TOWARD MODULARITY: THE SIMPLEST NON-ABELIAN EXAMPLE

April 8, 2013

Introduction

This talk bears on a result called the Modularity Theorem:

All rational elliptic curves arise from modular forms.

Taniyama first suggested in the 1950s that a statement along these lines might be true, and a precise conjecture was formulated by Shimura. A paper of Weil [1] provided strong theoretical evidence for the conjecture. The theorem was proved for a large class of elliptic curves by Wiles [2] with a key ingredient supplied by joint work with Taylor [3], completing the proof of Fermat's Last Theorem after some 350 years. The Modularity Theorem was proved completely by Breuil, Conrad, Diamond, and Taylor [4].

I will not attempt to explain (much less prove) the Modularity Theorem, but only to touch on the fact that:

Representations of Galois groups play a crucial role.

Modularity can be stated in terms of Riemann surfaces or complex Jacobians or complex Abelian varieties, or similarly but with the setting transferred from complex analysis to algebraic geometry over the rational numbers. In the context of arithmetic algebraic geometry, the issues of modularity can be studied in finite characteristic, i.e., we may reduce polynomial equations with integer coefficients modulo primes p. But it is ℓ-adic Galois representations—lifting back to characteristic zero but in a non-Archimedean environment—that provide modularity a framework rich enough in additional structure that the result can be proved.

The talk will sketch an example of the connection between modular forms and Galois groups, the simplest example involving a non-Abelian group.

References

[1] A. Weil, *Uber die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen*, Math. Annalen, vol. 168, pp. 149–156, 1967

[2] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math., vol. 141, no. 3, pp. 443–551, 1995

[3] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math., vol. 141, no. 3, pp. 553–572, 1995

[4] C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of ellipic curves over $\mathbb{Q}$: wild 3-adic exercises*, J. Amer. Math. Soc., vol. 14, no. 4, pp. 843–939, 2001

Part 1. Motivating Ideas

1. Quadratic Reciprocity and Eigenvalues

One idea of modularity is that:

Solution-counts can be viewed as eigenvalues.

For an elementary version of this idea, consider a situation from elementary number theory. Take a quadratic equation

$$\boxed{Q : x^2 = d, \qquad d \in \mathbb{Z}_{\neq 0} \text{ squarefree,}}$$

and for each prime number p define an integer $a_p(Q)$,

$$a_p(Q) = \begin{pmatrix} \text{the number of solutions } x \text{ of equation } Q \\ \text{working modulo } p \end{pmatrix} - 1.$$

The values $a_p(Q)$ extend multiplicatively to values $a_n(Q)$ for all positive integers n, meaning that $a_{mn}(Q) = a_m(Q)a_n(Q)$ for all m and n. By definition, the solution count is the Legendre symbol,

$$a_p(Q) = \left(\frac{d}{p}\right), \quad p > 2.$$

So:

"*We are done.*"

But the immediate point here is to place this elementary, fully-understood situation into two larger contexts, utterly different from one another.

The point of the talk as a whole is to place a slightly more complicated, yet still fully-understood situation into the two larger contexts as well. The issues that emerge are already far more substantive.

The idea of modularity is that the more tractable of the two situations, the *analytic side*, generates all situations that arise on the more difficult *arithmetic side*.

One statement of the Quadratic Reciprocity Theorem is:

$$a_p(Q) \text{ depends only on the value of } p \text{ modulo } 4|d|.$$

This can be reinterpreted as a statement that the solution-counts $\{a_2(Q),\ a_3(Q),\ a_5(Q), \dots\}$ arise as a system of eigenvalues on a finite-dimensional complex vector space associated to the equation Q.

Let $N = 4|d|$, let $(\mathbb{Z}/N\mathbb{Z})^\times$ be the multiplicative group of integer residue classes modulo N, and let V_N be the vector space of complex-valued functions on the group,

$$V_N = \{f : (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow \mathbb{C}\} \qquad (\text{where } N = N(d) = 4|d|).$$

For each prime p define a linear operator T_p on V_N,

$$T_p : V_N \longrightarrow V_N, \qquad (T_p f)(n) = \begin{cases} f(pn) & \text{if } p \nmid N, \\ 0 & \text{if } p \mid N, \end{cases}$$

where the product $pn \in (\mathbb{Z}/N\mathbb{Z})^\times$ uses the reduction of p modulo N. Consider a particular function $f = f_Q$ in V_N,

$$f : (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow \mathbb{C}, \qquad f(n) = a_n(Q) \text{ for } n \in (\mathbb{Z}/N\mathbb{Z})^\times.$$

This is well defined by Quadratic Reciprocity as stated above. Immediately, f is an eigenvector for the operators T_p,

$$\begin{aligned} (T_p f)(n) &= \begin{cases} f(pn) = a_{pn}(Q) = a_p(Q)a_n(Q) & \text{if } p \nmid N, \\ 0 & \text{if } p \mid N \end{cases} \\ &= a_p(Q) f(n) \quad \text{in all cases.} \end{aligned}$$

That is,

$$T_p f = a_p(Q) f \quad \text{for all primes } p.$$

And so indeed $\{a_p(Q)\}$ is a system of eigenvalues as claimed.

2. Quadratic Reciprocity and an Abelian Galois Number Field

Now we turn to the algebraic side. Let

$$\mathbb{F} = \mathbb{Q}(d^{1/2}), \quad d \in \mathbb{Z}_{\neq 0} \text{ squarefree},$$

Then $\mathbb{F}/\mathbb{Q}$ is a Galois extension of degree 2, and its Galois group $\mathrm{Gal}(\mathbb{F}/\mathbb{Q})$ is isomorphic to $\{\pm 1\}$. The Galois group is generated by

$$\sigma : d^{1/2} \longmapsto -d^{1/2},$$

and the isomorphism is

$$\mathrm{Gal}(\mathbb{F}/\mathbb{Q}) \xrightarrow{\sim} \{\pm 1\}, \qquad \sigma \mapsto -1.$$

The rational primes $p \nmid 2d$ are unramified (squarefree) in $\mathbb{F}$, and their behavior is (letting $\mathcal{O}_{\mathbb{F}}$ denote the ring of algebraic integers in $\mathbb{F}$)

$$p\mathcal{O}_{\mathbb{F}} = \begin{cases} \mathfrak{p}_1\mathfrak{p}_2 & \text{if } d \text{ is a square modulo } p, \\ \mathfrak{p} & \text{if } d \text{ is not a square modulo } p. \end{cases}$$

We want to associate elements of the Galois group to primes. Let $p \nmid 2d$ be a rational prime, and let $\mathfrak{p}$ be a maximal ideal of $\mathcal{O}_{\mathbb{F}}$ lying over p. Algebraic number theory guarantees a **Frobenius element** Frob_p of $\mathrm{Gal}(\mathbb{F}/\mathbb{Q})$, characterized by the condition

$$\mathrm{Frob}_p(x) \equiv x^p \pmod{\mathfrak{p}} \quad \text{for all } x \in \mathcal{O}_{\mathbb{F}}.$$

Thus Frob_p acts on the residue field $\mathcal{O}_{\mathbb{F}}/\mathfrak{p}$ literally by raising to the pth power. Because the Galois group is Abelian, the Frobenius depends only on the underlying rational prime p rather than on the ideal $\mathfrak{p}$ lying over it.

To compute the Frobenius element in the quadratic field case, note that

$$\left(d^{1/2}\right)^p = d^{(p-1)/2} d^{1/2}.$$

Euler's Lemma says that $d^{(p-1)/2} \equiv (d/p) \pmod{p}$, and so the Frobenius element multiplies $d^{1/2}$ by the Legendre symbol. There are infinitely many such p such that $(d/p) = 1$, and similarly for $(d/p) = -1$. Therefore every element of the Galois group of $\mathbb{F}$ takes the form Frob_p for infinitely many p, and there is an isomorphism

$$\mathrm{Gal}(\mathbb{F}/\mathbb{Q}) \xrightarrow{\sim} \{\pm 1\}, \qquad \mathrm{Frob}_p \longmapsto \left(\tfrac{d}{p}\right) \text{ for } p \nmid 4d.$$

Thus the system of eigenvalues $\{a_p(Q)\} = \{(d/p)\}$ also appears naturally in the simplest nontrivial character of a Galois group.

3. Dirichlet Characters: the One-Dimensional Abelian Case

Still in the Abelian environment, we illustrate proto-modularity more generally. Any Dirichlet character,

$$\chi : (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times,$$

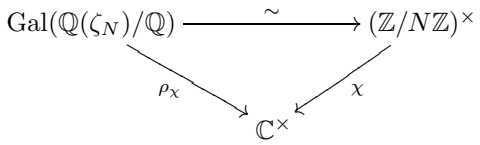
gives rise to a corresponding Abelian Galois group character,

$$\rho_\chi : \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \longrightarrow \mathbb{C}^\times \qquad (\text{where } \zeta_N = e^{2\pi i/N}),$$

as follows. There is an isomorphism

$$\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^\times, \qquad (\zeta_N \mapsto \zeta_N^a) \longmapsto a \pmod N.$$

So in the following diagram, we may define ρ_χ to make the triangle commute.



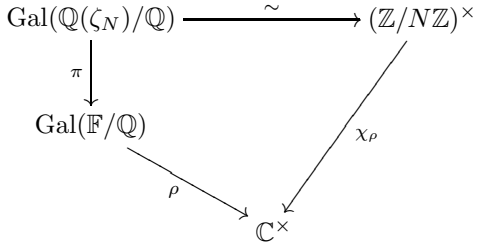
For the converse, consider any finite Abelian extension $\mathbb{F}/\mathbb{Q}$ and any character

$$\rho : \mathrm{Gal}(\mathbb{F}/\mathbb{Q}) \longrightarrow \mathbb{C}^\times.$$

The very substantive

Kronecker–Weber Theorem

states that $\mathbb{F}$ lies in $\mathbb{Q}(\zeta_N)$ for some N. Define χ_ρ to make the following diagram commute:



In sum, Dirichlet characters lead to Abelian Galois group characters, and the Kronecker–Weber Theorem says that Abelian Galois group characters arise from Dirichlet characters.

Here and in the Quadratic Reciprocity example we have yet to see any analysis on the "analytic side." That is about to change.

Part 2. Hecke's Construction

4. What is a Modular Form?

4.1. **Eisenstein series.** The German word *modul* connotes what we now would call a lattice. A *form* is a homogeneous function, such as a polynomial in two variables all of whose terms have the same total degree. The term *modular form* arose from functions such as *Eisenstein series*,

$$G_k(\Lambda) = \sum_{\lambda\in\Lambda}{}' \frac{1}{\lambda^k}, \quad \Lambda \subset \mathbb{C} \text{ a lattice.}$$

Here $k > 2$ is an even integer, and the primed summation sign means to omit $\lambda = 0$ from the summation. Clearly $G_k(m\Lambda) = m^{-k}G_k(\Lambda)$ for all nonzero $m \in \mathbb{C}$. That is, G_k is a function of modules, and a form. Any lattice $\Lambda = \lambda_1\mathbb{Z} \oplus \lambda_2\mathbb{Z}$ (where we may take λ_1/λ_2 to lie in the upper half plane $\mathcal{H}$) is dilated by $m = 1/\lambda_2$ to the lattice $m\Lambda = \Lambda_\tau = \tau\mathbb{Z} \oplus \mathbb{Z}$ where $\tau = \lambda_1/\lambda_2$. If we normalize our lattices by so dilating them, the Eisenstein series become functions of the single complex variable τ,

$$G_k(\tau) = \sum_{(c,d)}{}' \frac{1}{(c\tau + d)^k}, \quad \tau \in \mathcal{H}.$$

Some analysis in in play here in that the Eisenstein series converges nicely enough to be holomorphic.

The *modular group*,

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\},$$

acts on the upper half plane via fractional linear transformations,

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}(\tau) = \frac{a\tau + b}{c\tau + d}, \quad \tau \in \mathcal{H},$$

and one can check that the transformation law of the dehomogenized Eisenstein series is

$$G_k(\gamma(\tau)) = (c\tau + d)^k G_k(\tau), \quad \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

Again analysis is in play since the transformation law requires rearranging the terms of the Eisenstein series.

4.2. **Differential forms.** Complex analysis relies on path integrals of differentials $f(\tau)d\tau$, and $\mathrm{SL}_2(\mathbb{Z})$-invariant path integration on the upper half plane requires such differentials to be invariant when τ is replaced by any $\gamma(\tau)$. A small calculation shows that

$$d\gamma(\tau) = (c\tau + d)^{-2}d\tau, \quad \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

and so the relation $f(\gamma(\tau))\, d(\gamma(\tau)) = f(\tau)\, d\tau$ is

$$f(\gamma(\tau)) = (c\tau + d)^2 f(\tau), \quad \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

similarly to the transformation law for Eisenstein series. Although the exponent 2 in the previous display is the relevant exponent for modularity, in this talk we will see a similar formula with exponent 1.

4.3. **Fourier series.** Specialize the matrix $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ to $\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$ to see that modular forms are $\mathbb{Z}$-periodic,

$$f(\tau + 1) = f(\tau)$$

and thus a modular form has a Fourier series,

$$f(\tau) = \sum_{n=0}^{\infty} a_n(f)\, \mathbf{e}\,(n\tau)\,, \quad \text{where } \mathbf{e}\,(z) = e^{2\pi i z}.$$

(The fact that the sum is over $n \geq 0$ rather than over $n \in \mathbb{Z}$ is a further condition in the definition of a modular form.)

4.4. **The weight-k operator.** Introduce the notation

$$(f[\gamma]_k)(\tau) = (c\tau + d)^{-k} f(\gamma(\tau)).$$

Then the transformation condition for modularity is simply

$$f[\gamma]_k = f \quad \text{for all } \gamma \in \mathrm{SL}_2(\mathbb{Z}).$$

More generally, we may replace $\mathrm{SL}_2(\mathbb{Z})$ with a subgroup, and we may incorporate a character into the transformation law,

$$f[\gamma]_k = \chi(\gamma) f \quad \text{for all } \gamma \in \Gamma.$$

5. Example: The Basic Theta Function

5.1. **The Fourier transform.** Any function $f \in \mathcal{L}^1(\mathbb{R})$ has a *Fourier transform* $\mathcal{F}f : \mathbb{R} \longrightarrow \mathbb{C}$ given by

$$\mathcal{F}f(x) = \int_{y\in\mathbb{R}} f(y)e^{-2\pi iyx}dy.$$

Although the Fourier transform is continuous, it need not belong to $\mathcal{L}^1(\mathbb{R})$. But if $f \in \mathcal{L}^1(\mathbb{R}) \cap \mathcal{L}^2(\mathbb{R})$ then $\mathcal{F}f \in \mathcal{L}^2(\mathbb{R})$.

Conceptually the Fourier transform value $\mathcal{F}f(x) \in \mathbb{C}$ is a sort of inner product $\langle f, \psi_x\rangle$ where ψ_x is the frequency-x oscillation $\psi_x(y) = e^{2\pi iyx}$. Thus we might hope to resynthesize f from the continuum of oscillations weighted suitably by the inner products,

$$f(y) = \int_{x\in\mathbb{R}} \langle f, \psi_x\rangle \psi_x(y)\, dx = \int_{x\in\mathbb{R}} \mathcal{F}f(x)e^{2\pi ixy}\, dx, \quad y \in \mathbb{R}.$$

However, the question of which functions f satisfy the previous display, and the analysis of showing that they do, is nontrivial.

5.2. **Fourier transform of the Gaussian and its dilations.** Let g be the *Gaussian function*,

$$g(x) = e^{-\pi x^2}.$$

The Gaussian is well known to be its own Fourier transform,

$$\mathcal{F}g = g.$$

(One can show this with a complex contour integration. Alternatively, one can differentiate $\mathcal{F}g(\xi)$ under the integral sign and then integrate by parts to see that $(\mathcal{F}g)'(\xi) = -2\pi\xi\mathcal{F}g(\xi)$; also $\mathcal{F}g(0) = 1$, so $\mathcal{F}g$ and g satisfy the same differential equation and initial condition.)

For any function $f \in \mathcal{L}^1(\mathbb{R})$ and any positive number r, the r-dilation of f,

$$f_r(x) = f(xr),$$

has Fourier transform

$$\mathcal{F}(f_r) = r^{-1}(\mathcal{F}f)_{r^{-1}}.$$

So in particular, returning to the Gaussian function g,

$$\text{the Fourier transform of } g(xt^{1/2}) \text{ is } t^{-1/2}g(xt^{-1/2}), \quad t > 0.$$

5.3. **The theta function.** Let $\mathcal{H}$ denote the complex upper half plane. The *theta function* on $\mathcal{H}$ is

$$\vartheta : \mathcal{H} \longrightarrow \mathbb{C}, \qquad \vartheta(\tau) = \sum_{n\in\mathbb{Z}} e^{\pi in^2\tau}.$$

The sum converges very rapidly away from the real axis, making absolute and uniform convergence on compact subsets of $\mathcal{H}$ easy to show, and thus defining a holomorphic function. Clearly

$$\vartheta(\tau + 2) = \vartheta(\tau), \quad \tau \in \mathcal{H}.$$

Specialize to $\tau = it$ with $t > 0$, and write $\theta(t)$ for $\vartheta(it)$. Again let g be the Gaussian. The theta function along the positive imaginary axis is a sum of dilated Gaussians,

$$\theta(t) = \sum_{n\in\mathbb{Z}} e^{-\pi n^2 t}, \quad t > 0.$$

This is a sum of quickly decreasing functions whose graphs narrow as n grows.

5.4. **Poisson summation; transformation law of the theta function.** For any function $f \in \mathcal{L}^1(\mathbb{R})$ such that the sum $\sum_{d\in\mathbb{Z}} f(x+d)$ converges absolutely and uniformly on compact sets and is infinitely differentiable as a function of x, the *Poisson summation formula* is

$$\sum_{n\in\mathbb{Z}} f(x+n) = \sum_{n\in\mathbb{Z}} \mathcal{F}f(n) e^{2\pi i n x}.$$

The idea here is that the left side is the periodicization of f, and then the right side is the Fourier series of the left side, because the nth Fourier coefficient of the periodicization of f is the nth Fourier transform of f itself.

When $x = 0$ the Poisson summation formula specializes to

$$\sum_{n\in\mathbb{Z}} f(n) = \sum_{n\in\mathbb{Z}} \mathcal{F}f(n).$$

And especially, if $f(x)$ is the Gaussian $g(xt^{1/2})$ then Poisson summation with $x = 0$ shows that

$$\sum_{n\in\mathbb{Z}} g(nt^{1/2}) = t^{-1/2} \sum_{n\in\mathbb{Z}} g(nt^{-1/2}),$$

which is to say,

$$\theta(1/t) = t^{1/2}\,\theta(t), \quad t > 0.$$

Returning to the full theta function $\vartheta(\tau)$, the Uniqueness Theorem of complex analysis says that the previous display extends to

$$\vartheta(-1/\tau) = (-i\tau)^{1/2}\,\vartheta(\tau), \quad \tau \in \mathcal{H}.$$

Consequently,

$$\begin{aligned}
\vartheta\left(\frac{\tau}{2\tau+1}\right) &= \vartheta\left(-\frac{1}{-1/\tau-2}\right) \\
&= (i(1/\tau+2))^{1/2}\vartheta\left(-1/\tau-2\right) \\
&= (i(1/\tau+2))^{1/2}\vartheta\left(-1/\tau\right) \\
&= (i(1/\tau+2)(-i\tau))^{1/2}\vartheta\left(\tau\right) \\
&= (2\tau+1)^{1/2}\vartheta\left(\tau\right).
\end{aligned}$$

This transformation law and the earlier transformation law $\vartheta(\tau+2) = \vartheta(\tau)$ together say that the theta function is a modular form, although this time the exponent in the transformation law is $1/2$ and the relevant transformation matrices $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ must have b and c even.

For a modified version of the theta function,

$$\vartheta : \mathcal{H} \longrightarrow \mathbb{C}, \qquad \vartheta(\tau) = \sum_{n\in\mathbb{Z}} \mathbf{e}\left(n^2\tau\right), \quad \text{where } \mathbf{e}\left(z\right) = e^{2\pi i z},$$

the translation-invariance becomes

$$\vartheta(\tau+1) = \vartheta(\tau)$$

and the more complicated transformation law,

$$\vartheta\left(\left[\begin{array}{cc} a & b \\ c & d \end{array}\right]\tau\right) = (c\tau+d)^{1/2}\vartheta(\tau),$$

now requires that c be a multiple of 4. This condition is better suited for defining linear operators T_p on modular forms.

6. Modular Forms Via Theta Functions

Recall how we used Quadratic Reciprocity to motivate the Modularity Theorem, counting the solutions modulo p of the quadratic equation $x^2 = d$. Now consider a cubic equation instead,

$$\boxed{C : x^3 = d, \qquad d \in \mathbb{Z}_{>0} \text{ cubefree,}}$$

and for each prime p let

$$a_p(C) = (\text{the number of solutions modulo } p \text{ of equation } C) - 1.$$

Results from elementary number theory show that

$$a_p(C) = \begin{cases} 2 & \text{if } p \equiv 1 \pmod 3 \text{ and } d \text{ is a nonzero cube modulo } p, \\ -1 & \text{if } p \equiv 1 \pmod 3 \text{ and } d \text{ is not a cube modulo } p, \\ 0 & \text{if } p \equiv 2 \pmod 3 \text{ or } p \mid 3d. \end{cases} \tag{1}$$

We will sketch how Poisson summation and the Cubic Reciprocity Theorem from number theory construct a modular form having the solution-counts as its prime-index Fourier coefficients,

$$a_p(\theta_\chi) = a_p(C).$$

Furthermore, these coefficients are eigenvalues. The construction is one case of a general method due to Hecke [1].

Introduce the ring of **Eisenstein integers**, geometrically the hexagonal lattice,

$$A = \mathbb{Z}[\zeta_3] \quad \text{where } \zeta_3 = e^{2\pi i/3}.$$

The arithmetic of this ring, to be detailed below, is only slightly more complicated than the usual arithmetic of the rational integer ring $\mathbb{Z}$. Also we need a few auxiliary objects, the element $\alpha = i\sqrt{3}$ of A and the ring $B = \frac{1}{\alpha}A$ (the *inverse-different* of A). Thus $A \subset B \subset \frac{1}{3}A$. The three lattices are shown in figure 1.

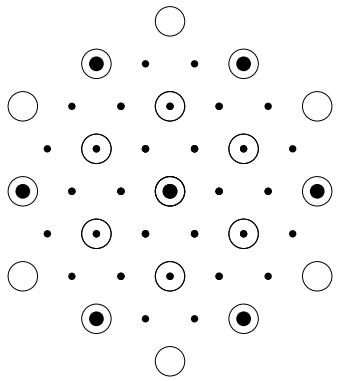


FIGURE 1. Three lattices

For any positive integer N and any $\overline{u}$ in the quotient group $\frac{1}{3}A/NA$ define a theta function, more complicated than the simple theta function from before,

$$\theta^{\overline{u}}(\tau, N) = \sum_{n \in A} \mathbf{e}\left(\tfrac{1}{N}|u + nN|^2\tau\right), \quad \tau \in \mathcal{H}.$$

The new ingredients here are

- The basic lattice is now $A \subset \mathbb{C}$ rather than $\mathbb{Z} \subset \mathbb{R}$.
- A dilation factor N (the *level*) is now present.
- Rather than take square-sizes over the (dilated) lattice, we do so over the $\overline{u}$-offset translate of it.

The basic properties of θ are as follows. The first and third are similar to the transformation laws of the basic theta function, while the second is the relation between θ at two different dilations, a symmetrization over the larger dilation to obtain the smaller one. The idea is shown in figure 2. (From now until near the end of the section the symbol d is unrelated to the d of the cubic equation C.)

$$\theta^{\overline{u}}(\tau + 1, N) = \mathbf{e}\left(\tfrac{|u|^2}{N}\right)\theta^{\overline{u}}(\tau, N), \qquad \overline{u} \in B/NA,$$

$$\theta^{\overline{u}}(\tau, N) = \sum_{\substack{\overline{v} \in B/dNA \\ \overline{v} \equiv \overline{u}\ (NA)}} \theta^{\overline{v}}(d\tau, dN), \qquad \overline{u} \in B/NA,\ d \in \mathbb{Z}^+,$$

$$\theta^{\overline{v}}(-1/\tau, N) = \frac{-i\tau}{N\sqrt{3}} \sum_{\overline{w} \in B/NA} \mathbf{e}\left(-\tfrac{\operatorname{tr}(vw^*)}{N}\right)\theta^{\overline{w}}(\tau, N), \quad \overline{v} \in B/NA.$$

The first two properties are elementary, but the third one relies on Poisson summation. Note that the exponent of $-i\tau$ in the third one is not 2 or 1/2 but rather 1.

All three laws require considerably more detail-management than the basic theta function, and comfort with the algebra of A, but nothing really new.

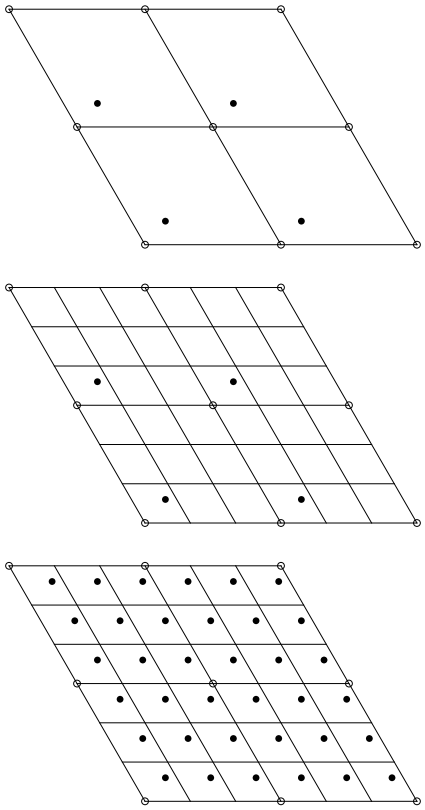


FIGURE 2. Point and translates, subgroup, symmetrization

The basic properties help us establish how the theta function transforms under the group

$$\Gamma_0(3N, N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : b \equiv 0 \pmod{N},\ c \equiv 0 \pmod{3N} \right\}.$$

The rule is

$$(\theta^{\overline{u}}[\gamma]_1)(\tau, N) = \left(\tfrac{d}{3}\right) \theta^{\overline{au}}(\tau, N), \quad \overline{u} \in A/NA,\ \gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \Gamma_0(3N, N).$$

Here $(d/3)$ is the Legendre symbol. Proving the transformation law is painstaking but still it is elementary. However, the transformation law is unsatisfactory on two counts: first, the group $\Gamma_0(3N, N)$ does not dovetail easily with linear operators; and second, the theta function on the right has offset $\overline{au}$ rather than the offset $\overline{u}$ on the left.

To move to a more convenient group and then construct a modular form from the theta functions, we conjugate and then symmetrize. The group

$$\Gamma_0(3N^2) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod{3N^2} \right\}$$

fits better into the theory of modular forms than the group $\Gamma_0(3N, N)$ from a moment ago. To conjugate, let $\delta = \left[\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right]$ so that

$$\delta\Gamma_0(3N^2)\delta^{-1} = \Gamma_0(3N, N)$$

and the conjugation preserves matrix entries on the diagonal. For any $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \Gamma_0(3N^2)$,

$$\begin{aligned} (\theta^{\overline{u}}[\delta\gamma]_1)(\tau, N) &= (\theta^{\overline{u}}[\gamma'\delta]_1)(\tau, N) && \text{where } \gamma' = \delta\gamma\delta^{-1} \in \Gamma_0(3N, N) \\ &= \left(\tfrac{d}{3}\right)(\theta^{\overline{au}}[\delta]_1)(\tau, N) && \text{since } d = d_{\gamma'}. \end{aligned} \tag{2}$$

The construction is completed by symmetrizing: Let $\chi : (A/NA)^\times \longrightarrow \mathbb{C}^\times$ be a character, lifted to A. Define

$$\theta_\chi(\tau) = \tfrac{1}{6} \sum_{\overline{u} \in A/NA} \chi(u)\theta^{\overline{u}}(N\tau, N).$$

Then θ_χ transforms as a modular form of exponent 1 under $\Gamma_0(3N^2)$,

$$\theta_\chi[\gamma]_1 = \psi(d)\theta_\chi, \quad \gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \Gamma_0(3N^2),$$

where the character in the transformation law is the given character times the Legendre symbol,

$$\psi(d) = \chi(d)\left(\tfrac{d}{3}\right).$$

Indeed, the desired transformation of θ_χ under $\Gamma_0(3N^2)$ follows from (2) since $\theta_\chi = \sum_{\overline{u}} \chi(u)\theta^{\overline{u}}[\delta]_1$. The Fourier expansion of θ_χ is

$$\theta_\chi(\tau) = \tfrac{1}{6} \sum_{n \in A} \chi(n)\mathbf{e}\left(|n|^2\tau\right) = \sum_{m=0}^{\infty} a_m(\theta_\chi)\mathbf{e}\left(m\tau\right)$$

where the Fourier coefficients are

$$a_m(\theta_\chi) = \tfrac{1}{6} \sum_{\substack{n \in A \\ |n|^2 = m}} \chi(n). \tag{3}$$

This formula shows that $\theta_\chi = 0$ unless χ is trivial on $A^\times$.

Some facts about the arithmetic of the Eisenstein integer ring A are as follows. First, A is a principal ideal domain. For each prime $p \equiv 1 \pmod 3$ there exists an element $\pi_p \in A$ such that $\pi_p\overline{\pi}_p = p$, but there is no such element if $p \equiv 2 \pmod 3$. The maximal ideals of A are

- for each prime $p \equiv 1 \pmod 3$, the two ideals $\langle\pi_p\rangle$ and $\langle\overline{\pi}_p\rangle$,
- for each prime $p \equiv 2 \pmod 3$, the ideal $\langle p\rangle$,
- for $p = 3$, the ideal $\langle\sqrt{-3}\rangle$.

Let $\pi_p = p$ for each prime $p \equiv 2 \pmod 3$, let $\pi_3 = \sqrt{-3}$, and take the set of generators of the maximal ideals,

$$\mathcal{S} = \{\pi_p, \overline{\pi}_p : p \equiv 1 \pmod 3\} \cup \{\pi_p : p \equiv 2 \pmod 3\} \cup \{\pi_3\}.$$

Then each nonzero $n \in A$ can be written uniquely as

$$n = u\prod_{\pi \in \mathcal{S}} \pi^{a_\pi}, \quad u \in A^*, \text{ each } a_\pi \in \mathbf{N},\ a_\pi = 0 \text{ for all but finitely many } \pi.$$

Correspondingly $\chi(n) = \prod_{\pi \in \mathcal{S}} \chi(\pi)^{a_\pi}$.

Recall Hecke's modular form

$$\theta_\chi(\tau) = \tfrac{1}{6}\sum_{n\in A}\chi(n)\mathbf{e}\left(|n|^2\tau\right) = \sum_{m=0}^{\infty} a_m(\theta_\chi)\mathbf{e}\left(m\tau\right), \qquad a_m(\theta_\chi) = \tfrac{1}{6}\sum_{\substack{n\in A\\ |n|^2=m}}\chi(n).$$

Its corresponding L-function is

$$L(s,\theta_\chi) = \sum_{m=1}^{\infty} a_m(\theta_\chi)m^{-s} = \tfrac{1}{6}\sum_{\substack{n\in A\\ n\neq 0}}\chi(n)|n|^{-2s} = \prod_{\pi\in\mathcal{S}}(1-\chi(\pi)|\pi|^{-2s})^{-1}.$$

The local Euler factors work out to

$$\begin{cases} (1-(\chi(\pi_p)+\chi(\bar{\pi}_p))p^{-s}+\chi(p)p^{-2s})^{-1} & \text{if } p\equiv 1 \pmod 3,\\ (1-\chi(p)p^{-2s})^{-1} & \text{if } p\equiv 2 \pmod 3,\\ (1-\chi(\sqrt{-3})3^{-s})^{-1} & \text{if } p=3. \end{cases}$$

That is,

$$L(s,\theta_\chi) = \sum_{m=1}^{\infty} a_m(\theta_\chi)m^{-s} = \prod_{p}(1-a_p(\theta_\chi)p^{-s}+\psi(p)p^{-2s})^{-1}.$$

This factorization of $L(\theta_\chi)$ says that θ_χ itself is an eigenfunction of a family of operators T_p called **Hecke operators**, whose eigenvalues are the Fourier coefficients $a_p(\theta_\chi)$.

The Hecke operator T_1 is trivial. Most of the Hecke operators of prime index are given by the baffling formula

$$(T_pf)(\tau) = \begin{cases} f(p\tau)+p^{-k}\sum_{j=0}^{p-1} f\left(\frac{\tau+j}{p}\right) & \text{if } p\nmid N,\\ p^{-k}\sum_{j=0}^{p-1} f\left(\frac{\tau+j}{p}\right) & \text{if } p\mid N. \end{cases}$$

(Note how our operator T_p in the Quadratic Reciprocity example at the beginning of the talk is a toy version of this.) The Hecke operators transfer to many different contexts, manifesting themselves differently in each, and finally in the environment of local fields they are recognizable as convolution operators. The Hecke operators of non-prime index are defined from T_1 and the T_p by a condition that a generating function factors as an Euler product,

$$\sum_{m=1}^{\infty} T_m m^{-s} = \prod_{p}(1-T_pp^{-s}+\langle p\rangle p^{k-1-2s})^{-1}.$$

(Here $\langle p\rangle f = f[\alpha]_k$ for any $\alpha = \left[\begin{smallmatrix} a & b\\ c & \delta\end{smallmatrix}\right] \in \Gamma_0(3N^2)$ with $\delta \equiv d \pmod{3N^2}$.) The similarity between this display and the Euler factorization of $L(s,\theta_\chi)$ is no coincidence: the Hecke operators are engineered precisely to pick out the modular forms whose L-functions have suitable Euler products.

Along with Poisson summation, the other ingredient for constructing a modular form to match the cubic equation C from the beginning of the section is the Cubic Reciprocity Theorem. The unit group of A is $A^\times = \{\pm 1, \pm\zeta_3, \pm\zeta_3^2\}$. Recall that $\theta_\chi = 0$ unless χ is trivial on $A^\times$. Let p be a rational prime.

- If $p \equiv 1 \pmod 3$ then there exists an element π of A which, along with its conjugate and units gives all elements of norm p,
$$\{n \in A : |n|^2 = p\} = A^\times \pi \cup A^\times \overline{\pi}.$$
The choice of π can be normalized, e.g., to $\pi = a + b\zeta_3$ where $a \equiv 2 \pmod 3$ and $b \equiv 0 \pmod 3$.
- But if $p \equiv 2 \pmod 3$ then p does not take the form $p = |n|^2$ for any $n \in A$, as is seen by checking $|n|^2$ modulo 3.

(See 9.1–9.6 of [2] for more on the arithmetic of A.)

A form of Cubic Reciprocity is as follows. (Now the symbol d again comes from the cubic equation at the beginning of the section, and the value of N, which has been free throughout this section, depends on d.)

Cubic Reciprocity Theorem. *Let $d \in \mathbb{Z}^+$ be cubefree and let*
$$N = 3 \prod_{p|d} p.$$
Then there exists a character
$$\chi : (A/NA)^\times \longrightarrow \{1, \zeta_3, \zeta_3^2\}$$
such that the multiplicative extension of χ to all of A is trivial on $A^\times$ and on primes $p \nmid N$, while on elements π of A such that $\pi\bar{\pi}$ is a prime $p \nmid N$ it is trivial if and only if d is a cube modulo p.

The character χ on $(A/NA)^\times$ is the cubic counterpart of the quadratic character $(d/\cdot)$ on $(\mathbb{Z}/N\mathbb{Z})^\times$ with $N = 4|d|$.

For the character χ of Cubic Reciprocity, Hecke's modular form $\theta_\chi(\tau, N)$ lies in the vector space
$$V_N = \mathcal{M}_1(3N^2, \psi) \qquad (\text{where } N = N(d) = 3\prod_{p|d} p),$$
with ψ the quadratic character with conductor 3 (in general $\psi(d) = \chi(d)(d/3)$ but now χ is trivial on primes $p \nmid N$). Formula (3) shows that the Fourier coefficients of prime index are
$$a_p(\theta_\chi) = \begin{cases} 2 & \text{if } p \equiv 1 \pmod 3 \text{ and } d \text{ is a nonzero cube modulo } p, \\ -1 & \text{if } p \equiv 1 \pmod 3 \text{ and } d \text{ is not a cube modulo } p, \\ 0 & \text{if } p \equiv 2 \pmod 3 \text{ or } p \mid 3d. \end{cases}$$
That is, the Fourier coefficients are the solution-counts (1) of equation C as anticipated at the beginning of the section. Furthermore, we have already seen that they are a collection of eigenvalues.

References

[1] E. Hecke, *Zur Theorie der elliptischen Modulfunktionen*, Math. Annalen, pp. 210–242, vol. 97, 1926

[2] Kenneth Ireland and Michael Rosen, **A Classical Introduction to Modern Number Theory**, Springer-Verlag, Graduate Texts in Mathematics **84**, second ed., 1992

Part 3. Simplest Case on the Arithmetic Side

7. A non-Abelian Galois Number Field

Let $d > 1$ be a cubefree integer, let $d^{1/3}$ denote the real cube root of d, and let

$$\mathbb{F} = \mathbb{Q}(d^{1/3}, \zeta_3) \quad \text{where } \zeta_3 = e^{2\pi i/3}.$$

Then $\mathbb{F}/\mathbb{Q}$ is a Galois extension of degree 6, and its Galois group $\mathrm{Gal}(\mathbb{F}/\mathbb{Q})$ is isomorphic to S_3, the symmetric group on three letters. The Galois group is generated by

$$\sigma : \begin{pmatrix} d^{1/3} \longmapsto \zeta_3 d^{1/3} \\ \zeta_3 \longmapsto \zeta_3 \end{pmatrix}, \qquad \tau : \begin{pmatrix} d^{1/3} \longmapsto d^{1/3} \\ \zeta_3 \longmapsto \zeta_3^2 \end{pmatrix},$$

and the isomorphism (noncanonical) is

$$\mathrm{Gal}(\mathbb{F}/\mathbb{Q}) \xrightarrow{\sim} S_3, \qquad \sigma \mapsto (1\,2\,3),\ \tau \mapsto (2\,3).$$

The rational primes not dividing $3d$ are unramified (squarefree) in $\mathbb{F}$, and their behavior is (letting $\mathcal{O}_\mathbb{F}$ denote the ring of algebraic integers in $\mathbb{F}$)

$$p\mathcal{O}_\mathbb{F} = \begin{cases} \mathfrak{p}_1 \cdots \mathfrak{p}_6 & \text{if } p \equiv 1 \pmod 3 \text{ and } d \text{ is a cube modulo } p, \\ \mathfrak{p}_1\mathfrak{p}_2 & \text{if } p \equiv 1 \pmod 3 \text{ and } d \text{ is not a cube modulo } p, \\ \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 & \text{if } p \equiv 2 \pmod 3. \end{cases} \tag{4}$$

Again we want to associate elements of the Galois group to primes. Let p be a rational prime and let $\mathfrak{p}$ be a maximal ideal of $\mathcal{O}_\mathbb{F}$ lying over p. As before, algebraic number theory guarantees a Frobenius element $\mathrm{Frob}_\mathfrak{p}$ of $\mathrm{Gal}(\mathbb{F}/\mathbb{Q})$, characterized by the condition

$$\mathrm{Frob}_\mathfrak{p}(x) \equiv x^p \pmod{\mathfrak{p}} \quad \text{for all } x \in \mathcal{O}_\mathbb{F}.$$

Because the Galois group is non-Abelian, the Frobenius now depends on the ideal $\mathfrak{p}$ lying over the rational prime p; however, the conjugacy class of $\mathrm{Frob}_\mathfrak{p}$ in $\mathrm{Gal}(\mathbb{F}/\mathbb{Q})$ depends only on p.

Since the conjugacy classes in any symmetric group S_n are specified by the cycle structure of their elements, in this case of S_3 they are

$$\{1\}, \quad \{(1\,2), (2\,3), (3\,1)\}, \quad \{(1\,2\,3), (1\,3\,2)\}.$$

So the conjugacy class of an element of S_3 is determined by the element's order (here we take great advantage of our group being so small), and therefore this holds in $\mathrm{Gal}(\mathbb{F}/\mathbb{Q})$ as well. To determine the conjugacy class of $\mathrm{Frob}_\mathfrak{p}$ it thus suffices to determine its order.

For any unramified rational prime p, i.e., $p \nmid 3d$, algebraic number theory tells us that the order is 6 divided by the number of factors of p in in formula (4), so the associated conjugacy class

$$\{\mathrm{Frob}_\mathfrak{p} : \mathfrak{p} \text{ lies over } p\} \tag{5}$$

is

$$\text{the elements of order } \begin{cases} 1 & \text{if } p \equiv 1 \pmod 3 \text{ and } d \text{ is a cube modulo } p, \\ 3 & \text{if } p \equiv 1 \pmod 3 \text{ and } d \text{ is not a cube modulo } p, \\ 2 & \text{if } p \equiv 2 \pmod 3. \end{cases}$$

Each conjugacy class takes the form (5) for infinitely many p, in consequence of the Tchebotarov Density Theorem.

8. The Connection With Hecke's Modular Form

We are ready to relate the simplest non-Abelian Galois number field to the earlier part of the talk. There is an embedding of S_3 in $\mathrm{GL}_2(\mathbb{Z})$ such that

$$(1\,2\,3) \longmapsto \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}, \qquad (2\,3) \longmapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

This gives a representation

$$\rho : \mathrm{Gal}(\mathbb{F}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}).$$

The trace of ρ is a well defined function on conjugacy classes (5) and therefore depends only on the underlying unramified rational primes p,

$$\mathrm{tr}\,\rho(\mathrm{Frob}_{\mathfrak{p}}) = \begin{cases} 2 & \text{if } p \equiv 1 \pmod 3 \text{ and } d \text{ is a cube modulo } p, \\ -1 & \text{if } p \equiv 1 \pmod 3 \text{ and } d \text{ is not a cube modulo } p, \\ 0 & \text{if } p \equiv 2 \pmod 3. \end{cases}$$

Similarly the determinant of ρ is defined on conjugacy classes over unramified primes,

$$\det \rho(\mathrm{Frob}_{\mathfrak{p}}) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 3, \\ -1 & \text{if } p \equiv 2 \pmod 3. \end{cases}$$

Recall the modular form $\theta_\chi(\tau) \in \mathcal{M}_1(3N^2, \psi)$ where $N = 3\prod_{p|d} p$ and ψ is the quadratic character with conductor 3. Comparing the previous two displays with the data for θ_χ shows that

$$\boxed{\mathrm{tr}\,\rho(\mathrm{Frob}_{\mathfrak{p}}) \textit{ is the Fourier coefficient } a_p(\theta_\chi) \textit{ when } p \nmid 3d}$$

and

$$\boxed{\det \rho(\mathrm{Frob}_{\mathfrak{p}}) \textit{ is the character value } \psi(p).}$$

In sum, the Galois group representation ρ, as described by its trace and determinant on Frobenius elements, arises from the modular form θ_χ.