MATH 776
APPLICATIONS: RECIPROCITY LAWS

ANDREW SNOWDEN

1. Quadratic reciprocity

For an odd prime number p and an integer a not divisible by p, put

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ is a square in } \mathbf{F}_p \\ -1 & a \text{ is not a square in } \mathbf{F}_p \end{cases}$$

This is called the **Legendre symbol**. We note that $a \mapsto \left(\frac{a}{p}\right)$ defines a group homomorphism $\mathbf{F}_p^\times \to \mu_2$, and, in fact, is the unique such non-trivial homomorphism. Put $p^* = (-1)^{(p-1)/2}p$. Quadratic reciprocity, originally proven by Gauss, is the following theorem, which we prove using ideas from class field theory:

Theorem 1.1. *Let p and q be distinct odd primes. Then*

$$\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right).$$

Proof. The field $\mathbf{Q}(\zeta_q)$ is Galois over $\mathbf{Q}$ with Galois group $\mathbf{F}_q^\times$. This group is cyclic of order $q-1$, and therefore has a unique index 2 subgroup, namely $(\mathbf{F}_q^\times)^2$. The corresponding quadratic extension of $\mathbf{Q}$ is $\mathbf{Q}(\sqrt{q^*})$. (Why? Hint: look at ramification! Alternatively, use Gauss sums.) We know that under the isomorphism $\mathrm{Gal}(\mathbf{Q}(\zeta_q)/\mathbf{Q}) \cong \mathbf{F}_q^\times$ we have $\mathrm{Frob}_p \mapsto p$. We therefore obtain the following:

$$\mathrm{Frob}_p = 1 \text{ in } \mathrm{Gal}(\mathbf{Q}(\sqrt{q^*})/\mathbf{Q}) \iff \left(\frac{p}{q}\right) = 1$$

On the other hand, by basic algebraic number theory, we know that the following statements are equivalent:

(a) $\mathrm{Frob}_p = 1$ in $\mathrm{Gal}(\mathbf{Q}(\sqrt{q^*})/\mathbf{Q})$.
(b) p splits in $\mathbf{Q}(\sqrt{q^*})$.
(c) $\left(\frac{q^*}{p}\right) = 1$.

Thus the theorem follows. □

Remark 1.2. The full statement of quadratic reciprocity includes two auxiliary laws:

$$\left(\frac{-1}{p}\right) = 1 \iff p = 1 \pmod 4$$

and

$$\left(\frac{2}{p}\right) = 1 \iff p = \pm 1 \pmod 8,$$

Date: January 29, 2019.

which can be proven by similar arguments. Using the law Theorem 1.1 and the above two laws, one can easily compute the Legendre character. □

Remark 1.3. Let us elaborate conceptually on the proof of Theorem 1.1. In any extension of $\mathbf{Q}$, the splitting of a prime number p corresponds to how some polynomial factors modulo p. The key input from class field theory is that, for abelian extensions, the behavior of p can be determined from the congruence class of p with respect to some modulus. So, given class field theory, it is clear that, in principle, there will a theorem of the form $\left(\frac{q^*}{p}\right) = 1$ if and only if p satisfies some congruence. Of course, in this specific application, the full force of class field theory is not necessary: we just need a good understanding of cyclotomic extensions. □

2. Cubic reciprocity

Let $\omega = \zeta_3$ be a primitive cubic root of unity. The ring of integers in the field $K = \mathbf{Q}(\omega)$ is $R = \mathbf{Z}[\omega]$, and called the ring of **Eisenstein integers**. It is a unique factorization domain, and its unit group is $\{\pm 1, \pm\omega, \pm\omega^2\} \cong \mathbf{Z}/6\mathbf{Z}$. Rational primes behave as follows:

- The extension of the ideal (3) factors as $(1-\omega)^2$; in fact, $3 = -\omega^2(1-\omega)^2$.
- If p is a prime number congruent to 2 modulo 3 then p remains prime in R.
- If p is a prime number congruent to 1 modulo 3 then p factors as $\pi\overline{\pi}$ for some prime element π of R.

An element of R is called **primary** if it is congruent to 1 modulo 3. Note that $R^\times \to (R/3R)^\times$ is a group isomorphism, and so if x is an element of R that is prime to 3 then there is a unique unit u such that ux is primary. In this way, primary elements of R are analogous to positive integers. The unique factorization theorem in R can be stated as: if $x \in R$ is non-zero then it factors uniquely as $u(1-\omega)^n\pi_1^{e_1}\cdots\pi_m^{e_m}$ where u is a unit and the π's are primary primes.

Suppose that π is a prime element of R coprime to 3. Letting $\kappa(\pi)$ denote the residue field, the reduction map $\mu_3 \to \kappa(\pi)$ is injective; in particular, $\mathrm{Nm}(\pi) \equiv 1 \pmod 3$. We thus see that if $a \in R$ is prime to π then $a^{(\mathrm{Nm}(\pi)-1)/3}$ is equivalent, modulo π, to a unique cubic root of unity. We define $\left(\frac{a}{\pi}\right)_3$ to be that cubic root of unity. This is called the **cubic residue character**. It is similar to the Legendre character in a number of respects. In particular, $\left(\frac{a}{\pi}\right)_3 = 1$ if and only if a is a cube modulo π.

The following theorem, called cubic reciprocity, is the analog of quadratic reciprocity, and due to Eisenstein:

Theorem 2.1. *Let π and θ be primary primes. Then*

$$\left(\frac{\pi}{\theta}\right)_3 = \left(\frac{\theta}{\pi}\right)_3.$$

Proof. We will only prove the following weaker statement:

$$\left(\frac{\pi}{\theta}\right)_3 = 1 \iff \left(\frac{\theta}{\pi}\right)_3 = 1.$$

A similar but slightly more complicated argument can be used to prove the full statement, see [S].

Let L be the field $K(\sqrt[3]{\pi})$, and consider the extension L/K. It is Galois, with Galois group cyclic of order 3, as K contains the cube roots of unity. We leave it as an exercise

to show that the extension ramifies only at $1-\omega$ and π. By the adelic formulation of class field theory, the global Artin map gives a surjection $\varphi\colon \mathbf{C}_K \to \mathrm{Gal}(L/K)$. Since K has class number 1, we have $\mathbf{C}_K = (\prod_{v\nmid\infty} U_v \times K_\infty^\times)/R^\times$. By the compatibility of the local and global Artin maps, the local units at all places away from 3 and π belong to the kernel of φ; of course, $K_\infty^\times$ also belongs to the kernel, as it is connected. One can show that the conductor at $1-\omega$ is 3; the conductor at π is necessarily π, since wild inertia is prime to 3. We thus see that φ induces a surjection

$$\kappa(\pi)^\times \cong ((R/3R)^\times \times \kappa(\pi)^\times)/R^\times \to \mathrm{Gal}(L/K).$$

Combined with the Kummer isomorphism $\mathrm{Gal}(L/K) \cong \mu_3$, we thus obtain a surjection $\varphi\colon \kappa(\pi)^\times \to \mu_3$. We thus find that $\varphi = \left(\frac{-}{\pi}\right)_3^{\pm 1}$. Note that the first isomorphism above embeds $\kappa(\pi)^\times$ as the primary elements of the right side; thus, since θ is primary, we see that Frob_θ corresponds to $\theta^{-1} \in \kappa(\pi)^\times$, and thus maps to $\left(\frac{\theta}{\pi}\right)^{\pm 1}$ in μ_3.

By the above analysis, we see that $\mathrm{Frob}_\theta = 1$ in $\mathrm{Gal}(L/K)$ if and only if $\left(\frac{\theta}{\pi}\right)_3 = 1$. However, this is equivalent to θ splitting in L, which is equivalent to π being a cube modulo θ, i.e., $\left(\frac{\pi}{\theta}\right)_3 = 1$. This completes the proof. □

3. Higher powers

Suppose that K is a number field containing the nth roots of unity. Given a prime ideal $\mathfrak{p}$ prime to n, and an element a prime to $\mathfrak{p}$, we define $\left(\frac{a}{\mathfrak{p}}\right)_n$ to be the unique nth root of unity satisfying

$$a^{(\mathrm{Nm}(\mathfrak{p})-1)/n} \equiv \left(\frac{a}{\mathfrak{p}}\right)_n \pmod{\mathfrak{p}}.$$

Given an arbitrary ideal $\mathfrak{b} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu(\mathfrak{p})}$ that is prime to n, and $a \in K$ prime to $\mathfrak{b}$, we define

$$\left(\frac{a}{\mathfrak{b}}\right)_n = \prod_{\mathfrak{p}} \left(\frac{a}{\mathfrak{p}}\right)_n^{\nu(\mathfrak{p})}.$$

When $\mathfrak{b} = (b)$ is a principal ideal, we put $\left(\frac{a}{b}\right)_n = \left(\frac{a}{\mathfrak{b}}\right)_n$.

Theorem 3.1. *If $a, b \in K^\times$ are relatively prime to each other and to n then*

$$\left(\frac{a}{b}\right)_n \left(\frac{b}{a}\right)_n^{-1} = \prod_{\mathfrak{p}\mid n\infty} \left(\frac{a,b}{\mathfrak{p}}\right)_n$$

where the quantities on the right side are local Hilbert symbols.

We have not yet defined the local Hilbert symbols. However, as the name suggests, they are purely local. Since the above theorem only uses them at primes $\mathfrak{p}$ dividing n and ∞, it is really an niteresting statement, despite containing these as yet undefined quantities. For example, to deduce classical quadratic recirprocity from it ($n = 2$ and $K = \mathbf{Q}$), one would only have to do two local computations, one at 2 and one at ∞.

References

[K] K. Kedlaya. Notes on class field theory. http://www.math.mcgill.ca/darmon/courses/cft/refs/kedlaya.pdf

[S] D. Speyer, Mathoverflow answer, https://mathoverflow.net/questions/234358/

[W] L. Washington. *Introduction to Cyclotomic Fields*, Chapter 14