓ_j to the horizontal axis. Then there are exactly p_j roots of f in $\mathbb{C}[[x - x_o]]k_{\text{sep}}$ with ord equal to m_j.

Proof: Let $\nu_1 < \ldots < \nu_m$ be the distinct ords of the roots, and suppose that there are exactly μ_i roots with ord ν_i. Let σ_j be the j^{th} symmetric function of the roots, so $c_i = \pm\sigma_i$.

Let $\rho_1, \ldots, \rho_{\mu_1}$ be the roots with largest ord. Since

$$\sigma_{\mu_1} = \rho_1 \ldots \rho_{\mu_1} + (\text{other products})$$

where the other products of μ_1 factors have strictly smaller ords. By the ultrametric inequality,

$$\text{ord}(\sigma_{\mu_1}) = \text{ord}(\rho_1 \ldots \rho_{\mu_1}) = \mu_1\nu_1$$

Similarly, let $\tau_1, \ldots, \tau_{\mu_2}$ be the second-largest batch of roots, namely, roots with ord ν_2. Then

$$\sigma_{\mu_1+\mu_2} = \rho_1 \ldots \rho_{\mu_1}\tau_1 \ldots \tau_{\mu_2} + (\text{other products})$$

where all the other products have strictly smaller ord. Again by the ultrametric inequality

$$\text{ord}(\sigma_{\mu_1+\mu_2}) = \text{ord}(\rho_1 \ldots \rho_{\mu_1}\tau_1 \ldots \tau_{\mu_2}) = \mu_1\nu_1 + \mu_2\nu_2$$

Generally,

$$\mathrm{ord}(\sigma_{\mu_1+\ldots+\mu_j}) = \mu_1\nu_1 + \ldots + \mu_j\nu_j$$

Therefore, the line segment connecting $N(n-\mu_1-\ldots-\mu_j)$ and $N(n-\mu_1-\ldots-\mu_{j+1})$ has slope $-\nu j+1$ and the projecting to the horizontal axis has length μ_{j+1}.

On the other hand, for

$$\mu_1\nu_1 + \ldots + \mu_j\nu_j < M < \mu_1\nu_1 + \ldots + \mu_{j+1}\nu_{j+1}$$

by the ultrametric inequality

$$\mathrm{ord}M \geq \min\left(\text{ord of products of } M \text{ roots}\right) = \mu_1\nu_1 + \ldots + \mu_j\nu_j + (M-\mu_1-\ldots-\mu_j)\nu_{j+1}$$

That is, $N(n-M)$ lies on or above the line segment connecting the two points $N(n-\mu_1-\ldots-\mu_j)$ and $N(n-\mu_1-\ldots-\mu_{j+1})$. ///

[6.0.2] Corollary: *(Irreducibility criterion)* Let f be monic of degree n over an ultrametric local field k as above. Suppose that the Newton polygon consists of a single line segment of slope $-a/n$ where a is relatively prime to n. Then f is irreducible in $k[x]$.

Proof: By the theorem, there are n roots of ord a/n. Since a is prime to n, the field $k(\alpha)$ generated over k by any one of these roots has ramification index divisible by n, by the following lemma, for example. But $[k(\alpha):k] \leq n$, so the field extension degree is exactly n. ///

[6.0.3] Lemma: Let α belong to the separable closure of the ultrametric field k, and suppose that $\mathrm{ord}\alpha = a/n$ with a relatively prime to n. Then $k(\alpha)$ has ramification index divisible by n (and, thus n divides $[k(\alpha):k]$).

Proof: Let ϖ be a local parameter in the extension $k(\alpha)$. Then

$$\mathrm{ord}\varpi = \frac{1}{e}$$

where e is the ramification index of the extension. Since α differs by a unit from some integer power of ϖ,

$$\frac{a}{n} = \mathrm{ord}\alpha \in \frac{1}{e}\cdot\mathbb{Z}$$

That is, $ea \in n\mathbb{Z}$. Since a is prime to n, it must be that n divides e, which divides the field extension degree in general. ///

[6.0.4] Corollary: *(Eisenstein's criterion)* Let f be monic of positive degree over a principal ideal domain R. Let E be the field of fractions of R. Let π be a prime element of R dividing all the coefficients of f (apart from the leading one, that of x^n), and suppose that π^2 does *not* divide the constant coefficient. Then f is irreducible in $E[x]$.

Proof: Let k be the π-adic completion of E, and $\mathfrak{o}$ the valuation ring in k. In fact, f is irreducible in $k[x]$. The hypothesis implies that the Newton polygon consists of a single segment connecting $(0,1)$ and $(n,0)$, with slope $-1/n$. Thus, by the previous corollary, f is irreducible in $k[x]$. ///

[6.0.5] Corollary: In the situation of the theorem, the polynomial f factors over k into polynomials f_i of degrees d_i, where all roots of f_i have ord $-m_i$. Let $m_i = a_i/d_i$, if a_i is relatively prime to d_i then f_i is *irreducible* over k and any root of f_i generates a totally ramified extension of k.

Proof: If α, β are Galois conjugates, then their ords are the same. Thus, the set of roots with a given ord is stable under Galois. That is, the monic factor f_i of f with these as roots has coefficients in the ground

field k. If the ord of α is of the form a/M with numerator prime to M then α generates an extension of degree divisible by M, by the lemma above. Thus, f_i is irreducible if in lowest terms $-m_i$ has denominator d_i. ///

[6.0.6] Remark: In this last corollary there is not conclusion about the irreducibility of the factor f_i if the denominator of $-m_i$ (in lowest terms) is not the maximum possible, d_i. That is, we reach a sharp conclusion only for totally ramified extensions.

---

7. *Newton-Puiseux series and proofs*

A *Newton-Puiseux* series is simply a power series in $x^{1/n}$ for some positive integer n.

[7.0.1] Theorem: The only algebraic extensions of $\mathbb{C}((x))$ are obtained by adjoining $x^{1/n}$ for $n = 2, \ldots$.

We will prove this after some examples that illustrate the sort of phenomena that the proof must accommodate.
