Example *(cont'd)*: *Function fields* in one variable... as algebraic parallels to $\mathbb{Z}$ and $\mathbb{Q}$.

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

$$\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \;=\; \lim_{d} \mathbb{Z}/d \;=\; \widehat{\mathbb{Z}} \;\approx\; \prod_p \mathbb{Z}_p$$

Remarks What *about* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$?

In Wiles' and Wiles-Taylor' mid-1990s proof of Fermat's Last Theorem, they proved part of the Taniyama-Shimura-Weil (1950s) conjecture: certain *two-dimensional representations* of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ 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-Weil 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:

$$p \;\longrightarrow\; \left(\frac{\sqrt{D}}{p}\right)_2 \;\in\; \mathrm{Gal}(\mathbb{Q}(\sqrt{D})/\mathbb{Q}) \;\approx\; \frac{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\sqrt{D}))}$$

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-Weil 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.

Example: the *circle* $G = S^1 = \mathbb{R}/\mathbb{Z}$ has one-dimensional representations $x \to e^{2\pi inx}$ indexed by integers n. *Fourier series* express *functions* on the circle as sums of exponential functions.

Similarly, $G = \mathbb{R}$ has one-dimensional representations $x \to e^{2\pi inx}$ 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.

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.

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...

But, back to *our* program:

Newton polygons over $\mathbb{Q}_p$

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

$$(0,0),\ (1, \mathrm{ord}_p\, a_{n-1}),\ (2, \mathrm{ord}_p\, a_{n-2}),\ \ \ldots\ \ (n, \mathrm{ord}_p\, a_o)$$

If we believe that $\mathrm{ord}_p(p^n \cdot \frac{a}{b}) = n$ 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 $\mathrm{ord}_p\, a_0 = 1$ 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:

$$\mathfrak{o}_\infty \;=\; \mathbb{C}(X) \cap \mathbb{C}[[1/X]] \qquad\qquad \mathfrak{m}_\infty \;=\; \mathbb{C}(X) \cap \frac{1}{X}\mathbb{C}[[1/X]]$$

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

$$Y^2 \; = \; 1 + \ldots + a_p Z^n \qquad\qquad (n \text{ even})$$

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, $Y = \sqrt{Z} + (\text{h.o.t.})$.