Class Field Theory

Jiwu Jang

July 7, 2023

This is a note on a series of lectures on class field theory, given by Bartu Bingol.

§1 Fermat's Last Theorem

Problem 1.1 (Fermat's Last Theorem)**.** Solve $x^p + y^p = z^p$ where $p > 2$ is a rational prime and $(x, y, z) \in \mathbb{Z}$ such that $p \nmid xyz$.

Easy examples first:

Example 1.2

Consider $x^2 + y^2 = z^2$. We can factor in $\mathbb{Z}[i]$: $(x + yi)(x - yi) = z^2$.

Example 1.3

Consider $x^3 + y^3 = z^3$. We have $(x + y)(x^2 - xy + y^2) = 1$, but if we consider $\mathbb{Z}[\zeta_3]$ where ζ_3 is a third primitive root of unity, then

$$(x + y)(x + \zeta_3 y)(x + \zeta_3^2 y) = z^3$$

§2 Lamé's "proof" of FLT

The following is Lamé's "proof" of Fermat's Last Theorem in 1847.

Consider $x^p + y^p = z^p$. If we consider $\mathbb{Z}[\zeta_p]$ where ζ_p is a p^{th} primitive root of unity, then

$$(x + y)(x + \zeta_p y)(x + \zeta_p^2 y) \dots (x + \zeta_p^{p-1}) = z^p$$

So, let us try to solve $x^p + y^p = z^p$ in $\mathbb{Z}[\zeta_p]$.

Lemma 2.1

$x + \zeta_p^i y$ and $x + \zeta_p^j y$ are coprime for all $i \neq j$.

Proof. Suppose that there existed a prime q such that $q \mid x + \zeta_p^i y$ and $q \mid x + \zeta_p^j y$. Then, $q \mid \zeta_p^i y - \zeta_p^j y$. Without loss of generality, assume $i > j$. Thus, $q \mid \zeta_p^j y \left(\zeta_p^{i-j} - 1\right)$. Since q is a prime, q divides at least one of the following:

$$\zeta_p^j, \quad y, \quad \zeta_p^{i-j} - 1$$

Moreover, $q \mid x - \zeta_p^{i-j} x$, hence $q \mid x\left(1 - \zeta_p^{i-j}\right)$. That is, q divides at least one of the following:

$$x, \quad \zeta_p^{i-j} - 1$$

But since x and y are coprime, $q \mid 1 - \zeta_p^{i-j}$.

Lemma 2.2

$1 - \zeta_p^k$ and $1 - \zeta_p$ are associates, that is, they differ by a unit.

Hint: take the conjugate of both sides.

Proof. Obviously $1 - \zeta_p \mid 1 - \zeta_p^k$. It remains to prove that $1 - \zeta_p^k \mid 1 - \zeta_p$. Taking the conjugate of both sides, we get $1 - \zeta_p^{p-k} \mid 1 - \zeta_p^{p-1}$. □

Because $1 - \zeta_p^{i-j}$ and $1 - \zeta_p$ are associates, we have $q \mid 1 - \zeta_p$, so taking the norm of both sides, $q^{p-1} \mid 2$, which is a contradiction. □

So, let us consider $x + \zeta_p y = u \cdot \alpha$.

Theorem 2.3 (Lamé)

For any $\beta \in \mathbb{Z}[\zeta_p]$, $\beta^p \equiv m \pmod p$ for some integer m.

Lemma 2.4 (Kummer)

Every unit $u \in \mathbb{Z}[\zeta_p]$ is of the form $\overline{u} \cdot \zeta_p^k$ for some k. (This holds only for rings with prime ideals.)

Proof. Explosive stuff, this needs the whole Chapter 14 of Lang's *Cyclotomic Fields II*. □

Let us combine everything:

$$x + \zeta_p y = u \cdot \alpha^p = u \cdot m \pmod p = \overline{u} \cdot \zeta_p^k \cdot m \pmod p \tag{1}$$

Moreover, we can take the conjugate of $x + \zeta_p y$, so by (1),

$$x + \zeta_p^{-1} y = \overline{u \cdot m} = \overline{u} \cdot m \pmod p \tag{2}$$

So combining (1) and (2), we have

$$(x + \zeta_p y) = (x + \zeta_p^{-1} y) \cdot \zeta_p^k \pmod p \tag{3}$$

This means

$$x + \zeta_p y = x \cdot \zeta_p^k + \zeta_p^{k-1} \cdot y \pmod p \tag{4}$$

Lemma 2.5

If a rational prime p divides $\gamma \in \mathbb{Z}[\zeta_p]$, then p divides each of the coefficients $a_0, a_1, \dots, a_{p-2}$ where $\gamma = a_0 + a_1 \cdot \zeta_p + \cdots + a_{p-2} \cdot \zeta_p^{p-2}$.

We do not need ζ_p^{p-1} since it is equal to $-(1 + \zeta_p + \zeta_p^2 \cdots + \zeta_p^{p-2})$.

Proof. Take an element $\beta \in \mathbb{Z}[\zeta_p]$ such that $\gamma = p \cdot \beta$. Then, we can write $a_0 + a_1 \cdot \zeta_p + \cdots + a_{p-2} \cdot \zeta_p^{p-2} = p \cdot (b_0 + b_1 \cdot \zeta_p + \cdots + b_{p-2} \cdot \zeta_p^{p-2})$.

This means

$$(a_0 - p \cdot b_0) + (a_1 - p \cdot b_1) \cdot \zeta_p + \cdots + (a_{p-2} - p \cdot b_{p-2}) \cdot \zeta_p^{p-2} = 0 \tag{5}$$

but since $1 + \zeta_p + \zeta_p^2 + \cdots + \zeta_p^{p-1} = 0$ and is irreducible, we know that 1, ζ_p, $\dots$, ζ_p^{p-2} are linearly independent, so $a_i = p \cdot b_i$ for all $0 \le i \le p-2$. □

This means

$$x + \zeta_p \cdot y = x \cdot \zeta_p + y \pmod{p} \tag{6}$$

So, we have

$$x - y + \zeta_p(y - x) = 0 \pmod{p} \tag{7}$$

which forces $x = y \pmod{p}$ due to linear independence. Do the same thing for

$$x^p + (-z)^p = (-y)^p \tag{8}$$

then $x = -z \pmod{p}$.

So, $3x^p = 0 \pmod{p}$, but this can happen only when $p = 3$ or $p \mid x$. But we know by Fermat, $x^3 + y^3 = z^3$ does not have a solution. So $p \mid x$, contradiction...? WRONG. $\mathbb{Z}[\zeta_p]$ is NOT a UFD!

Exercise 2.6. Prove that $\mathbb{Z}[\zeta_{23}]$ does not have unique factorization.

§3 Ideals

Definition 3.1. Let $(R, +, \cdot)$ be a ring. An ideal I of R is:

1. abelian group under addition
2. closed under multiplication by R: $\forall r \in R$, $\forall x \in I$, $rx \in I$.

Example 3.2

$R = \mathbb{Z}$. $I = \{0\}$, $\mathbb{Z}$, $2\mathbb{Z}$, $n\mathbb{Z}$.

Definition 3.3. We call an ideal $\mathfrak{p} \leqslant R$ *prime* if $ab \in \mathfrak{p}$ for some $a, b \in R$, then either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. We call an ideal $\mathfrak{m} \leqslant R$ *maximal* if there is no proper ideal containing $\mathfrak{m}$.

Example 3.4

$R = \mathbb{Z}$, then $\mathfrak{m} = 2\mathbb{Z}, 3\mathbb{Z}, p\mathbb{Z}$ for p rational prime.

Now, let's start our "construction." We want R to satisfy:

(1) $R \cap Q = \mathbb{Z}$

(2) R should include all roots of monic polynomials in $R[x]$ which has solutions in $\mathbb{Q}(\alpha)$.

(3) We want R to have a unique factorization.

(4) $\forall x \in \mathbb{Q}(\alpha)$, $\exists r_1, r_2 \in R$ and $r_2 \neq 0$ s.t. $\frac{r_1}{r_2}$.

We expect $R = \mathbb{Z}[\alpha]$. Let's consider $x = \sqrt{-3}$. This doesn't work. . . .

On the other hand, $\alpha = \zeta_3 = \frac{-1-\sqrt{-3}}{2}$. Then, $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$. But this means $R = \mathbb{Z}[\frac{-1-\sqrt{-3}}{2}]$. We want (2). Moreover, ζ_3 is a solution of x^2+x+1. So, $R = \mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$.

Definition 3.5. We call such rings $R \subseteq \mathbb{Q}(\alpha)$ a *ring of integers* (number rings), where α is an algebraic number.

Exercise 3.6. Why is R a ring?

For any $K = \mathbb{Q}(\alpha)$, we will denote $R = \mathcal{O}_K$.

> **Remark.** However, the main story was describing a ring that has a unique factorization in terms of prime ideals.

Definition 3.7. A ring R is called a *Dedekind domain* if it is integrally closed, nonzero prime ideals are maximal, and Noetherian.

Theorem 3.8

Let $K = \mathbb{Q}(\alpha)$ for some algebraic number α, then $\mathcal{O}_K$ is a Dedekind domain.

The ring that we wanted to have unique factorization is $\mathbb{Z}[\zeta_p]$. Is this a number ring for some $\mathbb{Q}(\alpha)$? It turns out that the answer is yes: $\mathbb{Z}[\zeta_p] = \mathcal{O}_K$ for $K = \mathbb{Q}(\zeta_p)$.

Nice, but we want to also obtain a set given exactly by prime ideals. We, of course, want to be able to multiply. But we also want this to form a group.

1. Is this set closed under "multiplication"?
2. Does this set have an identity?
3. Does every element have one and only one inverse?

In order to be able to understand this, we should describe what "multiplication" of ideals are. Consider $\mathcal{O}_K$. Let I and J be ideals of $\mathcal{O}_K$. Then, $I \cdot J := \{i_1 j_1 + \cdots + i_n j_n \mid i_k \in I,\ j_k \in J\}$ (which we can do, since I and J are Noetherian, hence finitely generated).

So, let us consider such a set, a collection of all $I \cdot J$, where I, J are prime.

The whole thing R is an identity, but this creates a problem: there are no inverses. (For example, take $\mathcal{O}_K = \mathbb{Z}$, then $\frac{3}{2}, \frac{4}{3} \notin \mathbb{Z}$, but $2 \in \mathbb{Z}$.) We want to have multiplicative inverses as well. But multiplicative inverses are in K, not $\mathcal{O}_K$. So, we need our set to contain some elements of K. Now, we have a collection $\{aI \mid a \in K \text{ s.t. for some } I \text{ and } J,\ aIJ = R\}$.

> **Remark.** The main takeaway is that Dedekind domains have a unique factorization in terms of prime ideals.

§4 Fractional ideals

In order to be able to give a proper description of a fractional ideal, we should first define an R-module.

Definition 4.1. Let $(R, +, \cdot)$ be a ring. Then, we call M an R-module if

(1) M is an abelian group under $+$.

(2) M has scalar multiplication by R:

  (i) $1 \cdot m = m$

  (ii) $n, m \in M$

  (iii) $(r_1 + r_2) \cdot M = r_1 M + r_2 M$ for each $r_1, r_2 \in R$, $m \in M$

  (iv) $(m_1 + m_2)r = m_1 r + m_2 r$ for each $m_1, m_2 \in M$, $r \in R$.

Example 4.2

Vector spaces are an R-module. They are modules over fields.

- Every ring R is an R-module.
- For $K = \mathbb{Q}(\alpha)$ where α is an algebraic number, and $\mathcal{O}_K$ being its number ring, K is an $\mathcal{O}_K$-module.

Let's fix our notation: $\mathcal{O}_K$ and K.

Definition 4.3. A *fractional ideal* I is an $\mathcal{O}_K$-submodule of K such that $a \cdot I \subseteq \mathcal{O}_K$ for some $a \in \mathcal{O}_K$.

Example 4.4

Consider $K = \mathbb{Q}$, $\mathcal{O}_K = \mathbb{Z}$ and $I = \frac{1}{2}\mathbb{Z}$. We can take $a = 2 \in \mathcal{O}_K$ so that $a \cdot I \in\subseteq \mathcal{O}_K$.

Definition 4.5. An *invertible ideal* I is an ideal such that there exists $J = \{x \in K \mid a \cdot J \subseteq \mathcal{O}_K$ for some $a \in \mathcal{O}_K$, with $I \cdot J = \mathcal{O}_K$.

Lemma 4.6

Principal ideals are invertible.

Proof. A principal ideal is an ideal generated by a single element, $x \in \mathcal{O}_K$. Consider $J = \frac{1}{x} \cdot \mathcal{O}_K$ (where $x \neq 0$). Then, $I \cdot J = (x\,\mathcal{O}_K) \cdot (\frac{1}{x}\,\mathcal{O}_K) = (x \cdot \frac{1}{x})\mathcal{O}_K = \mathcal{O}_K$. □

Exercise 4.7. Prove that the principal ideals in K form a subgroup of $I(\mathcal{O}_K) := P(\mathcal{O}_K)$, which is in turn a normal subgroup (thus we may quotient by $P(\mathcal{O}_K)$).

Exercise 4.8. Prove that the fractional ideals in K, denoted as $I(\mathcal{O}_K)$, form a group, with operation being ideal multiplication.

Lemma 4.9

All prime ideals in $\mathcal{O}_K$ are invertible.

Proof. Use localization. (The proof does not provide any insight, so it's omitted.) □

Theorem 4.10

All fractional ideals can be uniquely expressed by a product of prime ideals.

Proof. Let us take a fractional ideal $I = \langle x_1, \dots, x_n \rangle$. Since each $x_i \in K$, we can describe $x_i = \frac{\alpha_i}{\beta_i}$ for some α_i, $\beta_i \in \mathcal{O}_K$ such that $\beta_i \neq 0$.

Let S be the common denominator of x_i's. Then, $sI \subseteq \mathcal{O}_K$. We know that $\mathcal{O}_K$ is a Dedekind domain. This means that we can find prime ideals $\mathfrak{p}_J \leq \mathcal{O}_K$ such that $sI = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_m^{e_m}$ uniquely. Moreover, we can factorize $s\mathcal{O}_K = \mathfrak{q}_1^{f_1} \dots \mathfrak{q}_t^{f_t}$. By the previous lemma, we have $I = \mathfrak{q}_1^{-f_1} \dots \mathfrak{q}_t^{-f_t} \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_m^{e_m}$ uniquely. □

Definition 4.11. Define $\mathrm{Cl}(\mathcal{O}_K) := I(\mathcal{O}_K)/P(\mathcal{O}_K)$.

Definition 4.12. Define the class number $h_K := |\,\mathrm{Cl}(\mathcal{O}_K)|$ for a number ring R.

Lemma 4.13 (Minkowski bound)

For a number ring R, we have $h_K(R) = |\mathrm{Cl}(R)| < \infty$.

Theorem 4.14

$h_K(\mathcal{O}_K) = 1$ if and only if $\mathcal{O}_K$ has unique factorization.

Definition 4.15. A rational prime p is called *regular* if $p \nmid |\mathrm{Cl}(\mathbb{Z}[\zeta_p])|$.

Theorem 4.16 (Kummer)

Let p be a rational regular prime with $p \nmid xyz$. Then, $x^p + y^p = z^p$ does not have any non-trivial integer solutions. (The number of irregular primes is infinite.)

Proof. Let us factorize this in terms of ideals: $\langle x + y\zeta_p^1 \rangle \langle x + y\zeta_p^2 \rangle \dots \left\langle x + y\zeta_p^{p-1} \right\rangle = \langle z^p \rangle = \langle z \rangle^p$.

Lemma 4.17

$\langle x + y\zeta_p^1 \rangle$ and $\langle x + y\zeta_p^k \rangle$ are coprime.

Lemma 4.18

$\langle 1 - \zeta_p^i \rangle$ and $\left\langle 1 - \zeta_p^j \right\rangle$ are associates, $\forall i$, j such that $1 \leq i \neq j \leq p-1$.

Lemma 4.19

$\langle x + y\zeta_p^i \rangle = I_i^p$ for some ideal $I_i \leq \mathbb{Z}[\zeta_p]$.

Proof. Notice that $\langle z \rangle$ has a unique factorization, i.e., $\langle z \rangle = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$ which implies $\langle z^p \rangle = \mathfrak{p}_1^{pe_1} \dots \mathfrak{p}_r^{pe_r}$. Let us check the LHS now: we have $\mathfrak{q}_1^{f_1} \dots \mathfrak{q}_k^{f_k}$. By Lemma 1, $\mathfrak{q}_1, \dots, \mathfrak{q}_k$ are factors of only $\langle x + y\zeta_p^i \rangle$. □

By the previous lemma, we know that I_i^p is a principal ideal. Then, $[I_i^p] = [I_i]^p = [\mathbb{Z}[\zeta_p]]$, so the order of I_i is either p or 1, but since p is a regular prime, I_i is principal. The rest of the argument is exactly the same as what we did on Monday. □

Definition 4.20. Let K be a field. Then, L/K is called a *field extension* if $L \supseteq K$. (L/K is read L over K.)

Example 4.21

$K = \mathbb{Q}$ and $L = \mathbb{Q}(i)$.

Definition 4.22. Consider $p(x) \in \mathbb{Q}[x]$. Then, the *splitting field* of $p(x)$ is the minimal field extension of $\mathbb{Q}$ containing all roots of $p(x)$.

Example 4.23

Consider $\sqrt[3]{2}$. The minimal polynomial of $\mathbb{Q}(\sqrt[3]{2})$ is $p(x) = x^3 - 2$. But $\mathbb{Q}(\sqrt[3]{2})$ is **not** the splitting field of $p(x)$, because $\sqrt[3]{2} \cdot \zeta_3$ is a root of $p(x)$, but it is not in $\mathbb{Q}(\sqrt[3]{2})$. This means that we need a larger field that contains ζ_3 as well. Hence, the splitting field is $K = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$.

Remark. The order of performing the extensions to the field does not change the splitting field.

$$\begin{tikzcd}
& \mathbb{Q}(\sqrt[3]{2}, \zeta_3) & \\
\mathbb{Q}(\zeta_3) \arrow[ur] & & \mathbb{Q}(\sqrt[3]{2}) \arrow[ul] \\
& \mathbb{Q} \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

Figure 1: The splitting field of $x^3 - 2$ reached by two different order of extensions.

Consider the following fields: $\mathbb{Q}(\alpha) : a_0 + a_1\alpha + a_2\alpha^2$ and $a_i \in \mathbb{Q}$, and $\mathbb{Q}(\omega\alpha) : a_0 + a_1\omega\alpha + a_2\omega^2\alpha^2$.

Let us try to factorize $p(x) = x^3 - 2$ in $\mathbb{Q}(\alpha)$, that is,

$$x^3 - 2 = (x - \alpha)(x^2 + x\alpha + x\alpha^2) = (x - \alpha)(x - \omega\alpha)(x - \omega^2\alpha)$$

This means $\mathbb{Q}(\alpha)$ is not enough, so we should add $\omega\alpha$ as well. In this new field, every element is of the form $(a_0 + a_1\alpha + a_2\alpha^2)(a_3 + a_4\alpha + a_5\alpha^2)\omega\alpha$.

Now, let us do the same thing, that is, try to factorize $p(x)$ in $\mathbb{Q}(\omega)$. Consider the map $\sigma_1 : \mathbb{Q}(\alpha) \to \mathbb{Q}(\omega\alpha)$ with $\sigma_1 : \alpha \mapsto \omega\alpha$. Then, we can factorize $(x - \sigma_1(\alpha))(x^2 + \sigma_1(\alpha)x + \sigma_1(\alpha^2)) = (x - \omega\alpha)(x^2 + \omega\alpha x + \omega^2\alpha^2)$.

Thus, in our new field $\mathbb{Q}(\omega\alpha, \omega^2\alpha)$, every element is of the form $(a_0 + a_1\omega\alpha + a_2\omega^2\alpha^2) + (a_3 + a_4\omega\alpha + a_5\omega^2\alpha^2)\omega^2\alpha$.

Our original extension had $a_0 + a_1\alpha + a_2\alpha^2 + a_3\omega\alpha + a_4\omega\alpha^2 + a_5\omega\alpha^3$. Now, we have $a_0 + a_1\omega\alpha + a_2\omega^2\alpha^2 + a_3\omega^2\alpha + a_4\omega^2\alpha^2 + a_5\omega^4\alpha^3$.

Looking at the actions of σ_1, we have

$$\begin{aligned} \alpha &\mapsto \omega\alpha \\ \alpha^2 &\mapsto \omega^2\alpha^2 \\ \omega\alpha &\mapsto \omega^2\alpha \\ \omega\alpha^2 &\mapsto \alpha^2 \\ \omega &\mapsto \omega \\ 1 &\mapsto 1 \end{aligned}$$

and $\alpha \mapsto \omega\alpha \mapsto \omega^2\alpha \mapsto \alpha$.

Let's do the same thing with $\sigma_2 : \alpha \mapsto \omega^2\alpha$.

Looking at the actions of σ_2, we have

$$\begin{aligned} \alpha &\mapsto \omega^2\alpha \\ \alpha^2 &\mapsto \omega\alpha^2 \\ \omega\alpha &\mapsto \alpha \\ \omega\alpha^2 &\mapsto \omega^2\alpha^2 \\ \omega &\mapsto \omega \\ 1 &\mapsto 1 \end{aligned}$$

and $\alpha \mapsto \omega^2\alpha \mapsto \omega\alpha \mapsto \alpha$.

Let's do nothing: $e : \alpha \mapsto \alpha$ and $e : \omega \mapsto \omega$. This is the identity map.

This time, let us act nontrivially on ω as well. The only nontrivial choice for ω is $\omega \mapsto \omega^2$. Then, we have either $\alpha \mapsto \alpha$, $\alpha \mapsto \omega\alpha$, or $\alpha \mapsto \omega^2\alpha$.

If $\alpha \mapsto \alpha$, looking at the actions of σ_3, we have

$$\begin{aligned} \omega &\mapsto \omega^2 \\ \alpha &\mapsto \alpha \\ \alpha^2 &\mapsto \alpha^2 \\ \omega\alpha &\mapsto \omega^2\alpha \\ \omega^2\alpha &\mapsto \omega\alpha \\ 1 &\mapsto 1 \end{aligned}$$

If $\alpha \mapsto \omega\alpha$, looking at the actions of σ_4, we have

$$\begin{aligned} \omega &\mapsto \omega^2 \\ \alpha &\mapsto \omega\alpha \\ \alpha^2 &\mapsto \omega^2\alpha^2 \\ \omega\alpha &\mapsto \alpha \\ \omega^2\alpha &\mapsto \omega^2\alpha \\ 1 &\mapsto 1 \end{aligned}$$

If $\alpha \mapsto \omega^2\alpha$, looking at the actions of σ_5, we have

$$\begin{aligned} \omega &\mapsto \omega^2 \\ \alpha &\mapsto \omega^2\alpha \\ \alpha^2 &\mapsto \omega\alpha^2 \\ \omega\alpha &\mapsto \omega\alpha \\ \omega^2\alpha &\mapsto \alpha \\ 1 &\mapsto 1 \end{aligned}$$

Let's consider $\{e, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5\}$, which we call the Galois set. The set with the operation being function composition is a group, since it has the identity e, inverses (revert all the mappings), and associativity (composition is associative). This is called the Galois group. The Galois group permutes the roots of the polynomial.

§5 Galois extensions

Exercise 5.1. Find the Galois group of $x^5 + x - 2$, and whether that group is solvable.

$$\begin{tikzcd}
& & K \\
p \cdot \mathcal{O}_K \arrow[r, dotted, no head] & \mathcal{O}_K \arrow[ur, dotted, no head] & \mathbb{Q} \arrow[u] \\
p \arrow[u, dotted] \arrow[r, dotted, no head] & \mathbb{Z} \arrow[u, dotted, no head] \arrow[ur] &
\end{tikzcd}$$

Figure 2: The big picture.

Let us check some examples where we know how p behaves in $\mathcal{O}_K$.

1. Consider $K = \mathbb{Q}(i)$, then $\mathcal{O}_K = \mathbb{Z}[i]$. Take $p = 2$. Then, $2 \cdot \mathcal{O}_K = ?$. We know that $2 = (1+i)(1-i)$. Passing to the ideals, $2 \cdot \mathcal{O}_K = \langle 1+i \rangle \cdot \langle 1-i \rangle$. Since $1+i$ and $1-i$ are associates, we actually have $2 \cdot \mathcal{O}_K = \langle 1+i \rangle^2$.

2. Continue with $K = \mathbb{Q}(i)$, and $\mathcal{O}_K = \mathbb{Z}[i]$. Let's consider $p = 5$. Then, $5 \cdot \mathcal{O}_K = \langle 2+i \rangle \cdot \langle 2-i \rangle$.

> **Remark.** The maximum number of "splits" is the degree of the extension: $\mathbb{Q}(i)$ is a quadratic extension, hence there can be at most 2 splits.

In the general case, we consider $p \cdot \mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_t^{e_t}$, where $\mathfrak{p}_i$ is a prime ideal, and each $\mathfrak{p}_i \leq \mathcal{O}_K$.

Definition 5.2. The exponents e_i are called *ramification indices.*

- $p \cdot \mathcal{O}_K$ is still a prime — we say that p is inert.
- If $p \cdot \mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_t^{e_t}$ where each $e_i = 1$, then — we say that p splits.
- If $p \cdot \mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_t^{e_t}$ such that some $e_i > 1$, then — we say that p ramifies.

> **Remark.** For any extension, we only have finitely many ramified primes.

> **Remark.** Why do we care about ramification? Because it is closely related to algebraic geometry, especially multiple roots.

Let K/L be a field extension, such that there is a ramified prime of $p \cdot \mathcal{O}_K$, then the extension is called a *ramified extension.*

> **Remark.** Every $K/\mathbb{Q}$ algebraic extension of $\mathbb{Q}$ has at least one ramified prime, which is pretty bad.
>
> But there are some other fields whose extensions are unramified, for example, $\mathbb{Q}(\sqrt{-163})$.

Exercise 5.3. Let R be an integral domain and $\mathfrak{m}$ be a maximal ideal of it. Prove that $R/\mathfrak{m}$ is a field.

Let us fix $p \cdot \mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$. Then, $\mathcal{O}_K/\mathfrak{p}_i$ is a field. Moreover, $\mathbb{Z}/p$ is also a field. Then, $[\mathcal{O}_K/\mathfrak{p}_i : \mathbb{Z}/p]$ is called the inertial degree, denoted f_i.

Proposition 5.4

Let $K/\mathbb{Q}$ be a degree n extension, then, $\sum e_i f_i = n$.

Theorem 5.5 (Euler)

Let $K/\mathbb{Q}$ be a number field, p be a rational prime, $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in K$, and f be the minimal polynomial of α over $\mathbb{Q}$. Then, we can uniquely and explicitly factorize $p \cdot \mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$.

Proof. Let g be the minimal polynomial, such that $g := \mathfrak{g}_1^{e_1} \dots \mathfrak{g}_r^{e_r}$ be the factorization of it. Let us denote their mod p reduction by $\overline{g} = \overline{\mathfrak{g}}_1^{e_1} \dots \overline{\mathfrak{g}}_r^{e_r}$. Define $\mathfrak{p}_i := \langle p, \mathfrak{g}_i(\alpha) \rangle$. Then, the following chain of isomorphisms hold:

$$\begin{aligned} {}^{\mathcal{O}_K}\!\big/_{\mathfrak{p}_i} &= {}^{\mathbb{Z}[\alpha]}\!\big/_{\langle p, \mathfrak{g}_i(\alpha) \rangle} \\ &\cong {}^{\mathbb{Z}[x]}\!\big/_{\langle p, \mathfrak{g}_i(x), g(x) \rangle} \\ &\cong {}^{{}^{\mathbb{Z}}\!/_{p}[x]}\!\big/_{\langle \overline{\mathfrak{g}}_i(x), \overline{g}(x) \rangle} \\ &\cong {}^{{}^{\mathbb{Z}}\!/_{p}[x]}\!\big/_{\langle \overline{\mathfrak{g}}_i(x) \rangle} \end{aligned}$$

since $\mathfrak{g}_i \mid g$.

On the other hand,

$$ {}^{\mathcal{O}_K}\!\big/_{p\mathcal{O}_K} = {}^{\mathbb{Z}[\alpha]}\!\big/_{p\mathbb{Z}[\alpha]} \cong {}^{\mathbb{Z}[x]}\!\big/_{\langle p, g(x) \rangle} \cong {}^{\mathbb{Z}/p[x]}\!\big/_{\langle \overline{g}(x) \rangle} $$

taking the mod p reduction map. Since $\overline{\mathfrak{g}}_i$ are relatively coprime, we get

$$ {}^{{}^{\mathbb{Z}}\!/_{p}[x]}\!\big/_{\langle \overline{g}(x) \rangle} \cong \prod_i {}^{{}^{\mathbb{Z}}\!/_{p}[x]}\!\big/_{\langle \overline{\mathfrak{g}}_i^{e_i}(x) \rangle} $$

by the Chinese remainder theorem.

Consider the map $\mathcal{O}_K \to {}^{\mathcal{O}_K}/_{p\mathcal{O}_K}$ (mod p reduction), then since the map is a surjection, we have $\operatorname{Ker}\varphi = p\mathcal{O}_K$.

$$\begin{tikzcd}
 & \mathcal{O}_K \arrow[dl, two heads, "\gamma"'] \arrow[dr, two heads, "\varphi"] & \\
\prod_i {}^{\mathbb{Z}/p[x]}/_{\langle \overline{\mathfrak{g}}_i^{e_i}(x)\rangle} \arrow[rr, "\cong"] & & {}^{\mathcal{O}_K}/_{p\mathcal{O}_K}
\end{tikzcd}$$

Figure 3: The kernels of the maps φ and γ.

Note that the diagram commutes, so $\operatorname{Ker}\varphi \cong \operatorname{Ker}\gamma$.

We have $\operatorname{Ker}\gamma = \bigcap_i \langle \overline{\mathfrak{g}}_i^{e_i}(x)\rangle$. But $\operatorname{Ker}\gamma \cong \operatorname{Ker}\varphi = p\mathcal{O}_K$. A ring theoretic property says that since $\langle \overline{\mathfrak{g}}_i^{e_i}(x)\rangle$ are coprime, $\operatorname{Ker}\gamma = \prod_i \langle \overline{\mathfrak{g}}_i^{e_i}(x)\rangle \cong p\mathcal{O}_K$.

Exercise 5.6. Show that $\langle p, \overline{\mathfrak{g}}_i^{e_i}(\alpha)\rangle \cong \langle p, \mathfrak{g}_i(\alpha)\rangle_i^e$.

So, $p\mathcal{O}_K \cong \prod_i \langle p, \overline{\mathfrak{g}}_i(\alpha)\rangle^{e_i}$, end of the proof. □

Consider $\mathcal{O}_K = \mathbb{Z}[i]$. The minimal polynomial of i is x^2+1. What is $2\mathcal{O}_K$? Note that $x^2+1 = (x+1)^2 \pmod 2$, so $p\mathcal{O}_K = \langle 1+i\rangle^2$, thus it ramifies.

What is $17\mathcal{O}_K$? $x^2+1 \equiv (x+4)(x-4) \pmod{17}$.

Consider ζ_3. The minimal polynomial of ζ_3 is x^2+x+1. Then, x^2+x+1 mod 2 is irreducible, so 2 stays inert.

§6 Ramification theory

Remark (Book recommendations).

- Jarvis — Algebraic Number Theory.
- Janusz — Algebraic Number Theory. (*)
- Cassels-Frölich — Algebraic Number Theory. (***)
- Cox — Primes of the form x^2+ny^2.
- Washington — Introduction to Cyclotomic Fields. (**)
- Lorenzini — An Invitation to Arithmetic Geometry.
- Serre — Local Fields. (**)
- Fraleigh — Abstract Algebra.
- Eisenbud — Commutative Algebra towards Algebraic Geometry
- Hungerford — Algebra.
- Keith Conrad's notes on anything.

Stars (*) indicate difficulty.

All these work has been for primes and equations. So, let's solve one:

Example 6.1

Let us solve $x^3 = y^2 + 5$ in $\mathbb{Z}$.

Solution. If $2 \mid x$, then $y^2 \equiv 3 \pmod 8$, contradiction. Hence, $2 \nmid x$. Let $g = \gcd(x, y)$, then $g^2 \mid 5$, so $g = 1$. Thus, $\gcd(x, y) = 1$. Let $\mathfrak{p}_1 := \langle y + \sqrt{-5} \rangle$ and $\mathfrak{p}_2 := \langle y - \sqrt{-5} \rangle$, which are not necessarily prime ideals. Let us check if $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are coprime. Suppose not: then there is a prime ideal (which is maximal, since $\mathbb{Z}[\sqrt{-5}]$ is a Dedekind domain) $\mathfrak{p} \leq \mathbb{Z}[\sqrt{-5}]$ such that $\mathfrak{p}_1, \mathfrak{p}_2 \in \mathfrak{p}$. So, $x^3 \in \mathfrak{p} \implies x \in \mathfrak{p}$. Also, $y + \sqrt{-5} + y - \sqrt{-5} = 2y \in \mathfrak{p}$. So, either $2 \in \mathfrak{p}$ or $y \in \mathfrak{p}$. But, $(2, y) = 1$, so $y \notin \mathfrak{p}$. That means $2 \in \mathfrak{p}$. But x is odd, contradiction. Thus, $\langle y + \sqrt{-5} \rangle$ and $\langle y - \sqrt{-5} \rangle$ are coprime. Since we have unique factorization of ideals, there are some α_1, α_2 prime ideals such that $\langle y + \sqrt{-5} \rangle = \alpha_1^3$ and $\langle y - \sqrt{-5} \rangle = \alpha_2^3$.

Theorem 6.2 (Minkowski)

Let $h_K := |C_K| \leq \dfrac{n!}{n^n} \cdot \left(\dfrac{4}{\pi}\right)^s \cdot \sqrt{|\Delta_K|}$ where $n = [K : \mathbb{Q}]$, s is the number of conjugates of complex embeddings, and Δ_K is the discriminant of K.

So, we know that h_K is bounded above. Let's try to compute h_K for $\mathbb{Q}(\sqrt{-5}) = K$: for K, we have $s = 1$, and $|\Delta_K| = 20$. This means

$$h_K \leq \frac{2}{4} \cdot \frac{4}{\pi} \cdot 2\sqrt{5} = \frac{4\sqrt{5}}{\pi} < 3$$

hence $h_K = 1$ or $h_K = 2$. But since $h_K = 1$ implies the domain being a UFD, yet $\mathbb{Z}[\sqrt{-5}]$ is not a UFD, we know that $h_K = 2$. Hence, α_1^2 is the identity in C_K, meaning that α_1^2 is a principal ideal. Thus, α_1 is a principal ideal. Therefore, there is $\gamma \in \mathbb{Z}[\sqrt{-5}]$ such that $y + \sqrt{-5} = u \cdot \gamma^3$ where u is a unit. But the units of $\mathbb{Z}[\sqrt{-5}]$ are ± 1. Hence, WLOG, $y + \sqrt{-5} = \pm\gamma^3$. Let $\gamma = \sigma_1 + \sigma_2\sqrt{-5}$, then $1 = 3\sigma_1^2\sigma_2 - 5\sigma_2^3 = \sigma_2(3\sigma_1^2 - 5\sigma_2^2)$, which has no solution. □

> **Remark.** $\mathbb{Q}(\sqrt{-5})$ is a beautiful field, because it has some unramified extensions. We said "some" because eventually we will have ramifications. So, the object of interest is maximal unramified ideals.

Definition 6.3. Let H_K/K be the maximal abelian unramified extension (of course H_K and K are number fields). Then, H_K is called the *Hilbert class field* of K. (We say H_K/K is abelian if $\mathrm{Gal}(H_K/K)$ is abelian.)

Theorem 6.4

$\mathrm{Gal}(H_K/K) \cong C_K$.

Example 6.5

$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is always abelian.

Theorem 6.6 (Kronecker-Weber)

Every abelian Galois extension of $\mathbb{Q}$ is included in $\mathbb{Q}(\zeta_n)$ for some n.

Remark. Here's the final picture, which leads to various areas of research, like Langlands. . .

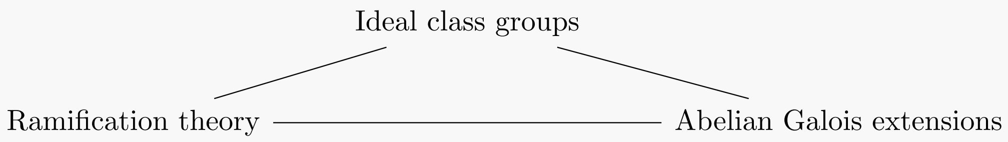

Figure 4: The even bigger picture.