CLASS FIELD THEORY

COURSE: RENÉ SCHOOF AND PETER STEVENHAGEN
NOTES: ROSS PATERSON

Disclaimer. These notes were taken live during lectures at the Spring School on Arithmetic Statistics held at CIRM from 8$^{\text{th}}$–12$^{\text{th}}$ May 2023. Any mistakes are the fault of the transcriber and not of the lecturer, they have not been proofread in any meaningful way.

Lecture 1 (Stevenhagen)

Recall the Fermat equation

$$x^n + y^n = z^n/\mathbb{Z}.$$

Note, an observation due to the likes of Kummer, that if we allow ourselves complex numbers then we can factorise

$$y^m = \prod_{i=1}^{m} (Z - \zeta_m^i X),$$

where $\zeta_m = e^{2\pi i/m}$. Kummer discovered that in fact we don't need to look at all of the complex numbers, but in fact we should look at 'number rings' $\mathbb{Z}[\zeta_m]$.

Algebraic Number Theory. Algebraic number theory is essentially doing arithmetic like we do for $\mathbb{Z}$, but now for number rings. These number rings live in number fields, much like $\mathbb{Z}$ lives in $\mathbb{Q}$, and in fact we end up with a diagram

$$\begin{tikzcd} K = \mathbb{Q}(\alpha) \supset \mathcal{O}_K \supseteq \mathbb{Z}[\alpha] \\ \mathbb{Q} \supset \mathbb{Z} \arrow[u, "n"] \end{tikzcd}$$

where $f = f_{\mathbb{Q}}^{\alpha} \in \mathbb{Z}[X]$ is the minimal polynomial of α. Some remarks.

- We would like to find $\mathcal{O}_K$, the ring of integers, which is free of rank $n/\mathbb{Z}$.
- $\mathcal{O}_K$ has unique prime factorisation.
- We have the class group $\mathrm{Cl}_K = I_K/P_K$, where I_K is the group of fractional ideals in $\mathcal{O}_K$ and P_K is the group of principal fractional ideals, and this is a finite abelian group.
- We have embeddings

$$\begin{tikzcd} K \arrow[r, "\text{complex}"] \arrow[dr, "\text{real}"] & \mathbb{C} \\ & \mathbb{R}, \arrow[u] \end{tikzcd}$$

  say we have r real embeddings and $2s$ complex ones (this is always even since for every complex embedding there is the complex conjugate embedding). Then $r + 2s + n$.

- $\mathcal{O}_K^\times = \mu_K \times \mathbb{Z}^{r+s-1}$, where μ_K is the finite group of roots of unity in K.
- The discriminant of the minimal polynomial of α, $\Delta(f)$, is related to the discriminant of the number field, Δ_K, by
$$\Delta(f) = [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2 \Delta_K.$$
- There is the Minkowski bound, which tells us that every class in Cl_K contains an integral ideal of norm at most the 'Minkowski constant' M_K, which is some explicit multiple of $\sqrt{\Delta_K}$. More precisely
$$M_K = \left(\frac{4}{\pi}\right)^s \left(\frac{n!}{n^n}\right)^2 \sqrt{\Delta_K}$$

Cyclotomic Rings. Okay so let us return to our example of cyclotomic rings. Let $K_m = \mathbb{Q}(\zeta_m)$, then the ring of integers is easy:
$$\mathcal{O}_K = \mathbb{Z}[\zeta_m].$$
There is already a natural action of $R_m = (\mathbb{Z}/m\mathbb{Z})^\times$ on this ring and field. For $a \in (\mathbb{Z}/m\mathbb{Z})^\times$ we have the map $\varphi_a : \zeta_m \mapsto \zeta_m^a$. Thus $\mathcal{O}_K$ is a $\mathbb{Z}[R_m]$-module.

Splitting of Primes. Recall we had the diagram
$$\begin{tikzcd} K = \mathbb{Q}(\alpha) \supset \mathbb{Z}[\alpha] \\ \mathbb{Q} \supset \mathbb{Z} \arrow[u, "n"] \end{tikzcd}$$
We want to know what 'lies above a prime $p \in \mathbb{Z}$', i.e. we want the factorisation
$$p\mathcal{O}_K = \prod_{i=1}^t \mathfrak{p}_i^{e_i}.$$
For $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$, we can take $\overline{f} = f \mod p$ and look at its factorisation
$$\overline{f} = \prod_{i=1}^t \overline{g}_i^{e_i} \in \mathbb{F}_p[X],$$
and this gives the correct e_i and moreover if we choose lifts of the $\overline{g}_i$ to $\mathbb{Z}[X]$ then $\mathfrak{p}_i = \langle p, g_i(\alpha)\rangle$.

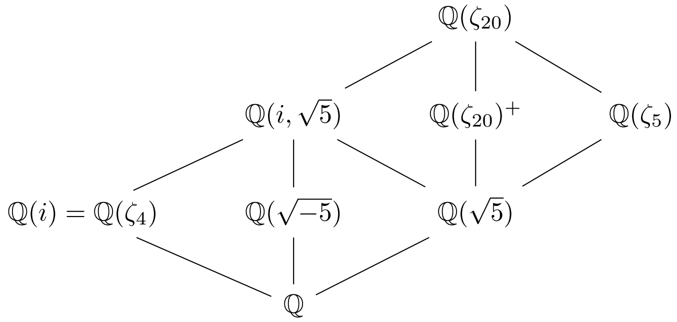
Moreover, for Galois extensions, $G = \mathrm{Gal}(K/\mathbb{Q})$ acts transitively on $\{\mathfrak{p} : \mathfrak{p} \mid p\}$, and $[K : \mathbb{Q}] = e \cdot f \cdot g$, where for p a prime of $\mathbb{Z}$:

- e is the ramification index of one (all) of the primes $\mathfrak{p}$ above p;
- f is the residue field degree, i.e. the degree of the extension $\mathcal{O}_K/\mathfrak{p} =: k_\mathfrak{p} \supseteq \mathbb{F}_p$;
- $g = \#\{\mathfrak{p} : \mathfrak{p} \mid p\}$.

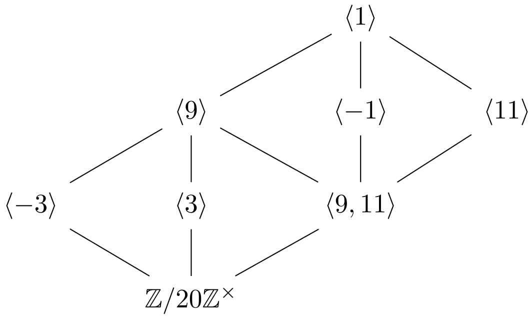
For $\mathfrak{p} \in \{\mathfrak{p} : \mathfrak{p} \mid p\}$, one takes the stabiliser $G_\mathfrak{p} = \mathrm{stab}_\mathfrak{p} \subseteq G$ and calls this the decomposition group. If the extension is unramified (i.e. $e = 1$) then this group is isomorphic via reduction to $\mathrm{Gal}(k_\mathfrak{p}/\mathbb{F}_p) = \langle \mathrm{Frob}_p \rangle$, where Frob_p is the Frobenius map $x \mapsto x^p$.

Example 1. For cyclotomic fields $G_\mathfrak{p} = \langle p \mod m\rangle$, and so $\mathbb{F}_p(\zeta_m)/\mathbb{F}_p$ has degree equal to the order of $p \in (\mathbb{Z}/m\mathbb{Z})^\times$

Example 2 (Cyclotomic fields with $m = 20$)**.** Compute for yourselves the following diagrams of subfields.



Note that the associated lattice of subgroups is



Example 3 (Cyclotomic Fields)**.** We have a correspondence

$$(\mathbb{Z}/m\mathbb{Z})^\times \leftrightarrow \mathrm{Gal}(K_m/\mathbb{Q})$$
$$p \leftrightarrow \mathrm{Frob}_p.$$

This is actually an example of a more general mapping known as the Artin symbol. Dirichlet proved that there is equidistribution here. That is, for every $a \in \mathbb{Z}/m\mathbb{Z}^\times$ the set of primes p such that $p \equiv a \mod m$ has density $1/\varphi(m)$. This is also an example of a more general phenomenon.

Theorem 4 (Dirichlet(1840's)–Frobenius–Chebotarev(1924))**.** *Let L/K be a finite Galois extension of number fields, $G = \mathrm{Gal}(L/K)$, $C \subseteq G$ be a conjugacy class. Then*

$$\{\mathfrak{p} \text{ of } K \ : \ \mathrm{Frob}_\mathfrak{p} \in C\}$$

has density (in an appropriate sense) equal to $\frac{\#C}{\#G}$.

This is a key result which is extremely important, and has many corollaries which are actually more classical, at least than Chebotarev.

Corollary 5. *Let L/K be a finite Galois extension of number fields, then*

$$\{\mathfrak{p} \ : \ \mathfrak{p} \text{ splits completely in } L/K\}$$

has density $\frac{1}{[L:K]}$.

Corollary 6. *If all $p \equiv 1 \mod m$ split in $L/\mathbb{Q}$ then $L \subseteq \mathbb{Q}(\zeta_m)$.*

Theorem 7 (Kronecker–Weber(middle of the 1800's)–Hilbert)**.** *Every finite abelian extension of $\mathbb{Q}$ is cyclotomic. That is, it is contained in a cyclotomic field $\mathbb{Q}(\zeta_m)$.*

key step of proof. If $\mathbb{Q} \subseteq L$ is totally unramified (i.e. unramified everywhere) then $\mathbb{Q} = L$. Moreover we have a map

$$\mathbb{Z}/m\mathbb{Z}^\times \to \mathrm{Gal}(L/\mathbb{Q})$$

Given by

$$p \mod m \mapsto \mathrm{Frob}_p.$$

□

Main Theorem of Class Field Theory.

Theorem 8 (CFT)**.** *Let K be a number field, and L/K be an abelian extension. Then L is a class field, i.e. it is contained in a ray class field modulo some modulus $\mathfrak{m}$, denoted $H_\mathfrak{m}$.*

Of course there are plenty of words here that need to be defined and understood, but the point is as follows: There is a 'ray class group modulo $\mathfrak{m}$' $\mathrm{Cl}_\mathfrak{m}$ generated by some set of primes $\mathfrak{p} \nmid \mathfrak{m}$ and such that

$$\begin{aligned} \mathrm{Cl}_\mathfrak{m} &\twoheadrightarrow \mathrm{Gal}(L/K) \\ [\mathfrak{p}] &\mapsto \mathrm{Frob}_\mathfrak{p}. \end{aligned}$$

By the end of this week you should hopefully see this as no more complicated than $\mathbb{Z}/m\mathbb{Z}^\times$! Let us see the definition.

Definition 9. A modulus of a number field K is a formal pair $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ where $\mathfrak{m}_0 \subseteq \mathcal{O}_K$ is a nonzero ideal and $\mathfrak{m}_\infty$ is a collection of real embeddings of K. We define the associated ray class group as follows.

$$\mathrm{Cl}_\mathfrak{m} = I(\mathfrak{m})/R_\mathfrak{m},$$

where

- $I(\mathfrak{m})$ is the group generated by the fractional ideals of K which are coprime to $\mathfrak{m}$; and
- $R_\mathfrak{m} = \langle \alpha\mathcal{O}_K \ : \ \alpha \equiv 1 \bmod^* \mathfrak{m}\rangle$ is the so-called ray modulo $\mathfrak{m}$, where $\alpha \equiv 1 \bmod^* \mathfrak{m}$ means that both for $\mathfrak{p} \mid \mathfrak{m}_0$ we have $v_\mathfrak{p}(\alpha - 1) \geq v_\mathfrak{p}(\mathfrak{m}_0)$ and for $\sigma \in \mathfrak{m}_\infty$ we have $\sigma(\alpha) > 0$.

Example 10 (Ray class groups for $\mathbb{Q}$)**.** For $K = \mathbb{Q}$ what do we get? Consider $\mathfrak{m} = \langle m\rangle$, then

$$\mathrm{Cl}_\mathfrak{m} = (\mathbb{Z}/m\mathbb{Z})^\times / \langle \pm 1\rangle .$$

If we add the infinite place and consider $\mathfrak{m} = \langle m\rangle \cdot \infty$ then

$$\mathrm{Cl}_\mathfrak{m} = \mathbb{Z}/m\mathbb{Z}^\times.$$

So we've already seen these!

Since the set of principal ideals coprime to $\mathfrak{m}$, call it $P(\mathfrak{m})$, lies between $I(\mathfrak{m})$ and $R_\mathfrak{m}$, we have a map

$$\mathrm{Cl}_\mathfrak{m} \to \mathrm{Cl}_K.$$

In fact this map is surjective, and moreover we obtain a short exact sequence

$$1 \longrightarrow (\mathcal{O}_K/\mathfrak{m})^\times / \mathrm{im}(\mathcal{O}_K^\times) \longrightarrow \mathrm{Cl}_\mathfrak{m} \longrightarrow \mathrm{Cl}_K \longrightarrow 0,$$

where $(\mathcal{O}_K/\mathfrak{m}\mathcal{O}_K)^\times = (\mathcal{O}_K/\mathfrak{m}_0)^\times \times \prod_{\sigma\in\mathfrak{m}_\infty}\langle -1\rangle$.

Every $\mathfrak{m}$ gives rise to an analogue of the cyclotomic fields, called the ray class field modulo $\mathfrak{m}$, which we denote by $H_\mathfrak{m}$.

Example 11. Consider the sets enumerated by $n \in \mathbb{Z}_{>0}$

$$S_n := \left\{p \ : \ p = x^2 + ny^2\right\}.$$

Then we know

$$S_1 = \left\{p \ : \ p = x^2 + y^2\right\} = \{p \equiv 1 \mod 4\}$$

which has density 1/2. Moreover similar results are easy enough for $n = 2, 3, 4$. This is seen by considering the factorisation of p in $\mathbb{Z}[\sqrt{-n}]$. However when we get to $n = 5$ there is a problem: the class group of $\mathbb{Z}[\sqrt{-5}]$ is $\mathbb{Z}/2\mathbb{Z}$ (not trivial), so factoring the prime p as an ideal is no longer sufficient.

Definition 12. For $\mathfrak{m} = 1$ the field $H = H_\mathfrak{m}$ is called the Hilbert class field, and $\mathrm{Cl}_K = \mathrm{Cl}_\mathfrak{m} \cong \mathrm{Gal}(H/K)$.

Lecture 2 (Stevenhagen)

Recall what we said yesterday: Class field theory is the direct generalisation of the Kronecker–Weber theorem, which gives us direct control on the abelian extensions of the rational numbers. More precisely, $L/\mathbb{Q}$ is abelian if and only if $L \subseteq \mathbb{Q}(\zeta_m)$ for some $m \in \mathbb{Z}_{>0}$. This actually gives you concrete control over the splitting behaviour of primes in this field since

$$\begin{aligned} \mathbb{Z}/m\mathbb{Z}^\times &\to \mathrm{Gal}(L/\mathbb{Q}) \\ p \mod m &\mapsto \mathrm{Frob}_p \end{aligned}$$

for $p \nmid m$.

Definition 13. The smallest m such that $L \subseteq \mathbb{Q}(\zeta_m)$ is called the conductor of $L/\mathbb{Q}$ and will be written m_L.

Remark 14. Note that $\mathbb{Q}(\zeta_m)$ needn't have conductor m: $\mathbb{Q}(\zeta_{10})$ has conductor 5, for example.

This all generalises as follows.

Theorem 15 (Class Field Theory). *K a number field then L/K is abelian if and only if $L \subseteq K_\mathfrak{m}$ for some modulus $\mathfrak{m}$ of K (where $K_\mathfrak{m}$ is the ray class field modulo $\mathfrak{m}$). We have a map*

$$\begin{aligned} \mathrm{Cl}_\mathfrak{m} &\to \mathrm{Gal}(L/K) \\ [\mathfrak{p}] &\mapsto \mathrm{Frob}_\mathfrak{p} \end{aligned}$$

which is an isomorphism if $L = K_\mathfrak{m}$.

Let $\mathfrak{m}$ be a modulus of K and note that $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty = \prod_{\mathfrak{p}\leq\infty}\mathfrak{p}^{n(\mathfrak{p})}$ and satisfies

$$n(\mathfrak{p}) \begin{cases} = 0 & \text{almost everywhere;} \\ = 0 & \text{for complex places;} \\ \leq 1 & \text{for real places.} \end{cases}$$

By definition, $\alpha \equiv 1 \bmod^* \mathfrak{m}$ if and only if $v_\mathfrak{p}(\alpha - 1) \geq n(\mathfrak{p})$ and $\sigma(\alpha) > 0$ for real places σ such that $n(\sigma) = 1$.

We have a sequence

$$\mathcal{O}_K^\times \longrightarrow \mathcal{O}_K/\mathfrak{m}^\times \longrightarrow \mathrm{Cl}_\mathfrak{m} \longrightarrow \mathrm{Cl}_K \longrightarrow 0\ .$$

Definition 16. For L/K abelian, the conductor is $\mathfrak{m}_{L/K}$ which is the minimal modulus such that $L \subseteq K_\mathfrak{m}$.

Below are some properties of the conductor:

- $\mathfrak{p} \mid \mathfrak{m}_{L/K}$ if and only if $\mathfrak{p}$ ramifies (by convention, a real embedding ramifies in L/K if its extension to L is complex).
- $\mathfrak{p}^2 \mid \mathfrak{m}_{L/K}$ if and only if $\mathfrak{p}$ is wildly ramified (meaning the ramification index $e_{L/K} \equiv 0 \mod p$ for p the prime number below $\mathfrak{p}$).

Recall the norm map $N_{L/K} : L^\times \to K^\times$, which can be extended to the ideals $I_L \to I_K$ and maps $\mathfrak{q} \mid \mathfrak{p}$ via $\mathfrak{q} \mapsto N_{L/K}\mathfrak{q} = \mathfrak{p}^{f(\mathfrak{q}/\mathfrak{p})}$. Using this we can define Artin's reciprocity law.

Theorem 17 (Artin's reciprocity law)**.** *The maps on Frobenii above induce an isomorphism*

$$\frac{I_K(\mathfrak{m})}{N_{L/K}I_L(\mathfrak{m}) \cdot R_\mathfrak{m}} \cong \mathrm{Gal}(L/K).$$

Maximal Abelian Extensions. The maximal abelian extension of $\mathbb{Q}$, denoted $\mathbb{Q}^{\mathrm{ab}}$, is, by the Kronecker–Weber theorem, equal to $\cup_{n\geq 1}\mathbb{Q}(\zeta_n)$. In fact

$$\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) \cong \widehat{\mathbb{Z}}^\times.$$

1. Idéles

Let K be a number field. Define the notation

Notation 18. For a prime ideal $\mathfrak{p}$, we let $A_\mathfrak{p}$ be the integers in the completion $K_\mathfrak{p}$ and $U_\mathfrak{p}$ be the units of $A_\mathfrak{p}$. For $n \geq 1$ we write $U_\mathfrak{p}^{(n)} = 1 + \mathfrak{p}^n \subseteq U_\mathfrak{p} = U_\mathfrak{p}^{(0)}$. We will write $\pi_\mathfrak{p}$ for a uniformizer of $A_\mathfrak{p}$.

For an infinite place v, if v is complex then we define $U_\mathfrak{p}^{(0)} = \mathbb{C}^\times$ and if it is real then $U_\mathfrak{p}^{(0)} = \mathbb{R}^\times$ and $U_{\mathfrak{p}^{(1)}} = \mathbb{R}_{>0}$.

Definition 19. The adèle ring is the restricted product

$$\mathbb{A}_K = \prod_{\mathfrak{p}\leq\infty}{}' K_\mathfrak{p} = \{(x_\mathfrak{p})_\mathfrak{p}\ :\ x_\mathfrak{p} \in A_\mathfrak{p} \text{ for almost all } \mathfrak{p}\}\,.$$

The idèle group is the restricted product

$$\mathbb{A}_K^* = \prod_{\mathfrak{p}\leq\infty}{}' K_\mathfrak{p}^* = \{(x_\mathfrak{p})_\mathfrak{p}\ :\ x_\mathfrak{p} \in U_\mathfrak{p} \text{ for almost all } \mathfrak{p}\}\,.$$

These groups come with natural product topologies.

Definition 20. For a finite abelian extension L/K the Artin map is defined by

$$\begin{aligned} \mathbb{A}_K^\times &\to \mathrm{Gal}(L/K) \\ \pi_\mathfrak{p} &\mapsto \mathrm{Frob}_\mathfrak{p} \end{aligned}$$

for $\mathfrak{p} \nmid \mathfrak{m}_{L/K}$, where $\pi_\mathfrak{p}$ is identified with $(1, \dots, 1, \pi_\mathfrak{p}, 1, \dots, 1)$.

Definition 21. For a modulus $\mathfrak{m} = \prod_{\mathfrak{p} \leq \infty} \mathfrak{p}^{n(\mathfrak{p})}$ we define the subgroup $W_{\mathfrak{m}} \subset \mathbb{A}_K^\times$ by

$$W_{\mathfrak{m}} = \prod_{\mathfrak{p} \leq \infty} U_{\mathfrak{p}}^{(n(\mathfrak{p}))}$$

Lemma 22. *$H \subset \mathbb{A}_K^\times$ is an open subgroup if and only if $H \supset W_{\mathfrak{m}}$ for some modulus $\mathfrak{m}$.*

The key lemma is

Lemma 23. *For every modulus $\mathfrak{m}$, there is an isomorphism*

$$\begin{aligned} \mathbb{A}_K^\times/(K^* W_{\mathfrak{m}}) &\cong \mathrm{Cl}_{\mathfrak{m}} \\ [\pi_{\mathfrak{p}}] &\mapsto [\mathfrak{p}], \end{aligned}$$

for $\mathfrak{p} \nmid \mathfrak{m}$.

Proof. Exercise. □

Definition 24. The idèle class group of K is $\mathbb{A}_K^\times/K^\times$.

Another way to phrase class field theory is the following.

Theorem 25.

$$\left\{K^{\mathrm{ab}} \supset L \supset K\right\} \leftrightarrow \left\{\text{Open subgroups of } \mathbb{A}_K^\times/K^\times\right\}.$$

Moreover L corresponds to $K^\times N_{L/K} \mathbb{A}_L^\times \mod K^\times$.

Remark 26. Note that $\mathbb{A}_L = L \otimes \mathbb{A}_K$, and so in particular there is a natural norm map $N_{L/K} : \mathbb{A}_L \to \mathbb{A}_K$ which restricts on $L^\times \subset \mathbb{A}_L$ to the usual norm map to K.

Example 27. Consider $K = \mathbb{Q}$. Then $\mathbb{A}_{\mathbb{Q}}^\times = \prod_p' \mathbb{Q}_p^\times \times \mathbb{R}$. In fact it is not hard to construct the isomorphism

$$\widehat{\mathbb{Z}}^\times \times \mathbb{R}_{>0} = \prod_p \mathbb{Z}_p^* \times \mathbb{R}_{>0} \cong \mathbb{A}_{\mathbb{Q}}^\times/\mathbb{Q}.$$

The discriminant of an abelian extension L/K can be written as

$$\Delta_{L/K} = \prod_{\chi \in \widehat{G}} \mathfrak{m}_\chi,$$

where for a character $\chi \in \widehat{G}$ $\mathfrak{m}_\chi$ is the conductor of the subfield $L^{\ker(\chi)} \subset L$.

Example 28. $\Delta_{\mathbb{Q}(\zeta_p)/\mathbb{Q}} = \pm p^{p-2}$

Theorem 29 (Local-Global)**.** *The diagram below commutes for every abelian extension L/K, every $\mathfrak{p}$ of K and $\mathfrak{q}$ of L such that $\mathfrak{q} \mid \mathfrak{p}$.*

$$\begin{tikzcd}
\mathbb{A}_K^\times/N_{L/K}\mathbb{A}_L^\times \cdot K^\times \arrow[r, "\sim"] & \mathrm{Gal}(L/K) \\
K_{\mathfrak{p}}^\times/N_{L/K}L_{\mathfrak{q}}^\times \arrow[r, "\sim"] \arrow[u] & \mathrm{Gal}(L_{\mathfrak{q}}/K_{\mathfrak{p}}). \arrow[u]
\end{tikzcd}$$

1.1. **Euler's Conjectures.** Below are questions and observations of Euler.

(1) For $p \equiv 1 \mod 3$, is $2 \in \mathbb{F}_p^{\times 3}$? This is equivalent to $p = x^2 + 27y^2$ for $x, y \in \mathbb{Z}$

(2) For $p \equiv 1 \mod 4$, is $2 \in \mathbb{F}_p^{\times 4}$? This is equivalent to $p = x^2 + 64y^2$ for $x, y \in \mathbb{Z}$.

Using our modern class field theoretic knowledge, we can take the following perspective. 1 is determined by the splitting behaviour of p in $x^3 - 2$, and similarly 2 is determined by the splitting behaviour of p in $x^4 - 2$.

We leave this as an exercise in the interest of time.

Lecture 3 (Schoof): Class Field Theory via Group Cohomology

This goes back to the Artin–Tate seminar in the 1950's, but you can find it in Cassels–Fröhlich, or in Serre's Corps Locaux. We will begin by talking about group cohomology.

Group Cohomology

Let G be a finite group and $\mathbb{Z}[G]$ the group ring. We have the category of (left) $\mathbb{Z}[G]$-modules, Gmod, (sometimes we will just say G-modules), and a functor

$$\text{Gmod} \to \text{Ab}$$

given by $M \mapsto M^G = \{m \in M : \sigma(m) = m \ \forall \sigma \in G\}$. We have right derived functors of this

$$M \mapsto H^k(G, M),$$

where for $k = 0$ note $H^0(G, M) = M^G$. We call these groups the cohomology groups. Moreover every short exact sequence in Gmod

$$0 \to A \to B \to C \to 0,$$

gives a long exact sequence of cohomology groups.

How are these constructed? Take a free resolution of $\mathbb{Z}$, with trivial G action,

$$\cdots \to F_1 \to F_0 \to \mathbb{Z} \to 0.$$

Apply $\text{Hom}_G(-, M)$ to this for M your G-module, and then take the cohomology of the complex

$$0 \longrightarrow \text{Hom}_G(F_0, M) \xrightarrow{\partial} \text{Hom}_G(F_1, M) \xrightarrow{\partial} \text{Hom}_G(F_2, M) \xrightarrow{\partial} \text{Hom}_G \ldots,$$

meaning that you take the group $\ker(\partial)/\text{im}(\partial)$ in $\text{Hom}_G(F_k, M)$ and call it $H^k(G, M)$.

This is nice, and doesn't depend on the choice of complex. Generally we prefer to take the standard complex, which is given as follows.

$$F_i = \mathbb{Z}[G^{i+1}]$$

with the maps

$$\partial : F_n \to F_{n-1}$$

given by $(g_1, \ldots, g_{n+1}) \mapsto \sum_{i=1}^{n+1} (-1)^i (g_1, \ldots, \widehat{g_i}, \ldots, g_{n+1})$, where the hat means that we exclude this term. Some example computations with this are as follows.

Example 30.

$$\begin{aligned} H^0(G,M) &= M^G \\ H^1(G,M) &= \frac{\{f : G \to M \ : \ f(\sigma\tau) = \sigma(f(\tau)) + f(\sigma)\}}{\{\sigma \mapsto \sigma(m) - m \ : \ m \in M\}} \end{aligned}$$

An explicit one:

$$H^1(G,\mathbb{Z}) = \mathrm{Hom}(G,\mathbb{Z}) = 0.$$

Another:

$$H^1(G,\mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z}) \cong G_{\mathrm{ab}}^{\mathrm{dual}}$$

A useful result about these groups is the following.

Theorem 31 (Hilbert 90). *Let L/K be a finite Galois extension with Galois group G. Then*

$$H^1(G,L^\times) = 0.$$

Proof. For a 1-cocycle f, note that by the linear independence of automorphisms of fields, the sum $\sum_{\sigma\in G} f(\sigma)\sigma \neq 0$ is a nonzero map $L^\times \to L^\times$. Take $\alpha \in L^\times$ with nonzero image and define

$$\beta := \sum_{\sigma\in G} f(\sigma)\sigma(\alpha) \neq 0.$$

Then for $\tau \in G$ note that

$$\tau(\beta) = \prod_{\sigma\in G} \tau(f(\sigma))\tau\sigma(\alpha) = \frac{1}{f(\tau)} \prod_{\sigma\in G} f(\tau\sigma)\tau\sigma(\alpha) = \frac{1}{f(\tau)}\beta.$$

In particular, f is the coboundary $\tau \mapsto \beta/\tau(\beta)$. □

Induced Modules. It is quite easy to show that if M is a free $\mathbb{Z}[G]$-module, then for all $q \geq 1$

$$H^q(G,M) = 0.$$

Moreover, there is the notion of an induced G-module:

$$M = \mathbb{Z}[G] \otimes X$$

where X is any abelian group. This module also satisfies, for all $q \geq 1$,

$$H^q(G,M) = 0.$$

Note that these are enough to conclude that if L/K is finite Galois with Galois group G then for all $q \geq 1$

$$H^q(G,L) = 0,$$

since $L \cong K[G] = K \otimes \mathbb{Z}[G]$.

Tate Cohomology. These groups are $\widehat{H}^k(G,M)$ for $k \in \mathbb{Z}$, where for $k > 0$ we define $\widehat{H}^k(G,M) := H^k(G,M)$. For non-positive k we need to do some defining. We do this with a complete resolution.

$$\begin{tikzcd}
\dots \arrow[r] & \mathbb{Z}[G^2] \arrow[r] & \mathbb{Z}[G] \arrow[rr, "N_G=\sum_{\sigma\in G}\sigma"] \arrow[dr, "\sigma\mapsto 1"] & & \mathbb{Z}[G] \arrow[r] & \mathbb{Z}[G^2] \arrow[r] & \dots \\
& & & \mathbb{Z} \arrow[ur] \arrow[dr] & & & \\
& & 0 \arrow[ur] & & 0 & &
\end{tikzcd}$$

As before, apply $\mathrm{Hom}_G(-,M)$ and take the cohomology of the complex on the top line. As some special computational cases we have

$$\widehat{H}^k(G,M) = \begin{cases} H^k(G,M) & \text{if } k \geq 1 \\ M^G/N_G(M) & \text{if } k = 0 \\ \ker(N_G)/\left\{(\sigma-1)m \ : \ m \in M,\ \sigma \in G\right\} & \text{if } k = -1 \\ H_{-k-1}(G,M) & \text{if } k \leq -2 \end{cases}$$

where the final groups for the negative case are homology groups, obtained by a similar construction to cohomology but using the covariants functor.

Example 32 (Trivial Module)**.**

$$\begin{aligned} H^1(G,\mathbb{Z}) &= 0 \\ \widehat{H}^0(G,\mathbb{Z}) &= \mathbb{Z}/\#G\mathbb{Z} \\ \widehat{H}^{-1}(G,\mathbb{Z}) &= 0 \\ \widehat{H}^{-2}(G,\mathbb{Z}) &= \widehat{H}^{-1}(G,I) \cong I/I^2 \cong G_{\mathrm{ab}} \end{aligned}$$

where $I := \langle \sigma - 1 \ : \ \sigma \in G\rangle \subseteq \mathbb{Z}[G]$ is the augmentation ideal. The final isomorphism is given in reverse by $\sigma \mapsto (\sigma - 1)$

Local Class Field Theory

Let L/K be a finite Galois extension of local fields with $G = \mathrm{Gal}(L/K)$, and write $n = \#G$. There are canonical isomorphisms for all $q \in \mathbb{Z}$:

$$\widehat{H}^q(G,\mathbb{Z}) \xrightarrow{\sim} \widehat{H}^{q+2}(G,L^\times)$$

As examples note that for $q = -1$ we get $0 = 0$ and for $q = 0$ we obtain $\mathbb{Z}/n\mathbb{Z} = H^2(G,L^\times)$. For $q = -2$ we obtain

$$G_{\mathrm{ab}} \cong K^\times/N_{L/K}L^\times$$

which we refer to as the reciprocity isomorphism.

The Isomorphism. How is this isomorphism defined?

Definition 33. We have pairings for $M, N \in \mathrm{Gmod}$

$$\widehat{H}^p(G,M) \otimes \widehat{H}^q(G,N) \to \widehat{H}^{p+q}(G,M \otimes N)$$

referred to as the cup products.

Then the isomorphisms above are given by the cup product

$$\widehat{H}^q(G,\mathbb{Z}) \otimes \widehat{H}^2(G,L^\times) \to \widehat{H}^{q+2}(G,L^\times)$$

where we cup with the element $1 \in \mathbb{Z}/n\mathbb{Z} \cong H^2(G,L^\times)$ where the isomorphism is the precise one above.

Global Class Field Theory

If L/K is a finite Galois extension of number fields, and $G = \mathrm{Gal}(L/K)$ and $n = \#G$ as before, then this works out similarly but now with the Idèle class group.

$$\widehat{H}^q(G,\mathbb{Z}) \xrightarrow{\sim} \widehat{H}^{q+2}(G,\mathbb{A}_L^\times/L^\times) \ .$$

For $q = -1$ we again get $0 = 0$, because $H^1(G,\mathbb{A}_L^\times/L^\times) = 0$.

Dimension Shifting.

Proposition 34 (Dimension Shifting)**.** *For every $M \in \mathrm{Gmod}$, there exists a module J with trivial cohomology and $M \subseteq J$, and similarly there is a J' with trivial cohomology and a surjection $M \to J'$.*

Proof. Set

$$\begin{aligned} J' = M \otimes \mathbb{Z}[G] &\to M \\ m \otimes \sigma &\mapsto \sigma(m) \\ M &\to J = \mathrm{Hom}(\mathbb{Z}[G], M) \\ m &\mapsto (\sigma \mapsto \sigma^{-1}(m)) \end{aligned}$$

Note that these are cohomologically trivial because they are induced. □

This allows us to take short exact sequences

$$0 \longrightarrow \ker \longrightarrow J' \longrightarrow M \longrightarrow 0,$$

and

$$0 \longrightarrow M \longrightarrow J \longrightarrow \mathrm{coker} \longrightarrow 0,$$

and compute cohomology. Since the middle terms are cohomologically trivial we get isomorphisms

$$\widehat{H}^q(G,M) \cong \widehat{H}^{q+1}(G,\ker),$$
$$\widehat{H}^q(G,M) \cong \widehat{H}^{q-1}(G,\mathrm{coker}).$$

and equate cohomology of M with that which is one degree lower (resp. higher) of the cokernel (resp. kernel). This is why we call it ‘dimension shifting’: we can increase or decrease the cohomological degree somewhat freely by switching the module. An example application is the following corollary.

Corollary 35. *For all $q \in \mathbb{Z}$, and all $M \in \mathrm{Gmod}$, the group $\widehat{H}^q(G,M)$ is $\#G$-torsion.*

Proof. By dimension shifting (Proposition 34) it is sufficient to prove this for $q = 0$, and in this case

$$\widehat{H}^q(G, M) = M^G/N_G(M).$$

For $m \in M^G$ note that $\#G \cdot m = N_G(m)$, showing the result. □

Class Field Theory. Okay, returning to Class Field Theory. We have an exact grid

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & \mathcal{O}_L^\times \arrow[r] \arrow[d] & L^\times \arrow[r] \arrow[d] & \mathrm{PId}_L \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & U_L \arrow[r] \arrow[d] & \mathbb{A}_L^\times \arrow[r] \arrow[d] & I_L \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & Q_L \arrow[r] \arrow[d] & \mathbb{A}_L^\times/L^\times \arrow[r] \arrow[d] & \mathrm{Cl}_L \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

where

$$\begin{aligned}
\mathbb{A}_L^\times &\to I_L \\
(x_\mathfrak{p}) &\mapsto \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(x_\mathfrak{p})} \\
U_L &:= \left\{(x_\mathfrak{p})_\mathfrak{p} \in \mathbb{A}_L^\times \ : \ v_\mathfrak{p}(x_\mathfrak{p}) = 0 \ \forall \mathfrak{p}\right\}.
\end{aligned}$$

People usually do class field theory by going from the top left to bottom right via the L-shape in the top right of this diagram. In fact it is much easier to to the bottom left!

$$0 \longrightarrow \mathcal{O}_L^\times \longrightarrow U_L \longrightarrow \mathbb{A}_L^\times/L^\times \longrightarrow \mathrm{Cl}_L \longrightarrow 0 \ .$$

Global class field theory is obtained by studying the cohomology of the idèle class group $\mathbb{A}_L^\times/L^\times$. It is in some sense proved using local class field theory. Where does this come in? Note that the U_L term satisfies $U_L = \prod_\mathfrak{p} \mathcal{O}_\mathfrak{p}^\times$ and there is the sequence

$$0 \to \mathcal{O}_\mathfrak{p}^\times \to K_\mathfrak{p}^\times \to \mathbb{Z} \to 0$$

which relates

$$\widehat{H}^q(G, U_L) = \prod_\mathfrak{p} \widehat{H}^q(G_\mathfrak{p}, \mathcal{O}_\mathfrak{p}^\times)$$

to $\widehat{H}^q(G, K_\mathfrak{p}^\times)$, which is the main object of study in local class field theory.

Lecture 4 (Stevenhagen)

Let K be a number field, and L/K a finite Galois extension. Recall that we have seen Artin's reciprocity law.

Theorem 36 (Artin Reciprocity)**.** *If $\mathfrak{m} = \mathfrak{m}_{L/K}$ is the conductor, then there is a unique continuous surjection*

$$\begin{tikzcd}
K_{\mathfrak{p}} \arrow[r] & \mathbb{A}_K^\times/K^\times \arrow[r] \arrow[d] & \mathrm{Gal}(L/K) \\
& \mathbb{A}_K^\times/K^\times W_{\mathfrak{m}} \arrow[r, "\sim"] & \mathrm{Cl}_{\mathfrak{m}} \arrow[u]
\end{tikzcd}$$

where the top row composes to send, for $\mathfrak{p}$ an unramified prime,

$$\pi_{\mathfrak{p}} \mapsto \mathrm{Frob}_{\mathfrak{p}}.$$

This is the only theorem you need to remember for Global Class Field Theory. In fact this induces

$$\begin{tikzcd}
\mathbb{A}_K^\times/K^\times N_{L/K}\mathbb{A}_L^\times \arrow[r, "\sim"] & \mathrm{Gal}(L/K) \\
K_{\mathfrak{p}}^\times/N_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}L_{\mathfrak{q}}^\times \arrow[r, "\sim"] \arrow[u] & G_{\mathfrak{p}} \arrow[u]
\end{tikzcd}$$

where the vertical arrows are injections.

Exercise 37. Show that

- $\mathfrak{p}$ unramified means that $N(U_{\mathfrak{q}}) = U_{\mathfrak{p}} = U_{\mathfrak{p}}^{(0)}$;
- $\mathfrak{p}$ tamely ramified means that $N(U_{\mathfrak{q}}) \supset 1 + \mathfrak{p} = U_{\mathfrak{p}}^{(1)}$

Question 38. *Why is this called reciprocity?*

Let us make an extended example. Consider the Legendre symbol for $a \in \mathbb{Z}$, $p \nmid 2a$ a prime then

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \in \mathbb{F}_p^{\times 2} \\ -1 & \text{if } a \notin \mathbb{F}_p^{\times 2} \end{cases}$$

Note that this precisely determines the splitting behaviour of p in $\mathbb{Q}(\sqrt{a})$.

Theorem 39 (Euler)**.**

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$$

Definition 40.

$$\left(\frac{a}{p}\right) = \frac{\mathrm{Frob}_p(\sqrt{a})}{\sqrt{a}}$$

In fact the conductor of $\mathbb{Q}(\sqrt{a})/\mathbb{Q}$ is exactly the discriminant.

Conjecture 41 (Euler (experimentally))**.** $\left(\frac{a}{p}\right)$ *only depends on $p \in \mathbb{Z}/4a\mathbb{Z}^\times$. Moreover, if $a > 0$ then the same is true but we only need to look in $(\mathbb{Z}/4a\mathbb{Z}^\times)/\{\pm 1\}$.*

This is proved in Gauss' quadratic reciprocity law.

Theorem 42 (Gauss' Quadratic Reciprocity Law)**.** *if $p \neq q$ are odd primes then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{2}}.$$

Note that if p is odd and $p^* = \pm p$ is the choice for which $p \equiv 1 \mod 4$, then we have a diagram of the form

$$\begin{tikzcd}
\mathbb{Q}(\zeta_p) \arrow[d, dash] \\
\mathbb{Q}(\sqrt{p^*}) \arrow[d, dash] \\
\mathbb{Q}
\end{tikzcd},$$

in which the splitting behaviour of q determines $(-1)^{(q-1)/2}\left(\frac{p}{q}\right)$. If one of our primes is 2 then the associated diagram of fields is a little more complicated:

$$\begin{tikzcd}
 & \mathbb{Q}(\zeta_8) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{-1}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{-2}) \arrow[d, dash] & \mathbb{Q}(\sqrt{2}) \arrow[dl, dash] \\
 & \mathbb{Q}. &
\end{tikzcd}$$

Proof of Quadratic Reciprocity. If $p \not\equiv q \mod 4$ then $p + q = 4a > 0$. Then

$$\left(\frac{p}{q}\right) = \left(\frac{p+q}{q}\right) = \left(\frac{4a}{q}\right) = \left(\frac{a}{q}\right) = \left(\frac{a}{p}\right) = \left(\frac{q}{p}\right).$$

Else if they are the same then do the same but with $p - q$. □

Question 43. *How do we create some kind of higher reciprocity?*

Maybe you want to define cubic reciprocity, so you take a prime $p \equiv 1 \mod 3$ and define $\left(\frac{2}{p}\right)_3$ to be 1 if 2 is a cube mod p. Then this is 1 if and only if $p = x^2 + 27y^2$.

Maybe since we're looking at cube roots, we should look at a field (instead of $\mathbb{Q}$) which has third roots of unity, i.e. $K = \mathbb{Q}(\zeta_3)$. Then if $\mathfrak{p} \nmid 3$ we must have $3 \mid \#k_{\mathfrak{p}}$, and we can define a Legendre-type symbol as above and show

$$\langle \zeta_3 \rangle \ni \left(\frac{\alpha}{\mathfrak{p}}\right)_3 \equiv \alpha^{(N(\mathfrak{p})-1)/3}.$$

This is equivalent to the following.

Definition 44. define

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_3 = \frac{\mathrm{Frob}_{\mathfrak{p}}(\sqrt[3]{\alpha})}{\sqrt[3]{\alpha}},$$

where the Frobenius is in the extension $K(\sqrt[3]{\alpha})/K$.

Note that again this is determined by splitting behaviour of $\mathfrak{p}$.

Kummer Theory. Let F be a field such that $\zeta_n \in F^\times$. Then there is a bijection between

$$\{E/F \ : \ \text{finite Galois with } n\mathrm{Gal}(E/F) = 0\}$$

and

$$\left\{F^{\times n} \subseteq W \subseteq F^\times\right\}.$$

This is given by $W \mapsto F(\sqrt[n]{W})$, and $E \mapsto E^{\times n} \cap F^{\times}$. Note we have a pairing

$$\mathrm{Gal}(E/F) \times W/F^{\times n} \to \langle \zeta_n \rangle$$

given by $(\sigma, w) \mapsto \sigma(\sqrt[n]{W})/\sqrt[n]{W}$. Using class field theory to identify $\mathrm{Gal}(E/F)$ with $F^{\times}/N_{E/F}E^{\times}$ we obtain a pairing induced by

$$\begin{aligned} F^{\times}/F^{\times n} \times F^{\times}/F^{\times n} &\to \langle \zeta_n \rangle \\ (\alpha, \beta) &\mapsto \frac{\sigma_\alpha(\sqrt[n]{\beta})}{\sqrt[n]{\beta}} =: (\alpha, \beta)_{F,n}\,. \end{aligned}$$

We call this the norm residue symbol. Below are some properties of this.

- $(\alpha, \beta)_{F,n} = 1$ if and only if $a \in N(F(\sqrt[n]{\beta})^{\times})$.
- $(-\beta, \beta)_{F,n} = 1 = (1 - \beta, \beta)_{F,n}$.
- $(\alpha, \beta)_{F,n} = 1$ if $\alpha, \beta, n \in U_F$.
- $(\alpha, \beta)_{F,n} = (\beta, \alpha)_{F,n}^{-1}$. This follows from the second property. A proof:

$$1 = (\alpha\beta, -\alpha\beta)_{F,n} = (\alpha, -\alpha)\,(\alpha, \beta)_{F,n}\,(\beta, \alpha)_{F,n}\,(\beta, -\beta)_{F,n} = (\alpha, \beta)_{F,n}\,(\beta, \alpha)_{F,n}$$

Return to CFT. Assume that $\zeta_n \in K^{\times}$.

Definition 45. Let $S = \{\mathfrak{p} \;:\; \mathfrak{p} \mid n\infty\}$, and for $\alpha \in K^{\times}$ let $S(\alpha) = S \cup \{\mathfrak{p} \;:\; v_{\mathfrak{p}}(\alpha) \neq 0\}$ Define the nth power residue symbol for $\mathfrak{p} \in S(\alpha)$ by

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_n = \frac{\mathrm{Frob}_{\mathfrak{p}}(\sqrt[n]{\alpha})}{\sqrt[n]{\alpha}} \in \langle \zeta_n \rangle\,,$$

where Frobenius is in $K(\sqrt[n]{\alpha})/K$ which is unramified for $\mathfrak{p} \in S(\alpha)$ and abelian of exponent n.

Remark 46. Note that this symbol only depends on $[\mathfrak{p}] \in \mathrm{Cl}_{K,\mathfrak{p}}$ where we take $\mathfrak{m} \mid n^* \{\mathfrak{p} \;:\; v_{\mathfrak{p}}(\alpha) \neq 0 \mod n\}$.

We can then define a more general symbol multiplicatively.

Definition 47. We define the 'n-power Jacobi symbol' to be

$$\left(\frac{\alpha}{\beta}\right)_n = \prod_{\mathfrak{p} \notin S(\alpha)} \left(\frac{\alpha}{\mathfrak{p}}\right)_n^{v_{\mathfrak{p}}(\beta)}.$$

Theorem 48 (Power Reciprocity Law)**.**

$$\left(\frac{\alpha}{\beta}\right)_n \left(\frac{\beta}{\alpha}\right)_n^{-1} = \prod_{\mathfrak{p} \in S(\alpha) \cap S(\beta)} (\alpha, \beta)_{n,\mathfrak{p}},$$

where $(\alpha, \beta)_{n,\mathfrak{p}}$ *is the* n *norm residue symbol above for* $K_{\mathfrak{p}}$.

Example 49. If $K = \mathbb{Q}$, $n = 2$, a, b both odd, then

$$\left(\frac{a}{b}\right)_2 \left(\frac{b}{a}\right)_2 = (a, b)_2\,(a, b)_\infty\,.$$

For the pairing at 2 note that $a, b \in \mathbb{Z}_2^{\times}$ by assumption, and $\mathbb{Z}_2^{\times}/\mathbb{Z}_2^{\times} \cong \mathbb{Z}/8\mathbb{Z}^{\times}$. Since this is generated by $-1, 5$ we can compute to obtain that the symbol is given by

	-1	5
-1	-1	1
5	1	1

For the infinite pairing we have $\mathbb{R}^\times/\mathbb{R}^{\times 2} = \langle -1\rangle$ and so the pairing is nontrivial if and only if both $a, b < 0$.

Exercise 50. $n = 3$, $K = \mathbb{Q}(\zeta_3) \supset \mathcal{O}_K = \mathbb{Z}[\zeta_3]$, $\mathcal{O}_K^\times = \langle -\zeta_3\rangle$. This has class number 1, let $\pi \in \mathcal{O}_K$ be a prime element with $\pi \equiv 1 \mod 3 = (1-\zeta_3)^2$ then show that

$$\left(\frac{\pi_1}{\pi_2}\right)_3 = \left(\frac{\pi_2}{\pi_1}\right)_3 .$$

Once you've done this, look at $n = 4$.

Quadratic reciprocity became trivial if you assumed class field theory, in fact the same is true for all of these reciprocity laws.

Theorem 51 (Product Formula)**.** *For $\alpha, \beta \in K^\times \ni \zeta_n$, then*

$$\prod_{\mathfrak{p}\leq\infty} (\alpha,\beta)_{n,\mathfrak{p}} = 1$$

How does this compare to Artin reciprocity?

Proof.

$$\begin{tikzcd}
\prod'_{\mathfrak{p}\leq\infty} K_{\mathfrak{p}}^\times \arrow[r] \arrow[d] & \oplus_{\mathfrak{p}}\mathrm{Gal}(K_{\mathfrak{p}}(\sqrt[n]{\beta})/K) \arrow[d, "(\sigma_{\mathfrak{p}})\mapsto\prod_{\mathfrak{p}}\sigma_{\mathfrak{p}}"] \\
\mathbb{A}_K^\times/K^\times \arrow[r] & \mathrm{Gal}(K(\sqrt[n]{\beta})/K).
\end{tikzcd}$$

Note that $\alpha \in K$, considered in the top left, gets mapped to the left hand side of the product formula if we go via the top right, and to 1 trivially if we go via the bottom left. □

Lecture 5 (Stevenhagen)

Rédei's Reciprocity Law

We will now discuss a result which is from the 21st century: Rédei's reciprocity law.

Statement. We'll start with the final result, don't worry that we don't know what the symbol is yet!

Theorem 52 (Rédei's Reciprocity)**.** *For $x \in \mathbb{Q}^\times$ we write $\Delta(x) = \mathrm{disc}(\mathbb{Q}(\sqrt{x}))$. Let $a, b, c \in \mathbb{Q}^\times$ be such that both of the following hold.*

- $\gcd(\Delta(a), \Delta(b), \Delta(c) = 1$.
- *For all $p \leq \infty$, $(a, b)_p = (a, c)_p = (b, c)_p = 1$.*

Then the Rédei symbol $[a, b, c] \in \{\pm 1\} \cong \mathbb{F}_2$ satisfies

$$[a, b, c] = [b, a, c] = [a, c, b].$$

The original result was restricted and due to Rédei (1939), later work was then done by a PhD student in Canada called Corsman (2007) but there were some issues with the proof which have since been corrected by Stevenhagen.

. Let $K = \mathbb{Q}(\sqrt{D})$ with $D = \mathrm{disc}(K) = \begin{cases} d & d \equiv 1 \mod 4 \text{ squarefree} \\ 4d & d \equiv 2,3 \mod 4\text{squarefree} \end{cases}$. Let $C = C_D$ be the (narrow) class group, given by

$$C_D = I/P^+$$

where I is the ideal group and $P^+ = \left\{ \langle \alpha \rangle \ : \ \alpha \in K,\ N_{K/\mathbb{Q}}(\alpha) > 0 \right\}$ are the positive principal ideals. Note that is the group $\mathrm{Cl}_{\infty_1,\infty_2}$ if K is real and Cl_K if K is complex.

Stevenhagen's Conjecture. If $D > 0$ then $\mathrm{Cl}_{\infty_1,\infty_2} = \mathrm{Cl}_K$ if and only if $N_{K/\mathbb{Q}}(\varepsilon_D) = -1$ where ε_D a choice of fundamental unit. Note the link to the negative Pell equation: $x^2 - dy^2 = -1$, for which there was a conjecture of Stevenhagen (1992) (now a theorem of Koymans–Pagano (2022)) that if

$$\mathcal{D} = \left\{ d > 0 \ : \ \substack{d \text{ is squarefree} \\ \text{no } p \equiv 3 \mod 4 \text{ divides } d} \right\}$$
$$\mathcal{D}^- = \left\{ d > 0 \ : \ x^2 - dy^2 \text{ is solvable over } \mathbb{Z} \right\}$$

then $\mathcal{D}^-$ has density around 58% (actually an explicit infinite product in powers of 2) in $\mathcal{D}$.

Class Groups Again. We are interested in the 2-part of C_D, where $D = \mathrm{disc}(\mathbb{Q}(\sqrt{D}))$. Gauss showed a bijection

$$C_D \leftrightarrow \mathcal{F}/\mathrm{SL}_2(\mathbb{Z})$$
$$\left\langle a, \frac{b + \sqrt{D}}{2} \right\rangle \leftrightarrow [(a,b,c)]$$

where $\mathcal{F}_D$ are the binary quadratic forms $aX^2 + bXY + cY^2$ with discriminant $D = b^2 - 4ac$ (note $a > 0$ if $D < 0$), and are acted on by $\mathrm{SL}_2(\mathbb{Z})$ as change of coordinates $\gamma \cdot f(x,y) = f(\gamma(x,y))$. On the left hand side are the 'ambiguous ideal classes': for $p \mid D$ we have $p\mathcal{O}_K = \mathfrak{p}^2$. In fact these generate

$$C_D[2] \cong \mathbb{Z}/2\mathbb{Z}^{t-1}$$

where $t = \#\{p \ : \ p \mid D\}$. Via Artin we have an isomorphism

$$C_D \cong \mathrm{Gal}(H^+/K)$$

where H^+/K is the narrow class field: the maximal abelian extension of K which is unramified at all finite places. We write $\mathfrak{G}$ for the genus field, identified below.

$$\begin{tikzcd}
 & H^+ \arrow[dd, dash, "C"] \\
\mathfrak{G} \arrow[ur, dash, "2C"'] & \\
 & K \arrow[ul, dash, "C/2C"] \arrow[d, dash] \\
 & \mathbb{Q}
\end{tikzcd}.$$

For p odd write $p^* = \pm p \equiv 1 \mod 4$ and write $2^* \in \{1, -4, \pm 8\}$ so that $D = \prod_{p \mid D} p^*$. Then in fact $\mathfrak{G} = \mathbb{Q}(\{\sqrt{p^*} \ : \ p \mid D\})$. Note that this really is unramified over K: adjoining $\sqrt{p^*}$ to K will at worst ramify above p but the ramification has already taken place when we adjoined $\sqrt{D}$ to $\mathbb{Q}$ to get K.

Example 53. If $K = \mathbb{Q}(\sqrt{-14})$ then we get $D = 8 \times -7$

$$\begin{tikzcd}
H \arrow[d, dash, "2"] \\
\mathfrak{G} = \mathbb{Q}\left(\sqrt{-7}, \sqrt{2}\right) \arrow[d, dash, "2"] \\
\mathbb{Q}(\sqrt{-14})
\end{tikzcd}$$

Note that since C is a finite abelian group, we have $C[2] \cong C/2C$. In general if A is a finite abelian 2-group then it has 2^k-ranks which totally determine its structure.

Definition 54. The 2^k-rank of an abelian 2-group A is

$$\mathrm{rk}_{2^k}(A) := \dim 2^{k-1}A/2^kA.$$

In our case we have $r_2(C_D) = t-1 = \#\{p \mid D\}-1$. Moreover r_4 is the dimension of $\ker(\varphi_4)$ in the following diagram.

$$\begin{tikzcd}
C[2] \arrow[r, "\varphi_4"] & C/2C \cong \mathrm{Gal}(\mathfrak{G}/K) \arrow[d, hook] \\
\mathbb{F}_2^t \arrow[u, two heads, "e_i \mapsto [\mathfrak{p}_i]"] \arrow[r, "R_4"] & \mathbb{F}_2^t = \mathrm{Gal}(\mathfrak{G}/\mathbb{Q}),
\end{tikzcd}$$

where $\mathfrak{p}_i$ are the ramified primes (with some chosen ordering), and R_4 is the Rédei map: a $t \times t$ matrix over $\mathbb{F}_2$ with (i,j) entry given by

$$\frac{\mathrm{Frob}_{\mathfrak{p}_i}(\sqrt{p_j^*})}{\sqrt{p_j^*}} \in \{\pm 1\} \cong \mathbb{F}_2.$$

If $i \neq j$ then this is $\left(\frac{p_i}{p_j}\right)$. In our earlier example this looks as follows.

Example 55. For $K = \mathbb{Q}(\sqrt{-14})$, it is easy enough to compute $R_4 = 0$ from the definition above. Since $\dim\ker(R_4) = \dim\ker(\varphi_4) + 1$ we obtain, with no need to look at ideal classes, that $r_4 = r_2 = 1$.

8-rank. The Rédei symbol occurs when we look at the 8-rank of $C = C_D$. We have

$$\begin{tikzcd}
\ker(R_4) \arrow[r] \arrow[drr, bend right, "R_8"'] & \ker(\varphi_4) \arrow[r] \arrow[d, "="] & 0 \\
 & C_D[2] \cap 2C_D \arrow[r] & 2C_D/4C_D
\end{tikzcd}$$

where $r_8 = r_4 - \mathrm{rk}(R_8)$. In order construct R_8, we will need to study extensions L/K which are (everywhere) unramified and cyclic of degree 4. Moreover, class field theory shows that such extensions are Galois over $\mathbb{Q}$ with $\mathrm{Gal}(L/\mathbb{Q}) \cong D_4$.

Elementary Galois theory, together with our work on Genus theory above, shows that such extensions are given by certain decompositions $D = d_1 d_2$ and will always be of the form in the diagram below with $\beta \in \mathbb{Q}(\sqrt{d_1})$ with Galois conjugate β' and such that $\beta\beta' = d_2 \cdot \square$.

$$\begin{tikzcd}
& & L \arrow[lld, dash] \arrow[ld, dash] \arrow[d, dash] \arrow[rd, dash] \arrow[rrd, dash] & & \\
\mathbb{Q}(\sqrt{\beta}) \arrow[rd, dash] & \mathbb{Q}(\sqrt{\beta'}) \arrow[d, dash] & \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}) \arrow[ld, dash] \arrow[d, dash] \arrow[rd, dash] & \cdot \arrow[d, dash] & \cdot \arrow[ld, dash] \\
& \mathbb{Q}(\sqrt{d_1}) \arrow[rd, dash] & K = \mathbb{Q}(\sqrt{D}) \arrow[d, dash] & \mathbb{Q}(\sqrt{d_2}) \arrow[ld, dash] & \\
& & \mathbb{Q} & &
\end{tikzcd}$$

Note that the existence of such β is equivalent to the solubility of the equation $x^2 - d_1 y^2 - d_2 z^2 = 0$ over $\mathbb{Z}$.

Rédei identified for which decompositions we could do this. The Rédei symbol $[d_1, d_2, m]$, where m is the norm of a product of ambiguous primes, is the appropriate coordinate of the matrix R_8.

Example 56. Returning to $K = \mathbb{Q}(\sqrt{-14})$, it is clear that $x^2 + 7y^2 - 8z^2 = 0$ has the solution $(1, 1, 1)$, so for $\beta = \sqrt{-1 + 2\sqrt{2}}$ and we add to our diagram

$$\begin{tikzcd}
H \arrow[dd, dash, "2"] \arrow[rd, dash, "="] & \\
& \mathbb{Q}(\sqrt{\beta}) \arrow[d, dash] \\
\mathfrak{G} = \mathbb{Q}\left(\sqrt{-7}, \sqrt{2}\right) \arrow[d, dash, "2"] & \mathbb{Q}(\sqrt{2}) \arrow[ld, dash] \\
\mathbb{Q}(\sqrt{-14}) &
\end{tikzcd}$$

Unfortunately from this point the lecturer was out of time, and so sketched the general definition of the Rédei symbol without having time to write it. I was unable to capture this. Rather than fill in the blanks myself, I will refer to the Stevenhagen's own article on this: [Ste18].

References

[Ste18] P. Stevenhagen, *Redei reciprocity, governing fields, and negative pell*, Preprint, arXiv:1806.06250 (2018). ↑1.1