CLASS FIELD THEORY

COURSE: RENÉ SCHOOF AND PETER STEVENHAGEN
NOTES: ROSS PATERSON

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

$$\begin{array}{c} K = \mathbb{Q}(\alpha) \supset \mathcal{O}_K \supseteq \mathbb{Z}[\alpha] \\ {\scriptstyle n}\big\uparrow \\ \mathbb{Q} \supset \mathbb{Z} \end{array}$$

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. Ok 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

$$\begin{array}{c} K = \mathbb{Q}(\alpha) \supset \mathbb{Z}[\alpha] \\ {\scriptstyle n}\big\uparrow \\ \mathbb{Q} \supset \mathbb{Z} \end{array}$$

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 stabiliset $G_\mathfrak{p} = \mathrm{stab}_\mathfrak{p} \subseteq G$ 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.

$$\begin{tikzcd}
 & & \mathbb{Q}(\zeta_{20}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
 & \mathbb{Q}(i, \sqrt{5}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \mathbb{Q}(\zeta_{20})^{+} \arrow[d, dash] & \mathbb{Q}(\zeta_5) \arrow[dl, dash] \\
\mathbb{Q}(i) = \mathbb{Q}(\zeta_4) \arrow[dr, dash] & \mathbb{Q}(\sqrt{-5}) \arrow[d, dash] & \mathbb{Q}(\sqrt{5}) \arrow[dl, dash] & \\
 & \mathbb{Q} & &
\end{tikzcd}$$

Note that the associated lattice of subgroups is

$$\begin{tikzcd}
 & & \langle 1 \rangle \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
 & \langle 9 \rangle \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \langle -1 \rangle \arrow[d, dash] & \langle 11 \rangle \arrow[dl, dash] \\
\langle -3 \rangle \arrow[dr, dash] & \langle 3 \rangle \arrow[d, dash] & \langle 9, 11 \rangle \arrow[dl, dash] & \\
 & \mathbb{Z}/20\mathbb{Z}^{\times} & &
\end{tikzcd}$$

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 equidistibution 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

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

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. Ideles

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 $(1, \ldots, 1, \pi_\mathfrak{p}, 1, \ldots, 1)$.

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

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

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

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

Precisely: let $f : \mathbb{A}_{\mathbb{Q}}^\times \to \mathbb{Q}^\times$ be defined by $f((x_v)_v) = \mathrm{sgn}(x_\infty)\prod_p p^{v_p(x_p)}$, and then define our map $\mathbb{A}_{\mathbb{Q}}^\times \to \widehat{\mathbb{Z}} \times \mathbb{R}_{>0}$ to be

$$((x_p)_p, x_\infty) \mapsto \left(\frac{x_w}{f((x_v)_v)}\right)_w.$$

Note that the kernel has to be $\mathbb{Q}$ by construction.

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 $\mathfrak{q} \mid \mathfrak{p}$.*

$$\begin{array}{ccc} \mathbb{A}_K^\times / N_{L/K}\mathbb{A}_L^\times \cdot K^\times & \xrightarrow{\sim} & \mathrm{Gal}(L/K) \\ \uparrow & & \uparrow \\ K_\mathfrak{p}^\times / N_{L/K} L_\mathfrak{q}^\times & \xrightarrow{\sim} & \mathrm{Gal}(L_\mathfrak{q}/K_\mathfrak{p}). \end{array}$$

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 similarlt 2 is determined by the splitting behaviour of p in $x^4 - 2$.

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