MATH 6122: Algebra II

Frank Qiang
Instructor: Matthew Baker

Georgia Institute of Technology
Spring 2025

Contents

Lecture 1

Jan. 7 — Motivation for Algebraic Number Theory

1.1 Motivation: Fermat's Last Theorem

Theorem 1.1 (Fermat's last theorem[1]). *$x^n + y^n = z^n$ has no nonzero integer solutions when $n \geq 3$.*

Remark. The $n = 3$ case was solved by Euler, and the $n = 4$ case was solved by Fermat. So we will assume $n \geq 5$. We can also assume n is prime, since if $n = pm$, then we can instead consider

$$(x^m)^p + (y^m)^p = (z^m)^p.$$

Thus any nonzero solution to $x^n + y^n = z^n$ also yields a nonzero solution to $x^p + y^p = z^p$. So let $p \geq 5$ be prime, and let $\zeta = \zeta_p$ be a primitive pth root of 1. Then consider

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

Note that $x + \zeta^j y \in \mathbb{Z}[\zeta] \subseteq \mathbb{C}$. Let us pretend for the moment that $\mathbb{Z}[\zeta]$ is a UFD.[2] One can check that

$$\gcd(x + \zeta^j y, x + \zeta^k y) = 1$$

whenever $j \neq k$. If $\mathbb{Z}[\zeta]$ were a UFD, then we could conclude that

$$x + y\zeta = u\alpha^p$$

for some $u \in \mathbb{Z}[\zeta]^\times$ and $\alpha \in \mathbb{Z}[\zeta]$.[3] For the sake of illustration, suppose $u = \pm\zeta^j$ for some j. Then

$$\alpha = a_0 + a_1\zeta + \dots + a_{p-2}\zeta^{p-2}$$

for $a_i \in \mathbb{Z}$. This gives

$$\alpha^p = a_0 + a_1 + \dots + a_{p-2} \pmod{p},$$

using Fermat's little theorem, $\zeta^p = 1$, and the binomial theorem. So $\alpha^p = a \pmod{p}$ with $z \in \mathbb{Z}$, and

$$x + y\zeta = \pm a\zeta^j \pmod{p}$$

for some $0 \leq j \leq p - 1$. Note that $\zeta^{p-1} = -(1 + \zeta + \dots + \zeta^{p-2})$, and one can check as an exercise that this implies $p|x$ or $p|y$. This would have proved the "first case" of Fermat's last theorem.

[1] This problem was finally resolved by Wiles-Taylor in 1995.

[2] It is far from it, and this is likely the mistake that Fermat originally made.

[3] In a UFD, if a product of relatively prime elements is a pth power, then each factor must itself be a pth power.

Remark. However, Kummer (c. 1850) observed that $\mathbb{Z}[\zeta]$ is rarely a UFD (in fact, $\mathbb{Z}[\zeta]$ is a UFD if and only if $p \leq 19$).[4] Also, when $p \geq 5$, the unit group of $\mathbb{Z}[\zeta]$ is always infinite (so that $\mathbb{Z}[\zeta]^\times \neq \{\pm\zeta^j\}$).

Theorem 1.2 (Kummer)**.** *Fermat's last theorem holds for all "regular" primes.*[5]

Remark. The first irregular prime is 37, so Kummer's method works for $3 \leq n \leq 36$.

1.2 Algebraic Integers

Remark. To resolve these issues, Kummer realized that one can replace elements of $\mathbb{Z}[\zeta]$ by "ideal elements." Later on, Dedekind look at Kummer's work and introduced the modern notion of an ideal. We will be working towards the *unique factorization of ideals into prime ideals* in certain cases.

Remark. We will work at the level of generality of Dedekind rings (as opposed to just number rings). This is because there is an analogue of such a unique factorization of ideals for function fields of curves in algebraic geometry, and this framework is general enough to capture both cases.

Definition 1.1. Let $K/\mathbb{Q}$ be a finite extension (i.e. a *number field*). Then $\alpha \in K$ is an *algebraic integer* if there exists a monic polynomial $f \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$.

Theorem 1.3. *Let $A \subseteq B$ be rings and let $b \in B$. Then the following are equivalent:*

1. *b is integral over A (i.e. there exists a monic $f \in A[x]$ such that $f(b) = 0$).*
2. *$A[b]$ is a finitely generated A-module.*[6]
3. *$A[b]$ is contained in a subring $C \subseteq B$ which is finitely generated as an A-module.*

Proof. $(1 \Rightarrow 2)$ This direction is standard, one only needs powers up to $\deg f$ since $f(b) = 0$.

$(2 \Rightarrow 3)$ This direction is clear since $A[b]$ itself satisfies the desired conditions.

$(3 \Rightarrow 1)$ The idea is to argue via determinants and use the Cayley-Hamilton theorem for modules. □

Corollary 1.3.1. *Integrality is transitive, i.e. if B is integral over A and C is integral over B, then C is integral over A.*[7]

Proof. A finitely generated module over a finitely generated module is finitely generated. □

Corollary 1.3.2. *If α, β are integral over A, then $\alpha \pm \beta, \alpha\beta$ are also integral over A.*

Proof. This is because $\alpha \pm \beta, \alpha\beta \subseteq C = A[\alpha][\beta]$. □

Theorem 1.4. *The set of all algebraic integers in K (denoted $\mathcal{O}_K$) forms a subring of K.*[8]

Remark. This theorem is not obvious: Given $f(\alpha) = 0$ and $g(\beta) = 0$, one must find a polynomial h such that $h(\alpha + \beta) = 0$. It is not immediately obvious how to do this.

---

[4] Kummer made the first real progress on Fermat's last theorem in a long time.

[5] A prime p is *regular* if p does not divide the order of the *ideal class group* of $\mathbb{Z}[\zeta]$.

[6] Here $A[b]$ is the smallest subring of B containing A and b, so $A[b] = \{a_0 + a_1 b + a_2 b^2 + \cdots + a_k b_k : a_i \in A\}$.

[7] We say that B is *integral over* A if every $b \in B$ is integral over A.

[8] The ring of algebraic integers $\mathcal{O}_K$ of a number field K is called a *number ring*.

Lecture 2

Jan. 9 — Algebraic Integers and Dedekind Domains

2.1 More on Algebraic Integers

Proposition 2.1. *Suppose $\alpha, \beta \in \overline{\mathbb{Z}} \subseteq \mathbb{C}$, then $\alpha + \beta, \alpha\beta \in \overline{\mathbb{Z}}$.*[1]

Proof. First, note that every algebraic integer is an eigenvalue of some integer matrix (e.g. take the companion matrix for the minimal polynomial). So take linear maps $T_\alpha : V_\alpha \to V_\alpha$ and $T_\beta : V_\beta \to V_\beta$ which have α and β as eigenvalues, respectively. Then one can check that the map on the direct sum

$$T_\alpha \oplus T_\beta : V_\alpha \oplus V_\beta \to V_\alpha \oplus V_\beta$$

has $\alpha + \beta$ as an eigenvalue. Similarly, by looking at the map on the tensor product

$$T_\alpha \otimes T_\beta : V_\alpha \otimes V_\beta \to V_\alpha \otimes V_\beta$$

has $\alpha\beta$ as an eigenvalue. Hence we see that $\alpha + \beta, \alpha\beta \in \overline{\mathbb{Z}}$ as well. □

Remark. This is a constructive proof of what we showed via finitely generated modules last time.

Lemma 2.1. *Let $\alpha \in K$ be an algebraic number. Then α is an algebraic integer, i.e. $\alpha \in \mathcal{O}_K$, if and only if the minimal polynomial of α over $\mathbb{Q}$, call it $f_\alpha \in \mathbb{Q}[x]$, has integer coefficients.*

Proof. ($\Leftarrow$) This direction is clear by the definition of an algebraic integer.

($\Rightarrow$) We need to show that if $\alpha \in \mathcal{O}_K$, then $f_\alpha \in \mathbb{Z}[x]$. By assumption, there exists some monic integer polynomial $h \in \mathbb{Z}[x]$ such that $h(\alpha) = 0$. From this, we know that $f_\alpha | h$ in $\mathbb{Q}[x]$.[2] Let $\alpha_1, \ldots, \alpha_n$ be the roots of f_α with $\alpha_1 = \alpha$. Since $f_\alpha | h$, we know that $h(\alpha_i) = 0$ for every i, so $h \in \mathbb{Z}[x]$ implies that $\alpha_i \in \overline{\mathbb{Z}}$ for each i. Thus the coefficients of f_α are elementary symmetric functions of the α_i,[3] so

$$f_\alpha \in (\overline{\mathbb{Z}} \cap \mathbb{Q})[x].$$

Thus it suffices to show that $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$ to conclude the result. For this, suppose $r/s \in \mathbb{Q}$ is the root of

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x].$$

[1] Here $\overline{\mathbb{Z}}$ is the set of algebraic integers.

[2] Note that it suffices to show that $f_\alpha | h$ in $\mathbb{Z}[x]$, so alternatively, a suitable version of Gauss's lemma immediately implies the desired result.

[3] These operations preserve the notion of being an algebraic integer.

We can assume $(r, s) = 1$ without loss of generality.[4] Plugging in, we obtain

$$(r/s)^n + a_{n-1}(r/s)^{n-1} + \cdots + a_1(r/s) + a_0 = 0.$$

Clearly denominators by multiplying by s^n, we obtain

$$r^n + a_{n-1}sr^{n-1} + \cdots + a_1 s^{n-1}r + a_0 s^n = 0$$

The right-hand side is divisible by s and every term on the left-hand side except r^n is divisible by s, so we must have $s|r^n$. Since $(r, s) = 1$, this implies that $s = \pm 1$, i.e. $r/s \in \mathbb{Z}$. □

Example 2.0.1. For $K = \mathbb{Q}$, we have $\mathcal{O}_K = \mathbb{Z}$. This follows from the previous lemma since the minimal polynomial of $a \in \mathbb{Q}$ is $x - a$, which has integer coefficients precisely when $a \in \mathbb{Z}$.

Example 2.0.2. Let $K = \mathbb{Q}(\sqrt{d})$, i.e. K is *quadratic number field*. Clearly $\mathbb{Z}[\sqrt{d}] \subseteq \mathcal{O}_K$, but this is not always an equality. For example,

$$\phi = \frac{1 + \sqrt{5}}{2} \notin \mathbb{Z}[\sqrt{5}],$$

but $x^2 - x - 1$ has ϕ as a root.

Exercise 2.1. Let d be a square-free integer and $K = \mathbb{Q}(\sqrt{d})$. Show that

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2, 3 \pmod 4, \\ \mathbb{Z}[(1 + \sqrt{d})/2] & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

Definition 2.1. Let S be a ring. If $R \subseteq S$ is a subring, then we say that R is *integrally closed* in S if whenever $\alpha \in S$ is integral over R, then $\alpha \in R$.

Remark. Recall that for a domain R, its *field of fractions* K is the localization

$$K = S^{-1}R$$

where $S = R \setminus \{0\}$. There is a natural embedding of R into K via $r \mapsto r/1$.

Lemma 2.2. *The fraction field of $\mathcal{O}_K$ is K. More precisely, for every $\alpha \in K$, there exists $m \in \mathbb{Z}$, $m \neq 0$, such that $m\alpha \in \mathcal{O}_K$.*

Proof. Since α is algebraic, there exists a monic polynomial $f_\alpha \in \mathbb{Q}[x]$ such that $f_\alpha(\alpha) = 0$. By clearing denominators, there exists $m \in \mathbb{Z}$ such that $mf_\alpha \in \mathbb{Z}[x]$. So we have

$$m\alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0 = 0,$$

and multiplying by m^{n-1} on both sides, we obtain

$$m^n\alpha^n + m^{n-1}b_{n-1}\alpha^{n-1} + \cdots + m^{n-1}b_1\alpha + m^{n-1}b_0 = 0,$$

which implies

$$(m\alpha)^n + b_{n-1}(m\alpha)^{n-1} + \cdots + m^{n-2}b_1(m\alpha) + m^{n-1}b_0 = 0.$$

This shows that $m\alpha$ is integral over $\mathbb{Z}$, i.e. $m\alpha \in \mathcal{O}_K$. □

[4] Here we write (r, s) to denote $\gcd(r, s)$.

Theorem 2.1. *The ring of integers $\mathcal{O}_K$ is integrally closed (in its fraction field).*

Proof. Transitivity of integrality implies that $\mathcal{O}_K$ is integrally closed in K. The theorem then follows from the fact that K is the fraction field of $\mathcal{O}_K$. □

Remark. This theorem says that (it implies the second equality)

$$\mathcal{O}_K = \{\alpha \in K \mid \alpha \text{ is integral over } \mathbb{Z}\} = \{\alpha \in K \mid \alpha \text{ is integral over } \mathcal{O}_K\}.$$

2.2 Dedekind Domains

Definition 2.2. A *Dedekind domain* is a Noetherian integrally closed domain of dimension 1.

Remark. Recall that all rings in this class are commutative and have a 1. A *dimension* 1 *domain* is a domain which is not a field and in which every nonzero prime ideal is maximal. In general, the *dimension* of a ring R is the maximum length of a chain of prime ideals of the form

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n.$$

In dimension 1, this corresponds to $(0) \subsetneq \mathfrak{p}$ being the maximum chain for every nonzero prime ideal $\mathfrak{p}$, which is equivalent to the other definition.

Remark. Our goal for now will be to show that $\mathcal{O}_K$ is a Dedekind domain.

Definition 2.3. Let k be either $\mathbb{Q}$ or $\mathbb{R}$ and V be a finite-dimensional k-vector space. A *complete lattice* in V is a discrete additive subgroup Λ of V which spans V, where discrete means that any bounded subset of Λ is finite (equivalent to being discrete in the sense of topology).

Proposition 2.2. *Let V be as above (dimension n over k) and $\Lambda \subseteq V$ an additive subgroup which spans V. Then the following are equivalent:*

1. *Λ is discrete.*
2. *Λ is generated by n elements.*
3. *$\Lambda \cong \mathbb{Z}^n$ as $\mathbb{Z}$-modules.*

Proof. (2 ⇔ 3) This follows by the structure theorem (Λ is torsion-free since $\Lambda \subseteq V$).

(1 ⇒ 2) Suppose Λ is discrete, and let $x_1, \ldots, x_n \in \Lambda$ be a basis for V. Let Λ_0 be the $\mathbb{Z}$-module which is spanned by $x_1, \ldots, x_n$. We claim that Λ/Λ_0 is finite, which implies that Λ is also generated by n elements (exercise). To see the claim, we note that there exists an integer $M > 0$ such that if $x = \sum \lambda_i x_i \in \Lambda$ with $\lambda_i \in k$ and all $|\lambda_i| < 1/M$, then $x = 0$. This is standard and follows from all norms being equivalent in a finite-dimensional vector space and the assumption that Λ is discrete.

Now let $y_1, y_2, \ldots$ be coset representatives for Λ/Λ_0. Without loss of generality (by translating in the coset), assume each $y_i \in C$, where C is the unit cube. Cover C by M^n boxes of the form

$$\frac{m_i}{M} \leq \lambda_i < \frac{m_i + 1}{M}$$

with $m_i \in \mathbb{Z}$ and $0 \leq m_i < M$. We must have $|\Lambda/\Lambda_0| \leq M^n$, since otherwise we end up with two $y_i \neq y_j$ in the same box by the pigeonhole principle, and $y_i - y_j \in C[1/M] \cap \Lambda = \{0\}$ leads to a contradiction.

(2 ⇒ 1) This proof is to be finished next class. □

Theorem 2.2. *If I is a nonzero ideal in a number ring $\mathcal{O}_K$, then $\mathcal{O}_K/I$ is finite.*

Proof. The strategy is to show that if $[K : \mathbb{Q}] = n$, then $\mathcal{O}_K \cong \mathbb{Z}^n$ and $I \cong \mathbb{Z}^n$ as $\mathbb{Z}$-modules. This will imply that $\mathcal{O}_K/I$ is finite, which follows from the proof of the structure theorem. In fact, we will show that I and $\mathcal{O}_K$ are lattices in $K \cong \mathbb{Q}^n \subseteq \mathbb{R}^n$. Note that it suffices to show that $\mathcal{O}_K$ is a lattice, since it immediately follows that $I \subseteq \mathcal{O}_K$ is also discrete, hence also a lattice as I is an additive subgroup.

The proof is to be finished next class. □

Corollary 2.2.1. *A number ring $\mathcal{O}_K$ is Noetherian.*

Proof. Suppose that we have an ascending chain of ideals

$$I = I_0 \subseteq I_1 \subseteq I_2 \subseteq \dots.$$

Suppose without loss of generality that $I_0 \neq 0$. Since $\mathcal{O}_K/I$ is finite, by an isomorphism theorem we see that there are only finitely many ideals in $\mathcal{O}_K$ containing I. This implies that the chain must eventually stabilize, i.e. that $\mathcal{O}_K$ is Noetherian. □

Corollary 2.2.2. *A number ring $\mathcal{O}_K$ is 1-dimensional.*

Proof. Verify as an exercise that $\mathcal{O}_K$ is not a field. Now let $\mathfrak{p}$ be a nonzero prime ideal, so that $\mathcal{O}_K/\mathfrak{p}$ is a finite domain, hence a field. This implies that $\mathfrak{p}$ is maximal, so $\mathcal{O}_K$ is 1-dimensional. □

Theorem 2.3. *A number ring $\mathcal{O}_K$ is a Dedekind domain.*

Lecture 3

Jan. 14 — Unique Factorization of Ideals

3.1 Norms for Field Extensions

Remark. Let $K/\mathbb{Q}$ be a finite extension of degree n. Our goal will be to define a *norm* $N_{K/\mathbb{Q}} : K \to \mathbb{Q}$ which also sends $\mathcal{O}_K \to \mathbb{Z}$. Note that there are n distinct embeddings $\sigma_1, \dots, \sigma_n : K \to \mathbb{C}$, e.g. choose a primitive element $\theta \in K$ (so that $K = \mathbb{Q}(\theta)$) with minimal polynomial f of degree n and define $\sigma : K \to \mathbb{C}$ by sending θ to some root of f, of which there are n choices.[1]

Definition 3.1. Given a finite extension $K/\mathbb{Q}$, define the *norm* $N_{K/\mathbb{Q}} : K \to \mathbb{Q}$ by

$$N_{K/\mathbb{Q}}(x) = \prod_{i=1}^{n} \sigma_i(x),$$

where $\sigma_1, \dots, \sigma_n : K \to \mathbb{C}$ are the n distinct embeddings of K into $\mathbb{C}$.

Exercise 3.1. Show that in fact $N_{K/\mathbb{Q}}(\gamma) \in \mathbb{Q}$. (Hint: One way is via Galois theory.)

Exercise 3.2. Define $[\gamma] : K \to K$ by $x \mapsto \gamma x$, which is a $\mathbb{Q}$-linear map. Show that $N_{K/\mathbb{Q}}(\gamma) = \det[\gamma]$.

Proposition 3.1. *We have the following properties of the norm $N = N_{K/\mathbb{Q}}$:*

1. *$N(\gamma) = 0$ if and only if $\gamma = 0$;*
2. *if $\gamma \in \mathcal{O}_K$, then $N(\gamma) \in \mathbb{Z}$.*

Proof. Check these properties as an exercise. □

Theorem 3.1. *A number ring $\mathcal{O}_K$ is a complete lattice in $K \cong \mathbb{Q}^n \subseteq \mathbb{R}^n$.*

Proof. We need to show that $\mathcal{O}_K$ is discrete. Note that there exists a basis $\alpha_1, \dots, \alpha_n$ for $K/\mathbb{Q}$ such that $\alpha_i \in \mathcal{O}_K$ for every i. Now suppose otherwise that $\mathcal{O}_K$ is not discrete, so there are arbitrarily small $\lambda_1, \dots, \lambda_n \in \mathbb{Q}$ such that $\alpha = \sum \lambda_i \alpha_i$ is nonzero and in $\mathcal{O}_K$. Then

$$N_{K/\mathbb{Q}}(\alpha) = \phi(\lambda_1, \dots, \lambda_n)$$

for some homogeneous polynomial ϕ of degree n (since each $\sigma(\alpha) = \sum \lambda_i \sigma(\alpha_i)$). Thus if $|\lambda_i| \ll 1$, the polynomial ϕ also gets small and we can obtain $0 < |N_{K/\mathbb{Q}}(\alpha)| < 1$, a contradiction since $N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$. □

Corollary 3.1.1. *If $I \subseteq \mathcal{O}_K$ is a nonzero ideal, then I is also a complete lattice in $\mathbb{R}^n$.*

[1] As an example of having n embeddings, consider $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R} \subseteq \mathbb{C}$, where we can send $\sqrt{2} \mapsto \pm\sqrt{2}$.

Proof. One needs to show that I contains a basis for $K/\mathbb{Q}$. Choose any nonzero $c \in I$ and consider $c\alpha_1, \ldots, c\alpha_n \in I$ (since I is an ideal). This will also be a basis for $K/\mathbb{Q}$ since $c \neq 0$. □

Corollary 3.1.2. *We have $|\mathcal{O}_K/I| < \infty$ for every nonzero ideal $I \subseteq \mathcal{O}_K$.*

Proof. This is because $\mathcal{O}_K \cong I \cong \mathbb{Z}^n$ as $\mathbb{Z}$-modules, so the result follows by the structure theorem. □

Remark. These details complete the proof from last time that $\mathcal{O}_K$ is a Dedekind domain.

Remark. The following is a preview of what we will do later in the class: We will define the *norm* of an ideal to be $N(I) = |\mathcal{O}_K/I|$. One can show that if $I = (\gamma)$, then $N(I) = N(\gamma)$. An extension of the previous techniques then leads to a proof of the finiteness of the *ideal class group*.

3.2 Unique Factorization of Ideals

Remark. Recall that for ideals $I = (\alpha_1, \ldots, \alpha_k)$ and $J = (\beta_1, \ldots, \beta_\ell)$, their *product* is $IJ = (\alpha_i\beta_j)_{i,j}$.

Example 3.1.1. Consider $R = \mathbb{Z}[\sqrt{-5}]$, which is the ring of integers $\mathcal{O}_K$ in $K = \mathbb{Q}(\sqrt{-5})$. Note that

$$6 = 2(3) = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

and these elements are irreducible and not associates, so R is not a UFD. However, let

$$\mathfrak{p}_1 = (2, 1 + \sqrt{-5}), \quad \mathfrak{p}_2 = (2, 1 - \sqrt{-5}), \quad \mathfrak{p}_3 = (3, 1 + \sqrt{-5}), \quad \mathfrak{p}_4 = (3, 1 - \sqrt{-5}).$$

None of these ideals are principal, but they are all prime ideals. One can check that

$$\mathfrak{p}_1\mathfrak{p}_2 = (4, 2 - 2\sqrt{-5}, 2 + 2\sqrt{-5}, 6) = (2),$$

that $\mathfrak{p}_3\mathfrak{p}_4 = (3)$, that

$$\mathfrak{p}_1\mathfrak{p}_3 = (6, 2 + 2\sqrt{-5}, 3 + 3\sqrt{-5}, 6) = (1 + \sqrt{-5}),$$

and finally that $\mathfrak{p}_2\mathfrak{p}_4 = (1 - \sqrt{-5})$. At the level of ideals, the original equation then becomes

$$(6) = (2)(3) = (\mathfrak{p}_1\mathfrak{p}_2)(\mathfrak{p}_3\mathfrak{p}_4) = (\mathfrak{p}_1\mathfrak{p}_3)(\mathfrak{p}_2\mathfrak{p}_4) = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

In fact, the previous nonunique factorization is now the same factorization in the language of ideals.

Lemma 3.1. *Let $I_1, \ldots, I_n$ be ideals in a commutative ring R, and let $\mathfrak{p}$ be a prime ideal. Suppose that $I_1 I_2 \ldots I_n \subseteq \mathfrak{p}$. Then $I_j \subseteq \mathfrak{p}$ for some j.*

Proof. Check this as an exercise, it follows from the definition of a prime ideal. □

Lemma 3.2. *Let R be a Noetherian ring, and $I \subseteq R$ be a nonzero ideal. Then there exist nonzero prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ such that $\mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_r \subseteq I$.*

Proof. Let Σ be the set of all I for which the lemma is false. If $\Sigma \neq \varnothing$, then since R is Noetherian, Σ has a maximal element (pick $I_1 \in \Sigma$, if it is not maximal, then we can find $I_2 \in \Sigma$ with $I_1 \subsetneq I_2$, and we obtain $I_1 \subsetneq I_2 \subsetneq \ldots$ by continuing; this chain must terminate since R is Noetherian). Let J be such a maximal element. Now J cannot be prime, so there exist $a, b \in R$ such that $ab \in J$ but $a, b \notin J$. Let

$$\mathfrak{a} = (J, a) \supsetneq J \quad \text{and} \quad \mathfrak{b} = (J, b) \supsetneq J.$$

Then $\mathfrak{a} \supseteq \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_m$ and $\mathfrak{b} \supseteq \mathfrak{q}_1\mathfrak{q}_2 \dots \mathfrak{q}_n$. Since $\mathfrak{ab} = (J^2, Ja, Jb, ab) \subseteq J$, we obtain

$$J \supseteq \mathfrak{ab} \supseteq \mathfrak{p}_1 \dots \mathfrak{p}_m\mathfrak{q}_1 \dots \mathfrak{q}_n,$$

which is a contradiction. Thus we must have $\Sigma = \varnothing$, so the lemma holds for every nonzero ideal I. □

3.3 Inverse Ideals

Example 3.1.2. Consider the problem of finding $(2)^{-1}$ in $\mathbb{Z}$. Logically, the answer should be something like $(1/2) = (1/2)\mathbb{Z} \subseteq \mathbb{Q}$, which is not an ideal in $\mathbb{Z}$.[2] This will satisfy $2((1/2)\mathbb{Z}) = \mathbb{Z}$.

Definition 3.2. Let R be an integral domain with fraction field K, and let I be a nonzero ideal in R. Then the *inverse ideal* I^{-1} of I is

$$I^{-1} = \{x \in K \mid xI \subseteq R\}.$$

Example 3.2.1. Let $R = \mathbb{Z}$ and $I = (2)$. Then we can see that

$$I^{-1} = \{x \in \mathbb{Q} \mid x(2) \subseteq \mathbb{Z}\} = \frac{1}{2}\mathbb{Z}.$$

Remark. Our goal at this point is to show that if R is Dedekind, then $II^{-1} = R$. Note that if M, N are two R-submodules of K, then their product is well-defined:

$$MN = R\text{-submodule of } K \text{ generated by } \{xy \mid x \in M, y \in N\},$$

e.g. $((1/2)\mathbb{Z})((1/3)\mathbb{Z}) = (1/6)\mathbb{Z}$. This is how we will make sense of the product II^{-1}.

Lemma 3.3. *If $I = (a)$, then $I^{-1} = (a^{-1})$ and $II^{-1} = (1) = R$.*

Proof. Check this as an exercise. □

Proposition 3.2. *If R is Dedekind, $I \neq 0$ is an ideal, and $\mathfrak{p} \neq 0$ is a prime ideal, then $\mathfrak{p}^{-1}I \neq I$.*

Proof. First consider the special case $I = R$, and we want to show that $\mathfrak{p}^{-1} \neq R$. We will find $x \in \mathfrak{p}^{-1}$ which is not in R. To do this, we will take $x = a^{-1}b = b/a$ for some $a, b \in R$. We want $(b/a)\mathfrak{p} \subseteq R$, so we should look for $b\mathfrak{p} \subseteq (a)$ with $b \notin (a)$. Let $a \in \mathfrak{p}$ be any nonzero element, and we will find a suitable b.

Since R is Noetherian, there exist prime ideals $\mathfrak{p}_i \neq 0$ such that $\mathfrak{p}_1 \dots \mathfrak{p}_r \subseteq (a) \subseteq \mathfrak{p}$. Without loss of generality, we can assume r is minimal. This then implies that $\mathfrak{p}_i \subseteq \mathfrak{p}$ for some i, which implies $\mathfrak{p}_i = \mathfrak{p}$ since R is 1-dimensional. Assume without loss of generality that $i = 1$, so $\mathfrak{p}_1 = \mathfrak{p}$.

If $r = 1$, then $\mathfrak{p} = (a)$, so that $\mathfrak{p}^{-1} = (a^{-1}) \neq R$ since a is not a unit. So now assume $r \geq 2$. Then

$$\mathfrak{p}_2 \dots \mathfrak{p}_r \not\subseteq (a)$$

by the minimality of r, so there exists $b \in \mathfrak{p}_2 \dots \mathfrak{p}_r$ such that $b \notin (a)$. But $b\mathfrak{p} = b\mathfrak{p}_1 \subseteq (a)$, so the element $x = b/a \in \mathfrak{p}^{-1}$ but is not in R. This proves the statement when $I = R$.

[2] Note that this is not an ideal of $\mathbb{Q}$ either since it is not closed under multiplication by elements of $\mathbb{Q}$. The inverse ideal $(2)^{-1}$ is instead a $\mathbb{Z}$-submodule of $\mathbb{Q}$, viewed as a $\mathbb{Z}$-module.

In the general case, using the hypothesis that R is Noetherian, we can write $I = (\alpha_1, \ldots, \alpha_n)$. Assume otherwise that $\mathfrak{p}^{-1}I = I$. Then for $x \in \mathfrak{p}^{-1}$, we can write

$$x\alpha_i = \sum_{j=1}^{n} a_{ij}\alpha_j, \quad a_{ij} \in R.$$

Let $A = (a_{ij})$ and define $T = xI_n - A$. Check as an exercise that $\det T = 0$. Since $\det T$ is a monic polynomial in x with coefficients in R, we see that x is integral over R. Since R is integrally closed, we must have $x \in R$, so we get $\mathfrak{p}^{-1} = R$. This contradicts the above special case. □

Remark. The key idea of the proof is Cayley-Hamilton for modules: Let R be a commutative ring and M a finitely generated R-module. Then if $JM = M$, there exists a with $1 - a \in J$ such that $aM = M$. The proof above uses a similar strategy to the proof of this statement.

Lecture 4

Jan. 16 — Ideal Class Group

4.1 Unique Factorization of Ideals, Continued

The following is a corollary of Proposition 3.2:

Corollary 4.0.1. *If R is Dedekind and $\mathfrak{p} \neq 0$ is a prime ideal, then $\mathfrak{p}^{-1}\mathfrak{p} = R = (1)$.*

Proof. First note that we have $\mathfrak{p} \subseteq \mathfrak{p}^{-1}\mathfrak{p} \subseteq R$ since $R \subseteq \mathfrak{p}^{-1}$ by the definition of $\mathfrak{p}^{-1}$. Furthermore, $\mathfrak{p}^{-1}$ is an R-submodule of K, so $\mathfrak{p}^{-1}\mathfrak{p}$ is an R-submodule of R, i.e. an ideal of R. Also, by Proposition 3.2, $\mathfrak{p}^{-1}\mathfrak{p} \neq \mathfrak{p}$. Now R being 1-dimensional implies that $\mathfrak{p}$ is maximal, so we must have $\mathfrak{p}^{-1}\mathfrak{p} = R$. □

Proposition 4.1. *A Dedekind domain R admits unique factorization of ideals into prime ideals.*

Proof. For uniqueness, suppose that $I = \mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$. Then $\mathfrak{q}_1 \dots \mathfrak{q}_s \subseteq \mathfrak{p}_1$, so we must have some $\mathfrak{q}_i \subseteq \mathfrak{p}_1$. Without loss of generality, assume $\mathfrak{q}_1 \subseteq \mathfrak{p}_1$, so that $\mathfrak{q}_1 = \mathfrak{p}_1$. Now multiplying by $\mathfrak{p}_1^{-1}$, we get

$$\mathfrak{p}_2 \dots \mathfrak{p}_r = \mathfrak{q}_2 \dots \mathfrak{q}_s.$$

Proceeding by induction finishes the proof for uniqueness.

Now we argue for existence. Let Σ be the set of all proper ideals of R which cannot be written as a product of prime ideals. If Σ is nonempty, then the Noetherian property of R implies that Σ has a maximal element J. Then $J \subsetneq \mathfrak{p}$ for some maximal ideal $\mathfrak{p}$, which is equivalently a nonzero prime ideal since R is one-dimensional. Since $R \subseteq \mathfrak{p}^{-1}$, we have the chain of inclusions

$$J \subsetneq J\mathfrak{p}^{-1} \subsetneq \mathfrak{p}\mathfrak{p}^{-1} = R.$$

Since J was maximal in Σ, we must have $J\mathfrak{p}^{-1} \notin \Sigma$, so we can write $J\mathfrak{p}^{-1} = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_r$. But then we have $J = \mathfrak{p}\mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_r$ which is a contradiction with $J \in \Sigma$. □

4.2 Ideal Class Group

Proposition 4.2. *In a Dedekind ring R, to contain is to divide, i.e. $I \subseteq J$ if and only if $J|I$.*[1]

Proof. ($\Rightarrow$) If $I \subseteq J$, then $IJ^{-1} \subseteq JJ^{-1} = R$.[2] Then $J' = IJ^{-1}$ is an ideal and satisfies $I = JJ'$.

($\Leftarrow$) This is the easier direction, verify this as an exercise. □

[1] We say that J *divides* I, written $J|I$, if $I = JJ'$ for some ideal J'.

[2] Note that we have technically only proved this property for prime ideals, but any ideals factors as prime ideals and we can argue via this factorization.

Definition 4.1. Let R be an integral domain. A *fractional ideal* of R is an R-submodule J of K such that aJ is an ideal for some $a \in R$.

Exercise 4.1. If $I \subseteq R$ is an ideal, then show that I^{-1} is a fractional ideal.

Exercise 4.2. If J is an R-submodule of K, then show that J is a fractional ideal if and only if J is finitely generated as an R-module.

Exercise 4.3. Show that set of nonzero fractional ideals in a Dedekind domain R forms a group under multiplication.

Remark. In fact, one can actually show that

$$I(R) = \{\text{nonzero fractional ideals}\} = \{\mathfrak{p}_1^{k_1}\mathfrak{p}_2^{k_2}\dots\mathfrak{p}_r^{k_r} \mid k_i \in \mathbb{Z}\}.$$

Due to unique factorization, this is actually the free abelian group on the set of nonzero prime ideals. We can also define

$$P(R) = \{\text{principal fractional ideals}\} = \{aR \mid a \in K\}.$$

Definition 4.2. The *ideal class group* of a Dedekind domain R is the quotient $\mathrm{Cl}(R) = I(R)/P(R)$.[3]

Exercise 4.4. Show that $\mathrm{Cl}(R)$ is also the equivalence classes of ideals under $\sim$, where $I \sim J$ if there exist $a, b \in R$ such that $aI = bJ$.

Remark. Our goal now will be to show that if $R = \mathcal{O}_K$ and $[K : \mathbb{Q}] < \infty$, then $\mathrm{Cl}(R)$ is finite. The key tool will be the norm $N : \{\text{ideals of } R\} \to \mathbb{N}$, where $\mathbb{N}$ contains 0.

Definition 4.3. We define the *norm* of an ideal $I \subseteq R$ to be $N(I) = |R/I|$.

Remark. To prove the finiteness of $\mathrm{Cl}(\mathcal{O}_K)$ where K is a number field, we will need to show the following properties of the norm N:

- $N((\alpha)) = N_{\mathbb{Q}}^K(\alpha)$.
- $N(IJ) = N(I)N(J)$.

Then, we will proceed to show the following:

- There exists $M \geq 0$ such that $\{\text{ideals } I \mid N(I) \leq M\}$ is finite.
- Letting $\nu(I) = \min_{\alpha \in I}\{N(I)/N(\alpha)\}$, there exists M such that $\nu(I) \leq M$ for every I. Moreover, $\nu(I) = 1$ if and only if I is principal. Note that $\nu(I) \in \mathbb{Z}$ by the multiplicative property of N.

4.3 Discriminants

Definition 4.4. Let L/K be a finite separable field extension, where $[L : K] = n$. Fix a Galois closure M of L/K, so there are n distinct embeddings $\sigma_1, \dots, \sigma_n : L \to M$ fixing K. The *norm* of $\alpha \in L$ is

$$N_K^L(\alpha) = \sigma_1(\alpha)\dots\sigma_n(\alpha) \in K.$$

Now let $\alpha_1, \dots, \alpha_n \in L$. The *discriminant* of $\alpha_1, \dots, \alpha_n$ is

$$\Delta(\alpha_1, \dots, \alpha_n) = \det \begin{bmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \cdots & \sigma_n(\alpha_n) \end{bmatrix}^2 = (\det T)^2.$$

[3] As a shorthand, we may write "the class group of a number field K" to mean $\mathrm{Cl}(\mathcal{O}_K)$.

Lemma 4.1. *For $\alpha_1, \dots, \alpha_n \in L$, the discriminant $\Delta(\alpha_1, \dots, \alpha_n) \in K$ and is nonzero if and only if $\alpha_1, \dots, \alpha_n$ form a basis for L/K.*

Proof. ($\Rightarrow$) One can show the contrapositive that if $\alpha_1, \dots, \alpha_n$ are linearly dependent, then $\Delta = 0$.

($\Leftarrow$) Let $\alpha_1, \dots, \alpha_n$ be a basis for L/K. By the primitive element theorem, there exists $\theta \in L$ such that $L = K(\theta)$, so that $1, \theta, \theta^2, \dots, \theta^{n-1}$ form a basis for L/K. Then we have

$$\begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = M \begin{bmatrix} 1 \\ \vdots \\ \theta^{n-1} \end{bmatrix}$$

for some matrix $M \in M_{n\times n}(K)$ with $\det M \neq 0$. This implies that

$$\begin{bmatrix} \sigma_i(\alpha_1) \\ \vdots \\ \sigma_i(\alpha_n) \end{bmatrix} = M \begin{bmatrix} 1 \\ \vdots \\ \sigma_i(\theta^{n-1}) \end{bmatrix}.$$

Thus if we define

$$T' = \begin{bmatrix} \sigma_1(1) & \cdots & \sigma_1(\theta^{n-1}) \\ \vdots & \ddots & \vdots \\ \sigma_n(1) & \cdots & \sigma_n(\theta^{n-1}) \end{bmatrix} = \begin{bmatrix} \sigma_1(1) & \cdots & \sigma_1(\theta)^{n-1} \\ \vdots & \ddots & \vdots \\ \sigma_n(1) & \cdots & \sigma_n(\theta)^{n-1} \end{bmatrix}$$

and $\Delta' = (\det T')^2$, then $T = T'M^t$ implies $\Delta = \Delta'(\det M)^2$. Now T' is a Vandermonde matrix, so

$$(\det T')^2 = \prod_{i\neq j} (\sigma_i(\theta) - \sigma_j(\theta)) \neq 0.$$

We can also see $\Delta' = (\det T')^2 \in K^\times$ (via Galois theory) and $(\det M)^2 \in K^\times$, so $\Delta \in K^\times$ as well. □

Theorem 4.1. *Let K be a number field and $\alpha \in \mathcal{O}_K$. Then $N((\alpha)) = N(\alpha)$.*

Proof. Let $\omega_1, \dots, \omega_n$ be a $\mathbb{Z}$-basis for $\mathcal{O}_K$, and let $\alpha_i = \alpha\omega_i$. Then $\alpha_1, \dots, \alpha_n$ is a $\mathbb{Z}$-basis for $\mathfrak{a} = (\alpha)$. Thus we may write

$$\begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = A \begin{bmatrix} \omega_1 \\ \vdots \\ \omega_n \end{bmatrix}$$

for some matrix $A \in M_{n\times n}(\mathbb{Z})$. Now the theory of finitely generated modules over a PID implies that $N(\mathfrak{a}) = |\det A|$. (This is because we have two free $\mathbb{Z}$-modules of rank n: $\mathcal{O}_K$ and $\mathfrak{a} \subseteq \mathcal{O}_K$. So if $A \sim A'$ where $A' = \operatorname{diag}(d_1, \dots, d_n)$ is in Smith normal form, then $|\mathcal{O}_K/\mathfrak{a}| = |(\mathbb{Z}/d_1) \times \cdots \times (\mathbb{Z}/d_n)|$, so we see that $N(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}| = |d_1 \dots d_n| = |\det A'| = |\det A|$.) Thus we have

$$\Delta(\alpha_1, \dots, \alpha_n) = (\det A)^2 \Delta(\omega_1, \dots, \omega_n).$$

But we can also see that

$$\begin{aligned} \Delta(\alpha_1, \dots, \alpha_n) = \Delta(\alpha\omega_1, \dots, \alpha\omega_n) &= \det \begin{bmatrix} \sigma_1(\alpha\omega_1) & \cdots & \sigma_1(\alpha\omega_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\alpha\omega_1) & \cdots & \sigma_n(\alpha\omega_n) \end{bmatrix}^2 \\ &= (\sigma_1(\alpha) \dots \sigma_n(\alpha))^2 \Delta(\omega_1, \dots, \omega_n) = N(\alpha)^2 \Delta(\omega_1, \dots, \omega_n). \end{aligned}$$

This shows that $N(\mathfrak{a})^2 = (\det A)^2 = N(\alpha)^2$, so that $N(\mathfrak{a}) = N(\alpha)$ since these values are positive. □

Lecture 5

Jan. 21 — Finiteness of the Class Group

5.1 Multiplicativity of the Norm

Theorem 5.1. *If $I, J \subseteq \mathcal{O}_K$ are ideals, then $N(IJ) = N(I)N(J)$.*

Proof. First observe that if $\mathfrak{a}, \mathfrak{b} \subseteq \mathcal{O}_K$ are relatively prime ideals (i.e. $\mathfrak{a} + \mathfrak{b} = (1)$), then

$$\mathcal{O}_K/\mathfrak{ab} \cong \mathcal{O}_K/\mathfrak{a} \times \mathcal{O}_K/\mathfrak{b}$$

by the Chinese remainder theorem, and the result immediately follows. One can also show that if $\mathfrak{p} \neq \mathfrak{q}$ are nonzero prime ideals in $\mathcal{O}_K$, then $\mathfrak{p}^s$ and $\mathfrak{q}^t$ are relatively prime for every s, t. Thus by unique factorization of I, J into prime ideals, it is enough to prove $N(\mathfrak{p}^m) = (N(\mathfrak{p}))^m$ for a prime ideal $\mathfrak{p}$.

To do this, observe that we have the chain of inclusions

$$\mathcal{O}_K \supsetneq \mathfrak{p} \supsetneq \mathfrak{p}^2 \cdots \supsetneq \mathfrak{p}^m,$$

and it suffices to show that $[\mathfrak{p}^k : \mathfrak{p}^{k+1}] = N(\mathfrak{p})$ for each $0 \leq k < m$. We will show the stronger result that $\mathcal{O}_K/\mathfrak{p} \cong \mathfrak{p}^k/\mathfrak{p}^{k+1}$ as abelian groups. To do this, pick $\gamma \in \mathfrak{p}^k \setminus \mathfrak{p}^{k+1}$ (note that $\mathfrak{p}^k \neq \mathfrak{p}^{k+1}$ by unique factorization) and define $\phi : \mathcal{O}_K \to \mathfrak{p}^k/\mathfrak{p}^{k+1}$ by $x \mapsto \gamma x$. Since $\gamma x \in \mathfrak{p}^{k+1}$ whenever $x \in \mathfrak{p}$, this induces a map $\phi : \mathcal{O}_K/\mathfrak{p} \to \mathfrak{p}^k/\mathfrak{p}^{k+1}$, which we prove is an isomorphism in Proposition 5.1. □

Proposition 5.1. *The map $\phi : \mathcal{O}_K/\mathfrak{p} \to \mathfrak{p}^k/\mathfrak{p}^{k+1}$ by $x \mapsto \gamma x$ is an isomorphism of abelian groups.*

Proof. We will show the following claims:

1. $(\gamma) + \mathfrak{p}^{k+1} = \mathfrak{p}^k$. This implies that ϕ is surjective.
2. $(\gamma) \cap \mathfrak{p}^{k+1} = \gamma\mathfrak{p}$. This means that if $\gamma x \in \gamma\mathfrak{p}$, then $x \in \mathfrak{p}$, i.e. ϕ is injective.

(1) Let $I = (\gamma) + \mathfrak{p}^{k+1}$. Since we already know that $\mathfrak{p}^k | (\gamma)$, we have $\mathfrak{p}^k | I$. But $I \supsetneq \mathfrak{p}^{k+1}$, so $I | \mathfrak{p}^{k+1}$, and the containment being strict implies that we must have $I = \mathfrak{p}^k$.

(2) Let $I' = (\gamma) \cap \mathfrak{p}^{k+1}$. Since $\gamma \in \mathfrak{p}^k$, we have $\gamma\mathfrak{p} \subseteq I'$. This is one containment. Conversely, let $x \in I'$. Write $x = \gamma y$, where $y \in \mathcal{O}_K$ and $\gamma y \in \mathfrak{p}^{k+1}$. Now note that[1]

$$\mathrm{ord}_{\mathfrak{p}}(\gamma) + \mathrm{ord}_{\mathfrak{p}}(y) = \mathrm{ord}_{\mathfrak{p}}(\gamma y) \geq k + 1.$$

But $\mathrm{ord}_{\mathfrak{p}}(\gamma) = k$ (since $\gamma \in \mathfrak{p}^k \setminus \mathfrak{p}^{k+1}$), so $\mathrm{ord}_{\mathfrak{p}}(y) \geq 1$. This implies that $\mathfrak{p} | (y)$, so $y \in \mathfrak{p}$. Since $x = \gamma y$, this gives $x \in \gamma\mathfrak{p}$. This yields the other containment, and so $I' = \gamma\mathfrak{p}$. □

[1] Here $\mathrm{ord}_{\mathfrak{p}}(\alpha) = \mathrm{ord}_{\mathfrak{p}}(\mathfrak{a})$ is the largest integer m such that $\mathfrak{p}^m | \mathfrak{a}$, where $\mathfrak{a} = (\alpha)$.

Corollary 5.1.1. *Let $[K:\mathbb{Q}] = n$ and $p \in \mathbb{Z}$ be a prime number. Write*

$$(p) = p\mathcal{O}_K = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i},$$

where the $\mathfrak{p}_i$ are distinct prime ideals. Then $\sum_{i=1}^{r} e_i f_i = n$, where $N(\mathfrak{p}_i) = p^{f_i}$.

Proof. Since the norm is multiplicative, we have

$$p^n = N(p\mathcal{O}_K) = N(p) = \prod_{i=1}^{n} \sigma_i(p)$$

since each σ_i fixes p. Then since $p\mathcal{O}_K = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$, we have[2]

$$p^n = N(p\mathcal{O}_K) = N(\prod \mathfrak{p}_i^{e_i}) = \prod (N(\mathfrak{p}_i))^{e_i} = \prod (p^{f_i})^{e_i} = \prod p^{e_i f_i}.$$

Thus $n = \sum_{i=1}^{r} e_i f_i$, which is the desired result. □

Remark. In the above case, we will say that the $\mathfrak{p}_i$ "lie over" p.

5.2 Finiteness of the Class Group

Theorem 5.2. *Let K be a number field. Then there exists $M > 0$ such that every nonzero ideal I of $\mathcal{O}_K$ contains a nonzero element α with $|N(\alpha)| \leq M \cdot N(I)$. Equivalently, α satisfies*

$$\inf_{\alpha \in I} \frac{N(\alpha)}{N(I)} \leq M,$$

and the above infimum is 1 if and only if I is principal.

Proof. Choose an integral basis $\alpha_1, \ldots, \alpha_n$ of $\mathcal{O}_K$, and let I be a nonzero ideal. Choose m such that $m^n \leq N(I) < (m+1)^n$. Then define the set

$$\Sigma = \left\{ \sum_{j=1}^{n} m_j \alpha_j : 0 \leq m_j \leq m, m_j \in \mathbb{Z} \right\}.$$

Note that $\#\Sigma = (m+1)^n > N(I) = |\mathcal{O}_K / I|$, so by the pigeonhole principle there exist $x \neq y$ in $\mathcal{O}_K$ such that $\alpha = x - y \in I$, and we can write $\alpha = \sum m_j \alpha_j$ where $|m_j| \leq m$ for every j. Then

$$|N(\alpha)| = \prod_{i=1}^{n} |\sigma_i(\alpha)| \leq \prod_{i=1}^{n} \sum_{j=1}^{n} |m_j||\sigma_i(\alpha_j)| \leq m^n \prod_{i=1}^{n} \sum_{j=1}^{n} |\sigma_i(\alpha_j)| \leq N(I) \cdot M,$$

where $M = \prod_{i=1}^{n} \sum_{j=1}^{n} |\sigma_i(\alpha_j)|$ is independent of I (but depends on the choice of integral basis). □

Corollary 5.2.1. *Every ideal class in $\mathcal{O}_K$ contains a nonzero ideal of norm at most M.*

[2]Note that $\mathcal{O}_K/\mathfrak{p}_i$ is a finite field (since $\mathfrak{p}_i \neq 0$ is prime, hence maximal in $\mathcal{O}_K$) and a vector space over $\mathbb{Z}/p$ since $(p) \subseteq \mathfrak{p}_i$. So $\mathcal{O}_K/\mathfrak{p}_i$ has prime characteristic, hence $N(\mathfrak{p}_i) = |\mathcal{O}_K/\mathfrak{p}_i| = p^{f_i}$ for some f_i.

Proof. Let $C \in \mathrm{Cl}(\mathcal{O}_K)$, and let I be an ideal with $[I] = C^{-1}$. By the above theorem, choose $\alpha \in I$ such that $|N(\alpha)| \leq M \cdot N(I)$. Now $(\alpha) = IJ$ for some J, so $[J] = [I]^{-1} = C$, and

$$N(J) = \frac{|N(\alpha)|}{N(I)} \leq M,$$

which proves the desired result. □

Lemma 5.1. *The set of ideals with norm bounded by M is finite, i.e. $|\{I : N(I) \leq M\}| < \infty$.*

Proof. One way to proceed is to write $I = \prod \mathfrak{p}_i^{e_i}$, and then use $N(\mathfrak{p}_i) = p^{f_i}$.

Another way to prove this is to note that if $|N(I)| = m$, then $mx = 0$ in $\mathcal{O}_K/I$ for every $x \in \mathcal{O}_K$. So $I \supseteq m\mathcal{O}_K$. But $\mathcal{O}_K/m\mathcal{O}_K$ is finite, so there are only finitely many ideals containing $m\mathcal{O}_K$. □

Corollary 5.2.2. *The ideal class group of a number field $\mathrm{Cl}(\mathcal{O}_K)$ is finite.*

Proof. Each ideal class can be represented by an ideal of norm bounded by M, and there are only finitely many such ideals. Thus there can only be finitely many ideal classes. □

5.3 Computing Rings of Integers

Remark. Recall that if $[K : \mathbb{Q}] = n$ and $\alpha_1, \ldots, \alpha_n \in K$ are a basis for $K/\mathbb{Q}$, then $\Delta(\alpha_1, \ldots, \alpha_n) \in \mathbb{Q}^\times$. Moreover, if $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$, then $\Delta(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$. Also, if $\alpha_1, \ldots, \alpha_n$ are a $\mathbb{Z}$-basis for $\mathcal{O}_K$, then

$$\Delta(\alpha_1, \ldots, \alpha_n) = \Delta_K = \Delta(\mathcal{O}_K)$$

is independent of the choice of $\mathbb{Z}$-basis. So Δ_K is an invariant of K (or of $\mathcal{O}_K$), called its *discriminant*.

Proposition 5.2. *Let $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$ be a basis for $K/\mathbb{Q}$, and let $d = \Delta(\alpha_1, \ldots, \alpha_n)$. Then*

$$\mathbb{Z}[\alpha_1, \ldots, \alpha_n] \subseteq \mathcal{O}_K \subseteq \mathbb{Z}\left[\frac{\alpha_1}{d}, \ldots, \frac{\alpha_n}{d}\right].$$

Proof. Suppose $\alpha \in \mathcal{O}_K$, so we can write (since $\alpha_1, \ldots, \alpha_n$ is a basis for $K/\mathbb{Q}$)

$$\alpha = c_1\alpha_1 + \cdots + c_n\alpha_n, \quad c_i \in \mathbb{Q}.$$

We want to show that $dc_j \in \mathbb{Z}$. Note that $\sigma_i(\alpha) = c_1\sigma_i(\alpha_1) + \cdots + c_n\sigma_i(\alpha_n)$, so

$$\begin{bmatrix} \sigma_1(\alpha) \\ \vdots \\ \sigma_1(\alpha) \end{bmatrix} = T \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix},$$

where $T = (\sigma_i(\alpha_j))$. Multiplying both sides by $\operatorname{adj} T$, we get (note that $T \operatorname{adj} T = \delta I$, where $\delta = \det T$)

$$\begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix} = \delta \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix},$$

where the $\beta_i \in \mathcal{O}_K$. Let $m_j = \delta\beta_j$, and noting that $\delta^2 = d$ by definition, we have

$$\begin{bmatrix} m_1 \\ \vdots \\ m_n \end{bmatrix} = d \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix}.$$

This tells us that $dc_i \in \mathcal{O}_K$ for every i. But the c_i were also rational, so in fact $dc_i \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$. □

Lemma 5.2. *Let $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$ be a basis for $K/\mathbb{Q}$. Let*

$$M = \mathbb{Z}\text{-module spanned by } \alpha_1, \ldots, \alpha_n.$$

Then $\Delta_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) = \Delta_K \cdot |\mathcal{O}_K/M|^2$.

Proof. Check this as an exercise; it is a calculation involving determinants. □

Corollary 5.2.3. *Let $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$ be a basis for $K/\mathbb{Q}$. If $\Delta(\alpha_1, \ldots, \alpha_n)$ is square-free, then the $\alpha_1, \ldots, \alpha_n$ form an integral basis.*

Proof. If the α_i do not form a basis, then the Δ will contain a $|\mathcal{O}_K/M|^2$ factor by the lemma. □

Example 5.0.1. Let $K = \mathbb{Q}(\sqrt{d})$, where d is square-free. Then we can see that

$$\Delta_{K/\mathbb{Q}}(1, \sqrt{d}) = \det \begin{bmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{bmatrix}^2 = 4d.$$

Thus $4d = \Delta_{K/\mathbb{Q}} \cdot |\mathcal{O}_K/M|^2$, where $M = \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \sqrt{d}$. Since d is square-free, $[\mathcal{O}_K : M] = 1$ or 2. Now if we have $|\mathcal{O}_K/(\mathbb{Z} + \mathbb{Z}\sqrt{d})| = 2$, then at least one of

$$\frac{1}{2}, \quad \frac{\sqrt{d}}{2}, \quad \frac{1+\sqrt{d}}{2}, \quad \frac{1-\sqrt{d}}{2}$$

must be an algebraic integer. The first two are obviously not algebraic integers, and the third is an algebraic integer if and only if the fourth one is (since they are conjugates). So the index is 2 if and only if $(1 + \sqrt{d})/2 \in \mathcal{O}_K$. By looking at the coefficients of the minimal polynomial

$$x^2 - x + \frac{1-d}{4},$$

this happens if and only if $(1 - d)/4 \in \mathbb{Z}$, which is equivalent to $d \equiv 1 \pmod 4$.

Lecture 6

Jan. 23 — Computing Rings of Integers

6.1 More on Computing of Rings of Integers

Lemma 6.1. *Let $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$ be a basis for $K/\mathbb{Q}$, and suppose that $\mathcal{O}_K/(\mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n)$ has exponent m, i.e. $m\alpha \in \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$ for every $\alpha \in \mathcal{O}_K$. Then*

$$\mathcal{O}_K \subseteq \mathbb{Z}\frac{\alpha_1}{m} \oplus \cdots \oplus \mathbb{Z}\frac{\alpha_n}{m}.$$

Moreover, if $\mathcal{O}_K \neq \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$, then there exist $0 \leq m_i \leq m-1$, not all zero, such that

$$m_1\frac{\alpha_1}{m} + \cdots + m_n\frac{\alpha_n}{m} \in \mathcal{O}_K.$$

Proof. The idea is the following: Let $M = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$, so $m\mathcal{O}_K \subseteq M$. Then $\mathcal{O}_K \subseteq (1/m)M$, which proves the first part. Now if $\mathcal{O}_K \neq M$, then there exists a nonzero element of $(1/m)M$ which is not in M. This gives a nonzero element in the quotient:

$$\frac{(1/m)M}{M} = \left[m_1\frac{\alpha_1}{m} + \cdots + m_n\frac{\alpha_n}{m}\right]$$

for some m_i, as in the statement. □

Example 6.0.1. We can apply this lemma to our example from last lecture: Let $K = \mathbb{Q}(\sqrt{d})$, where d is square-free. Then $\Delta(1, \sqrt{d}) = 4d$, so $\Delta_K | 4d$. Then we have

$$\frac{4d}{\Delta_K} = [\mathcal{O}_K : (\mathbb{Z} \oplus \mathbb{Z}\sqrt{d})]^2 = 1^2 \text{ or } 2^2.$$

Thus by the lemma, either $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ or one of

$$\frac{1}{2}, \quad \frac{\sqrt{d}}{2}, \quad \frac{1+\sqrt{d}}{2}$$

is in $\mathcal{O}_K$. The first two are obvious not in $\mathcal{O}_K$, and $(1+\sqrt{d})/2 \in \mathcal{O}_K$ if and only if $d \equiv 1 \pmod 4$. Thus if $d \equiv 1 \pmod 4$, then $1, (1+\sqrt{d})/2$ is an integral basis for $\mathcal{O}_K$.

Proposition 6.1. *Let $[K : \mathbb{Q}] = n$ and $\alpha \in \mathcal{O}_K$ with minimal polynomial of degree n. Suppose further that the minimal polynomial of α is Eisenstein at p. Then $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$.*[1]

[1] Recall that $\mathbb{Z}[\alpha] = \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \cdots \oplus \mathbb{Z}\alpha^{n-1}$.

Proof. Let the minimal polynomial of α be

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

with $p|a_i$ for every i and $p^2 \nmid a_0$ (since f is Eisenstein at p). Suppose otherwise that $p|[\mathcal{O}_K : \mathbb{Z}[\alpha]]$. Then by Cauchy's theorem, there exists $\xi \in \mathcal{O}_K$ such that $[\xi] \in \mathcal{O}_K/\mathbb{Z}[\alpha]$ has order p. Then

$$p\xi = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$$

where $b_i \in \mathbb{Z}$, not all divisible by p. Let j be the smallest index such that $p \nmid b_j$. Then

$$\mathcal{O}_K \ni \eta = \xi - \left(\frac{b_0}{p} + \frac{b_1}{p}\alpha + \cdots + \frac{b_{j-1}}{p}\alpha^{j-1}\right) = \frac{b_j}{p}\alpha^j + \frac{b_{j+1}}{p}\alpha^{j+1} + \cdots + \frac{b_n}{p}\alpha^n.$$

So we have

$$\mathcal{O}_K \ni \eta\alpha^{n-j-1} = \frac{b^j}{p}\alpha^{n-1} + \frac{\alpha^n}{p}(b_{j+1} + b_{j+2}\alpha + \dots).$$

Also notice that

$$\frac{\alpha^n}{p} = -\frac{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}}{p} \in \mathcal{O}_K$$

since f was Eisenstein at p. Since $(b_{j+1} + b_{j+2}\alpha + \dots) \in \mathcal{O}_K$, we see that $b_j\alpha^{n-1}/p \in \mathcal{O}_K$ and $p \nmid b_j$. So

$$\mathbb{Z} \ni N_{\mathbb{Q}}^K\left(\frac{b_j}{p}\alpha^{n-1}\right) = \frac{b_j^n}{p^n}N(\alpha^{n-1}) = \frac{b_j^n}{p^n}a_0^{n-1}.$$

Now $p \nmid b_j$ and $p^2 \nmid a_0$ so we have at most $n-1$ factors of p in the numerator, a contradiction. □

Proposition 6.2. *For $K = \mathbb{Q}(\sqrt[3]{2})$, we have $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{2}]$.*

Proof. Let $\alpha = \sqrt[3]{2}$ and $M = \mathbb{Z}[\alpha] = \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}\alpha^2$. Let $m = |\mathcal{O}_K/M|$. Then

$$m^2\Delta(\mathcal{O}_K) = \Delta(1, \alpha, \alpha^2) = \Delta(f_\alpha),$$

where f_α is the minimal polynomial of α (check that $\Delta(1, \alpha, \alpha^2) = \Delta(f_\alpha)$). Recall that up to signs,

$$\Delta(f) = \prod_{\text{roots } \alpha_i} f(\alpha_i).$$

For a cubic polynomial $f(x) = x^3 + ax + b$, the discriminant is $\Delta f = -4a^3 - 27b^2$ (for a quadratic $f(x) = x^2 + bx + c$, it is $\Delta f = b^2 - 4c$). Thus for $f_\alpha(x) = x^3 - 2$, we have

$$m^2\Delta(\mathcal{O}_K) = \Delta(f_\alpha) = -108 = -6^2 \cdot 3.$$

Thus the index m divides 6, and since f_α is Eisenstein at 2, we have $2 \nmid m$. Now notice that

$$\mathbb{Z}[\alpha] = \mathbb{Z}[\beta], \quad \text{where } \beta = \alpha - 2.$$

The minimal polynomial of β is $g(x) = (x+2)^3 - 2 = x^3 + 6x^2 + 12x + 6$. Then g is Eisenstein at 3, so $3 \nmid m$. Thus we must have $m = 1$, which proves that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. □

Remark. Later on, we will show that if $K = \mathbb{Q}(\zeta_n)$ for some $n \geq 1$ (where ζ_n is a primitive nth root of unity), then $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$. The proof will largely involve similar types of ideas.

Remark. In general if $K = \mathbb{Q}(\theta)$ and we only work with $\mathbb{Z}[\theta]$ instead of $\mathcal{O}_K$, we may run into trouble since $\mathbb{Z}[\theta]$ may not be integrally closed (hence we may not have unique factorization of ideals).

6.2 Computing Factorizations of Ideals

Proposition 6.3. *Let $K = \mathbb{Q}(\sqrt{d})$, where d is square-free. Let p be an odd prime with $p \nmid d$. Then:*

(a) if $(\frac{d}{p}) = 1$, then $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ where $\mathfrak{p}_1 = (p, a + \sqrt{d}) \neq \mathfrak{p}_2 = (p, a - \sqrt{d})$, and $a^2 \equiv d \pmod{p}$;

(b) if $(\frac{d}{p}) = -1$, then $p\mathcal{O}_K = \mathfrak{p}$ is prime in $\mathcal{O}_K$.

In the above, $(\frac{d}{p})$ is the Legendre symbol.

Proof. (a) Note that

$$\mathfrak{p}_1\mathfrak{p}_2 = (p^2, p(a + \sqrt{d}), p(a - \sqrt{d}), a^2 - d) \subseteq (p)$$

since each of the above terms is divisible by p. But $p^2 \in \mathfrak{p}_1\mathfrak{p}_2$ and $p(a + \sqrt{a}) + p(a - \sqrt{d}) = 2ap$ so

$$(p) = (\gcd(p^2, 2ap)) \subseteq \mathfrak{p}_1\mathfrak{p}_2.$$

This gives the equality $\mathfrak{p}_1\mathfrak{p}_2 = (p)$. Now we show that $\mathfrak{p}_i$ is prime. Note that

$$N(\mathfrak{p}_1)N(\mathfrak{p}_2) = N(p) = p^2.$$

It is enough to show that $a + \sqrt{d} \notin (p)$ (this implies $\mathfrak{p}_1 \neq (p)$, so $N(\mathfrak{p}_1) = |\mathcal{O}_K/\mathfrak{p}_1| < |\mathcal{O}_K/(p)| = p^2$ and we must have $N(\mathfrak{p}_1) = p$). Now if $p|(a + \sqrt{d})$, then $p|(a - \sqrt{d})$ as well, so $p|2a$. This is a contradiction. Thus $N(\mathfrak{p}_i) = p$, which implies that $\mathfrak{p}_i$ is a prime ideal (otherwise the norm would also factor). It only remains to show that $\mathfrak{p}_1 \neq \mathfrak{p}_2$, which is left as an exercise.

(b) It is enough to show that there is no prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ such that $N(\mathfrak{p}) = p$. Equivalently, it suffices to show that if $\mathfrak{p}$ is a prime ideal, then $\mathcal{O}_K/\mathfrak{p} \ncong \mathbb{Z}/p\mathbb{Z}$. Note that $x^2 - d$ has a root in $\mathcal{O}_K$ and thus in $\mathcal{O}_K/\mathfrak{p}$, so $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{Z}/p\mathbb{Z}$ would imply that d is a square modulo p, contradicting $(\frac{d}{p}) = -1$. □

Exercise 6.1. Show that if $p|d$, then $p\mathcal{O}_K = \mathfrak{p}^2$ for some prime ideal $\mathfrak{p}$.

Theorem 6.1 (Kummer)**.** *Let $K = \mathbb{Q}(\theta)$ with $\theta \in \mathcal{O}_K$. Suppose p is a prime such that $p \nmid [\mathcal{O}_K : \mathbb{Z}[\theta]]$. Let g be the minimal polynomial of θ. Factor $g \bmod p$ as*

$$g(x) \equiv g_1(x)^{e_1} \dots g_r(x)^{e_r} \pmod{p},$$

where $g_i(x) \in \mathbb{Z}[x]$, $\overline{g_i(x)}$ is irreducible over $\mathbb{F}_p$, and the $\overline{g_i}$ are pairwise distinct.[2] *Then*

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r},$$

where $\mathfrak{p}_i = (p, g_i(\theta))$ is a prime ideal, $N(\mathfrak{p}_i) = p^{f_i}$ where $f_i = \deg g_i$, and the $\mathfrak{p}_i$ are distinct.

Remark. Note that this generalizes the quadratic case: $x^2 - d \bmod p$ factors if and only if d is a square modulo p, and the ideals are $(p, g_i(\theta))$ for $g_1 = x - a$ and $g_2 = x + a$.

[2]Here $\overline{g(x)}$ denotes the reduction of $g(x)$ modulo p.

Lecture 7

Jan. 28 — Kummer's Theorem

7.1 Kummer's Theorem

Lemma 7.1. *Let $\theta \in \mathcal{O}_K$ and assume $p \nmid [\mathcal{O}_K : \mathbb{Z}[\theta]]$. Then*

$$\mathcal{O}_K/p\mathcal{O}_K \cong \mathbb{Z}[\theta]/p\mathbb{Z}[\theta].$$

Proof. Consider the map $\psi : \mathbb{Z}[\theta] \hookrightarrow \mathcal{O}_K \twoheadrightarrow \mathcal{O}_K/p\mathcal{O}_K$. Note that we have $p\mathbb{Z}[\theta] \subseteq \ker\psi$, so ψ induces a map $\overline{\psi} : \mathbb{Z}[\theta]/p\mathbb{Z}[\theta] \to \mathcal{O}_K/p\mathcal{O}_K$ on the quotient. We will show that $\overline{\psi}$ is an isomorphism, by checking:

1. $\ker\psi = p\mathbb{Z}[\theta]$.

   Let $\alpha \in \ker\psi$. Then $\alpha \in \mathbb{Z}[\theta] \cap p\mathcal{O}_K$, so $\alpha = p\beta$ for some $\beta \in \mathcal{O}_K$. Then $\overline{\beta} \in \mathcal{O}_K/\mathbb{Z}[\theta]$ has order dividing p since $p\overline{\beta} = \overline{\alpha} = 0$. Therefore $\overline{\beta} = 0$, so $\beta \in \mathbb{Z}[\theta]$. This gives $\alpha \in p\mathbb{Z}[\theta]$, so $\ker\psi = p\mathbb{Z}[\theta]$.

2. ψ is surjective.

   Note that if $(|G|, p) = 1$ where G is a finite abelian group, then $[p] : G \to G$ is injective and hence bijective. So let $\gamma \in \mathcal{O}_K$, so that $\overline{\gamma} \in \mathcal{O}_K/\mathbb{Z}[\theta]$ is a multiple of p, i.e. $\overline{\gamma} = p\overline{\gamma'}$ for some $\gamma' \in \mathcal{O}_K$. Then $\gamma - p\gamma' \in \mathbb{Z}[\theta]$, so $\psi(\gamma - p\gamma') = \gamma$. Since $\gamma - p\gamma' \in \mathbb{Z}[\theta]$, this shows that ψ is surjective.

Thus $\overline{\psi}$ is bijective, so it is an isomorphism $\mathbb{Z}[\theta]/p\mathbb{Z}[\theta] \to \mathcal{O}_K/p\mathcal{O}_K$. □

Theorem 7.1 (Kummer)**.** *Let $K = \mathbb{Q}(\theta)$ and p be a prime. Assume that $p \nmid [\mathcal{O}_K : \mathbb{Z}[\theta]]$, and let $g(x)$ be the minimal polynomial of θ. Write (let $\overline{g}$ denote the reduction of g modulo p)*

$$\overline{g} = \prod_{i=1}^{r} (\overline{g_i})^{e_i},$$

where $g_i(x) \in \mathbb{Z}[x]$ and $\overline{g_i} \in \mathbb{F}_p[x]$ is irreducible and monic, with $g_1, \ldots, g_r$ distinct. Then

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_r^{e_r},$$

where $N(\mathfrak{p}_i) = p^{f_i}$ for $f_i = \deg g_i$, and $\mathfrak{p}_i = (p, g_i(\theta))$ are distinct prime ideals.

Proof. Let $\mathfrak{p}_i = (p, g_i(\theta))$ as in the statement. Then

$$\mathcal{O}_K/\mathfrak{p}_i = \mathcal{O}_K/(p, g_i(\theta)) \cong \mathbb{Z}[\theta]/(p, g_i(\theta)) \cong \mathbb{Z}[x]/(p, g_i(x))$$

The first isomorphism follows from the lemma, which holds only when $p \nmid [\mathcal{O}_K : \mathbb{Z}[\theta]]$. Note that

$$\mathbb{F}_p[\theta]/(\overline{g_i}(\theta)) \cong \mathbb{Z}[\theta]/(p, g_i(\theta)) \cong \mathbb{Z}[x]/(p, g_i(x)) \cong \mathbb{F}_p[x]/(\overline{g_i}(x)).$$

Since $\overline{g_i}$ is irreducible of degree f_i, the quotient is a field of size p^{f_i}. This proves that $N(\mathfrak{p}_i) = p^{f_i}$ and also that $\mathfrak{p}_i$ is a maximal ideal (so in particular, a prime ideal). Now if $n = [K : \mathbb{Q}]$, then

$$\sum_{i=1}^{r} e_i f_i = \deg \overline{g} = n.$$

Check as an exercise that the $\mathfrak{p}_i$ are distinct (use the fact that $\overline{g_i}$ and $\overline{g_j}$ are relatively prime, so that $(\overline{g_i}, \overline{g_j}) = 1$ in $\mathbb{F}_p[x]$). Now we will show that $p\mathcal{O}_K \cong \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$. First observe that

$$\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r} = (p, g_1(\theta))^{e_1} \dots (p, g_r(\theta))^{e_r} \subseteq (p, g_1(\theta)^{e_1} \dots g_r(\theta)^{e_r}) = (p).$$

(Check the above inclusion as an exercise. Note that for $\overline{g}(x) = \overline{g_1}(x)\overline{g_2}(x)$, we can find h such that $g_1 + g_2 = 1 + ph$, so that $(p, g_1(\theta))(p, g_2(\theta)) = (p^2, pg_1(\theta), pg_2(\theta), g_1(\theta)g_2(\theta)) = (p)$ as $p(1 + ph) = p + p^2h$ and $g(\theta) = 0$). Thus $p\mathcal{O}_K | \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$, which implies that

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1'} \dots \mathfrak{p}_r^{e_r'}$$

with $0 \le e_i' \le e_i$. But $n = \sum e_i' f_i = \sum e_i f_i$, so $e_i' = e_i$ for all i, which completes the proof. □

7.2 Ramification

Definition 7.1. Let $\mathfrak{p}_i, e_i, f_i, r$ be defined as in the statement of the previous theorem. We say that the $\mathfrak{p}_i$ are prime ideals *lying over* p, and e_i is called the *ramification index* of $\mathfrak{p}_i$ over p.

If $e_i = 1$, then we say that $\mathfrak{p}_i$ is *unramified* over p. Otherwise if $e_i > 1$, we say that p is *ramified*. Finally if $e_i = n$, then we say that $\mathfrak{p}$ is *totally ramified*, i.e. $p\mathcal{O}_K = \mathfrak{p}^n$.

If $p\mathcal{O}_K$ is prime, then we say that p is *inert*. If $r = n$, i.e. if $p\mathcal{O}_K = \mathfrak{p}_1 \dots \mathfrak{p}_n$ for distinct $\mathfrak{p}_i$, then we say that p *splits completely* in $\mathcal{O}_K$ (or in K). The f_i is called the *residue degree*.

Corollary 7.1.1. *If the minimal polynomial of $\theta \in \mathcal{O}_K$ is Eisenstein at p and $K = \mathbb{Q}(\theta)$, then p is totally ramified in $\mathcal{O}_K$.*

Proof. We have previously shown that $p \nmid [\mathcal{O}_K : \mathbb{Z}[\theta]]$, so Kummer's theorem applies. Let $g(x)$ be the minimal polynomial of θ. Then $\overline{g(x)} = x^n$ in $\mathbb{F}_p[x]$ since $g(x)$ is Eisenstein at p. Thus by Kummer's theorem, we have $p\mathcal{O}_K = \mathfrak{p}^n$ where $\mathfrak{p} = (p, \theta)$, i.e. p is totally ramified. □

Corollary 7.1.2. *Only finitely many primes ramify in any number field $K/\mathbb{Q}$. More specifically, if $p \nmid [\mathcal{O}_K : \mathbb{Z}[\theta]]$ for some $\theta \in \mathcal{O}_K$, then p ramifies in K if and only if $p | \Delta_K$.*

Proof. Note that p ramifies in $\mathcal{O}_K$ if and only if $\overline{g}$ has a multiple root in $\mathbb{F}_p[x]$, if and only if $\Delta(\overline{g}) = 0$ in $\mathbb{F}_p[x]$. Now recall that we have

$$\Delta_K = \frac{\Delta_{\mathbb{Z}[\theta]}}{[\mathcal{O}_K : \mathbb{Z}[\theta]]^2},$$

so $p | \Delta_K$ if and only if $p | \Delta_{\mathbb{Z}[\theta]}$ (since $p \nmid [\mathcal{O}_K : \mathbb{Z}[\theta]]$ by hypothesis). So we look at $\Delta_{\mathbb{Z}[\theta]}$ instead. Taking g to be the minimal polynomial of θ, this happens if and only if $p | \Delta(g) \equiv \Delta_K$. □

Remark. The above corollary holds in greater generality (without the hypothesis that $p \nmid [\mathcal{O}_K : \mathbb{Z}[\theta]]$), but the proof requires some more advanced tools.

7.3 More Computing of Rings of Integers

Remark. Recall that $\mathcal{O}_{\mathbb{Q}(\sqrt[3]{2})} = \mathbb{Z}[\sqrt[3]{2}]$. We will now generalize this result.

Theorem 7.2. *Let p be a prime and $a \neq 0, \pm 1$ be a square-free integer such that $(p, a) = 1$. Let $\theta = \sqrt[p]{a}$. Letting $K = \mathbb{Q}(\theta) = \mathbb{Q}[x]/(x^p - a)$, we have $\mathcal{O}_K = \mathbb{Z}[\theta]$ if and only if $a^{p-1} \not\equiv 1 \pmod{p^2}$.*

Proof. ($\Leftarrow$) Let $K = \mathbb{Q}(\theta)$ and assume that $a^p \not\equiv a \pmod{p^2}$. The discriminant of $x^p - a$ is

$$\Delta(\theta) = \pm p^p a^{p-1} = \Delta_K \cdot [\mathcal{O}_K : \mathbb{Z}[\theta]]^2.$$

Note that $x^p - a$ is Eisenstein at every prime dividing a. Now observe that

$$(x + a)^p - a$$

is Eisenstein at p (since $p^2 \nmid (a^p - a)$ by hypothesis), and $\mathbb{Z}[\theta] = \mathbb{Z}[\theta - a]$, so $p \nmid [\mathcal{O}_K : \mathbb{Z}[\theta]]$.

($\Rightarrow$) Suppose that $\mathcal{O}_K \neq \mathbb{Z}[\theta]$. Kummer's theorem implies that $p\mathcal{O}_K = \mathfrak{p}^p$ where $\mathfrak{p} = (p, \theta - a)$. Note that

$$x^p - a \equiv (x - a)^p \pmod{p}$$

by Fermat's little theorem, and that $N(\mathfrak{p}) = p$. Now $\theta - a \in \mathfrak{p}$ (and $\theta - a \notin \mathfrak{p}^2$), so

$$p \in \mathfrak{p}^2 = (p^2, p(\theta - a), (\theta - a)^2)$$

since $\mathfrak{p}^2 | (p) = \mathfrak{p}^p$ and $p \geq 2$, so $(p) \subseteq \mathfrak{p}^2$. Thus we have $(\theta - a) = \mathfrak{p}\mathfrak{a}$ for some ideal $\mathfrak{a}$ which is relatively prime to $\mathfrak{p}$. Now $(p, N(\mathfrak{a})) = 1$ since $N(\mathfrak{a}) = \prod q_i^{e_i f_i}$ where $\mathfrak{a} = \mathfrak{q}_1^{e_1} \dots \mathfrak{q}_r^{e_r}$ for $\mathfrak{q}_i \neq \mathfrak{p}$, so $q_i \neq p$. Then

$$a^p - a = |N(\theta - a)| = N(\mathfrak{p}\mathfrak{a}) = pN(\mathfrak{a})$$

where $N(\mathfrak{a})$ is relative prime to p, so p^2 does not divide $a^p - a$. □

Remark. Next class, we will show that $\mathbb{Q}(\sqrt{-5})$ has class number 2, which we will use to solve the Diophantine equation $y^2 = x^3 - 5$ in $\mathbb{Z}$ via arithemtic in $\mathbb{Z}[\sqrt{-5}]$, by writing

$$x^3 = y^2 + 5 = (y + \sqrt{-5})(y - \sqrt{-5}).$$

We will fix our previous issue by arguing that if a product of ideals is a cube, then each ideal is a cube when the class number is not a multiple of 3. This is similar to Kummer's work on Fermat's last theorem.

Lecture 8

Jan. 30 — Computing Ideal Class Groups and Applications

8.1 Computing Ideal Class Groups

Example 8.0.1. Let $K = \mathbb{Q}(\sqrt{2})$. We know that $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$. Recall that every ideal class in $\mathrm{Cl}(\mathcal{O}_K)$ contains an ideal of norm $\leq M$, where (if $\mathcal{O}_K = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$ as $\mathbb{Z}$-modules)

$$M = \prod_{i=1}^{n} \sum_{j=1}^{n} |\sigma_i(\alpha_j)|.$$

Thus in this case, we have $M = (1+\sqrt{2})^2 \approx 5.8 < 6$. Thus every ideal class contains an ideal of norm ≤ 5. We will want to factor the ideals $(2), (3), (5)$ in $\mathcal{O}_K$ via Kummer's theorem. We need to factor

$$x^2 - 2 \pmod{p}, \quad p = 2, 3, 5.$$

Mod 2, we have $x^2 - 2 \equiv x^2 \pmod{2}$, so $(2) = \mathfrak{p}_2^2$. Now $x^2 - 2$ is irreducible mod both 3 and 5 since 2 is not a quadratic residue mod 3 or 5. Thus $(3) = \mathfrak{p}_3$ and $(5) = \mathfrak{p}_5$ with $f_3 = f_5 = 2$. Thus

$$N(\mathfrak{p}_2) = 2, \quad N(\mathfrak{p}_3) = 9, \quad N(\mathfrak{p}_5) = 25.$$

So any nonzero ideal in $\mathcal{O}_K$ is equivalent to $\mathfrak{p}_2$ or (1) (since $\mathfrak{p}_2^2 = (2)$ is principal). Thus

$$\mathrm{Cl}(\mathcal{O}_K) = \{(1), [\mathfrak{p}_2]\},$$

which is isomorphic to either $\{1\}$ if $\mathfrak{p}_2$ is principal or $\mathbb{Z}/2\mathbb{Z}$ if $\mathfrak{p}_2$ is not principal. But $\mathfrak{p}_2 = (\sqrt{2})$, so

$$\mathrm{Cl}(\mathbb{Z}[\sqrt{2}]) = \{1\}.$$

This also implies that $\mathbb{Z}[\sqrt{2}]$ is a PID, and hence a UFD.

Example 8.0.2. Let $K = \mathbb{Q}(\sqrt{-5})$, where we have seen that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. By a similar reasoning as above, we have $M = (1+\sqrt{5})^2 < 11$. So we want to find all nonzero prime ideals of norm ≤ 10. We consider $x^2 + 5 \pmod{p}$ for $p = 2, 3, 5, 7$, where we can factor

$$\begin{aligned}
&p = 2 : x^2 + 5 \equiv x^2 + 1 \equiv (x+1)^2 \pmod{2},\\
&p = 3 : x^2 + 5 \equiv x^2 - 1 \equiv (x-1)(x+1) \pmod{3},\\
&p = 5 : x^2 + 5 \equiv x^2 \pmod{5},\\
&p = 7 : x^2 + 5 \equiv (x+3)(x+4) \pmod{7}.
\end{aligned}$$

Thus we have $(2) = \mathfrak{p}_2^2$, $(3) = \mathfrak{p}_3\mathfrak{p}_3'$, $(5) = \mathfrak{p}_5^2 = (\sqrt{-5})^2 = (\sqrt{-5})$, and $(7) = \mathfrak{p}_7\mathfrak{p}_7'$. Since (5) is principal, we only need to consider $(2), (3), (7)$, which each have norm ≤ 10. Thus

$$\mathrm{Cl}(\mathcal{O}_K) = \langle [\mathfrak{p}_2], [\mathfrak{p}_3], [\mathfrak{p}_7] \rangle,$$

where we note that $\mathfrak{p}_3'$ and $\mathfrak{p}_7'$ are inverses to $\mathfrak{p}_3$ and $\mathfrak{p}_7$, respectively, since their product is principal, so we do not need to include them as generators. Note that $\mathcal{O}_K^\times = \{\pm 1\}$, so we do not need to worry much about units. If any of the $\mathfrak{p}_p$ is principal, then it is generated by an element $\alpha = a + b\sqrt{-5}$ with

$$p = N(\alpha) = a^2 + 5b^2.$$

This cannot happen for $p = 2, 3, 7$, so $\mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_7$ are not principal. Now $N(1 + \sqrt{-5}) = 6$, so

$$(1 + \sqrt{-5}) = \mathfrak{p}_2\mathfrak{p}_3 \text{ or } \mathfrak{p}_2\mathfrak{p}_3'.$$

This means that one of $\mathfrak{p}_3$ or $\mathfrak{p}_3'$ is an inverse to $\mathfrak{p}_2$ in $\mathrm{Cl}(\mathcal{O}_K)$, so in fact

$$\mathrm{Cl}(\mathcal{O}_K) = \langle [\mathfrak{p}_2], [\mathfrak{p}_7] \rangle.$$

Also note that $[\mathfrak{p}_2]^2 = 1$ since $\mathfrak{p}_2^2 = (2)$ is principal. We can also see that $N(3 + \sqrt{-5}) = 14$, so

$$(3 + \sqrt{-5}) = \mathfrak{p}_2\mathfrak{p}_7 \text{ or } \mathfrak{p}_2\mathfrak{p}_7'.$$

Thus we also do not need $\mathfrak{p}_7$ as a generator, so $\mathrm{Cl}(\mathcal{O}_K) = \langle [\mathfrak{p}_2] \rangle$. Since $[\mathfrak{p}_2]^2 = 1$ and $\mathfrak{p}_2$ is not principal,

$$\mathrm{Cl}(\mathbb{Z}[\sqrt{-5}]) = \mathbb{Z}/2\mathbb{Z}.$$

8.2 Applications of Class Group Computations

Theorem 8.1. *The Diophantine equation $y^2 = x^3 - 5$ has no integer solutions.*

Proof. Assume that we have a solution x, y to the above equation. Writing $x^3 = y^2 + 5$, we can factor

$$x^3 = (y + \sqrt{-5})(y - \sqrt{-5}).$$

in $\mathbb{Z}[\sqrt{-5}]$. By looking at the equation mod 4, we see that x must be odd. Also, $(x, y) = 1$ since otherwise $(x, y) = 5$ and one can derive a contradiction with the equation $y^2 = x^3 - 5$.

Now we claim that $(y + \sqrt{-5})$ and $(y - \sqrt{-5})$ are coprime (equivalent to comaximal in a Dedekind domain) ideals. To see this, suppose otherwise that $\mathfrak{p}$ divides both. Then $\mathfrak{p}|(x^3) = (x)^3$, so we must have $\mathfrak{p}|(x)$ by unique factorization. Also, $\mathfrak{p}|(2y)$. But $\mathfrak{p}|(x)$ means that $N(\mathfrak{p})$ is odd, so $\mathfrak{p} \nmid (2)$. Thus $\mathfrak{p}|(y)$. Then $(x, y) = 1$ implies that $\mathfrak{p}|(1)$, a contradiction. Thus $(y + \sqrt{-5})$ and $(y - \sqrt{-5})$ are coprime.

Thus we may write

$$(x)^3 = (y + \sqrt{-5})(y - \sqrt{-5}).$$

Since the above ideals are relatively prime, unique factorization implies that each of $(y \pm \sqrt{-5})$ is the cube of some ideal. Write $(y + \sqrt{-5}) = \mathfrak{a}^3$ for some ideal $\mathfrak{a}$. Then $[\mathfrak{a}]^3 = 1$ in $\mathrm{Cl}(\mathbb{Z}[\sqrt{-5}])$, so $\mathrm{Cl}(\mathbb{Z}[\sqrt{-5}]) = \mathbb{Z}/2\mathbb{Z}$ implies that $[\mathfrak{a}] = 1$. Thus $\mathfrak{a} = (\alpha)$ for some $\alpha = a + b\sqrt{-5}$, so

$$(a + b\sqrt{-5})^3 = \alpha^3 = \pm(y + \sqrt{-5})$$

as elements. Finish the proof and derive a contradiction from here as an exercise. □

8.3 Cyclotomic Fields

Theorem 8.2. *Let $m = p^k$ for $k \geq 1$. Then the ring of integers of $\mathbb{Q}(\zeta_m)$ is $\mathbb{Z}[\zeta_m]$.*

Remark. Recall that the minimal polynomial for ζ_m over $\mathbb{Q}$ is

$$\Phi_m(x) = \frac{x^{p^k} - 1}{x^{p^{k-1}} - 1} = x^{(p-1)p^{k-1}} + x^{(p-2)p^{k-1}} + \cdots + x^{p^{k-1}} + 1.$$

This polynomial is irreducible over $\mathbb{Z}$ (e.g. $\Phi_m(x+1)$ is Eisenstein at p), with

$$\deg \Phi_m(x) = \phi(m) = (p-1)p^{k-1}.$$

Note that $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ is Galois with Galois group isomorphic to $(\mathbb{Z}/m\mathbb{Z})^\times$.

Lemma 8.1. *For any $m \geq 1$, the discriminant $\Delta(\zeta_m) = \operatorname{disc}(\Phi_m) = \Delta(1, \zeta_m, \zeta_m^2, \dots)$ divides $m^{\phi(m)}$.*

Proof. Since $\Phi_m | (x^m - 1)$, we can write $x^m - 1 = \Phi_m(x)g(x)$ for a polynomial g. Taking a derivative,

$$mx^{m-1} = \Phi_m'(x)g(x) + \Phi_m(x)g'(x).$$

Plugging in $x = \zeta_m^j$ for $(j, m) = 1$ (these are the conjugates of ζ_m),

$$m\zeta_m^{j(m-1)} = \Phi_m'(\zeta_m^j)g(\zeta_m^j)$$

since $\Phi_m(\zeta_m^j) = 0$. Taking the norm in $\mathbb{Q}(\zeta_m)/\mathbb{Q}$, we have

$$m^{\phi(m)} = N(m\zeta_m^{m-1}) = N(\Phi_m'(\zeta_m^j))N(g(\zeta_m^j)) = \pm\Delta(\zeta_m)N(g(\zeta_m^j)),$$

where $N(g(\zeta_m^j)) \in \mathbb{Z}$ since an integer polynomial evaluated at an algebraic integer is an algebraic integer, and the norm of an algebraic integer is an integer. Also, $g(\zeta_m^j) \neq 0$, so $\Delta(\zeta_m) | m^{\phi(m)}$. □

Proof of Theorem 8.2. Since $\Phi_m(x+1)$ is Eisenstein at p, we have $p \nmid [\mathcal{O}_{\mathbb{Q}(\zeta_m)} : \mathbb{Z}[\zeta_m]]$. But

$$\Delta(\zeta_m) = \Delta(\mathbb{Q}(\zeta_m)) \cdot [\mathcal{O}_{\mathbb{Q}(\zeta_m)} : \mathbb{Z}[\zeta_m]]^2$$

and $\Delta(\zeta_m)$ is a power of p by the lemma, so $[\mathcal{O}_{\mathbb{Q}(\zeta_m)} : \mathbb{Z}[\zeta_m]]$ is a power of p. So $[\mathcal{O}_{\mathbb{Q}(\zeta_m)} : \mathbb{Z}[\zeta_m]] = 1$. □

Remark. Using field/Galois theory, we will show that $\mathcal{O}_{\mathbb{Q}(\zeta_m)} = \mathbb{Z}[\zeta_m]$ for all $m \geq 1$ next time.

8.4 First Case of Fermat's Last Theorem

Remark. Our current goal is: If p is an odd prime and $u \in \mathbb{Z}[\zeta_p]^\times$, then $u/\overline{u} = \zeta_p^k$ for some $k \in \mathbb{Z}$.

Lemma 8.2. *If m is a positive integer, then the roots of unity in $\mathbb{Q}(\zeta_m)$ are*

$$\begin{cases} \text{primitive } m\text{th roots of } 1 & \text{if } m \text{ is even,} \\ \text{primitive } (2m)\text{-th roots of } 1 & \text{if } m \text{ is odd.} \end{cases}$$

Proof. If m is odd, then $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{2m})$. So assume without loss of generality that m is even. Suppose $\zeta \in \mathbb{Q}(\zeta_m)$ and $\zeta^k = 1$ for some k. We want to show that $k | m$. Assume without loss of generality that $\zeta = e^{2\pi i/k}$. Since $\zeta_k, \zeta_m \in \mathbb{Q}(\zeta_m)$, one can check as an exercise that $\zeta_r \in \mathbb{Q}(\zeta_m)$ where $r = \operatorname{lcm}(k, m)$. Then $\mathbb{Q}(\zeta_r) \subseteq \mathbb{Q}(\zeta_m)$, so taking degrees implies that $\phi(r) \leq \phi(m)$. Also $m | r$, which one can check implies that $\phi(m) \leq \phi(r)$. This means that $\phi(m) = \phi(r)$, so $m = r$ and thus $k | m$. □

Lecture 9

Feb. 4 — Fermat's Last Theorem

9.1 First Case of Fermat's Last Theorem, Continued

Theorem 9.1 (Kronecker)**.** *If $\alpha \in \mathbb{C}$ is a nonzero algebraic integer, all of whose complex conjugates have absolute value* 1*, then α is a root of unity.*

Proof. Let $f(x) \in \mathbb{Z}[x]$ be the minimal polynomial of α (since α is an algebraic integer, f is monic):

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_0.$$

Then there exists $C > 0$ such that $|a_i| \leq C$ for all i, where C depends only on n (this is because each $|a_i| = |\sigma_i(\alpha_1, \ldots, \alpha_n)| \leq 2^n = C$ by the triangle inequality, where σ_i is the ith elementary symmetric polynomial). Since the a_i are integers, there are only finitely possible choices for f. Then since each f only has finitely many roots, there are only finitely many possible choices for α.

The same argument applies to $\alpha, \alpha^2, \alpha^3, \ldots$, so we see that $\{\alpha, \alpha^2, \alpha^3, \ldots\}$ is a finite set. Thus there exist $i < j$ such that $\alpha^i = \alpha^j$, which implies that $\alpha^{j-i} = 1$, i.e. α is a root of unity. □

Remark. The algebraic integer assumption is necessary, e.g. consider $(3/5) + (4/5)i$.

Lemma 9.1. *If $\alpha \in \mathbb{Z}[\zeta_p]$, then $\alpha^p \equiv a \pmod{p}$ for some $a \in \mathbb{Z}$.*

Proof. Let $\zeta = \zeta_p$ and write

$$\alpha = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}$$

with $a_i \in \mathbb{Z}$. By the binomial theorem, we have (all the cross-terms are divisible by p)

$$\alpha^p \equiv a_0^p + (a_1\zeta)^p + \cdots + (a_{p-2}\zeta^{p-2})^p \equiv a_0 + a_1 + \cdots + a_{p-2} \pmod{p},$$

where the second step is by $\zeta^p = 1$ and Fermat's little theorem. So we can take $a = a_0 + \cdots + a_{p-2}$. □

Theorem 9.2 (Kummer)**.** *Let p be an odd prime. If $u \in \mathbb{Z}[\zeta_p]$ is a unit, then $u/\overline{u} = \zeta_p^k$ for some $k \in \mathbb{Z}$.*

Proof. Let $\alpha = u/\overline{u} \in \mathbb{Z}[\zeta_p] \subseteq \mathbb{C}$. Then all conjugates of α have absolute value 1 (the key point is that $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is abelian, so complex conjugation commutes with taking the other conjugates). So α is a root of unity, which implies that $\alpha = \pm\zeta_p^k$ for some k. All that remains is to show that the sign is $+$.

Suppose for sake of contradiction that $u/\overline{u} = -\zeta_p^k$. Then raising both sides to the kth power, we find that $u^p = -\overline{u}^p$. By the lemma, there is $a \in \mathbb{Z}$ such that $u^p \equiv a \equiv \overline{u}^p \pmod{p}$ (the second congruence comes from taking complex conjugates of both sides). This implies that $2u^p \equiv 0 \pmod{p}$, so we get $p | u^p$ since p is an odd prime. This is a contradiction as u^p is a unit. □

Definition 9.1. A prime p is *regular* if $p \nmid |\mathrm{Cl}(\mathbb{Z}[\zeta_p])|$, and p is *irregular* otherwise.

Remark. Kummer realized that class numbers are related to certain congruences of Bernoulli numbers, which gives a better criterion for a prime to be regular.

Remark. It is known that there are infinitely many irregular primes, with the smallest being $p = 37$. Thus the below theorem, due to Kummer, works for all primes $p \leq 31$.

Theorem 9.3 (Fermat's last theorem for regular primes, first case)**.** *Let $p \geq 5$ be a regular prime and $p \nmid xyz$. Then the equation $x^p + y^p = z^p$ has no solutions for non-zero integers x, y, z.*

Proof. Let $\zeta = \zeta_p$ and write (the following equality is on the level of ideals)

$$(x + y)(x + \zeta y) \dots (x + y\zeta^{p-1}) = (z)^p. \tag{$*$}$$

Check as an exercise that the ideals on the left-hand side are pairwise relatively prime. Due to unique factorization of ideals into prime ideals, we must have $(x + y\zeta) = I^p$ for some ideal I. Now I must be principal since p is regular (since $(x + y\zeta)$ is principal but p does not divide the class number). So

$$x + y\zeta = u \cdot \alpha^p \quad \text{for some } \alpha \in \mathbb{Z}[\zeta].$$

We claim that $x \equiv y \pmod{p}$ $(**)$. Assuming $(**)$ for now, we have $x \equiv -z \pmod{p}$ as well (we can use symmetry to apply the same argument to the equation $x^p + (-z)^p = (-y)^p$, since p is odd), so

$$2x^p \equiv x^p + u^p \equiv z^p \equiv -x^p \pmod{p}.$$

This implies that $p|3x^p$, which is a contradiction since $p \geq 5$ and $p \nmid x$.

Now we prove $(**)$ via the result about $u/\overline{u} = \zeta^p$. We have $\alpha^p \equiv a \pmod{p}$ for some $a \in \mathbb{Z}$, so

$$x + y\zeta \equiv ua \pmod{p}.$$

Then $\overline{\zeta}_p = \zeta_p^{-1}$ implies that

$$x + y\zeta^{-1} = \overline{x + y\zeta} \equiv \overline{u}a \pmod{p}.$$

So $(x + y\zeta)\overline{u} \equiv (x + y\zeta^{-1})u \pmod{p}$, which implies

$$x + y\zeta \equiv (x + y\zeta^{-1})\frac{u}{\overline{u}} \pmod{p}.$$

Thus $x + y\zeta \equiv x\zeta^k + y\zeta^{k-1} \pmod{p}$ for some $0 \leq k \leq p - 1$ (use $u/\overline{u} = \zeta^k$). Show as an exercise that this is only possible if $k = 1$ (note that the powers of ζ form an integral basis, so a representation in powers of ζ must be unique). This then implies that $x \equiv y \pmod{p}$, which completes the proof. □

9.2 More on Cyclotomic Fields

Definition 9.2. If $K \subseteq K_1, K_2 \subseteq L$, then the *compositum* of K_1 and K_2 is the smallest subfield of L containing both K_1 and K_2.

Remark. If everything is Galois in the above definition, $K = K_1 \cap K_2$, and K_1, K_2 are *linearly disjoint*, i.e. that we have $[K_1K_2 : K] = [K_1 : K][K_2 : K]$, then one obtains the result

$$\mathrm{Gal}(K_1K_2/K_2) \cong \mathrm{Gal}(K_1/K).$$

Proposition 9.1. *Let K, K' be number fields of degree n, n', respectively. Assume that*

1. *K, K' are both Galois over $\mathbb{Q}$,*
2. *$K \cap K' = \mathbb{Q}$,*
3. *and $(|\Delta_K|, |\Delta_{K'}|) = 1$.*

Then if $\alpha_1, \dots, \alpha_n$ is an integral basis for $\mathcal{O}_K$ and $\alpha'_1, \dots, \alpha'_{n'}$ is an integral basis for $\mathcal{O}_{K'}$, then $\{\alpha_i \alpha_{j'}\}$ is an integral basis for $\mathcal{O}_{KK'}$.

Proof. Let $\alpha \in \mathcal{O}_{KK'}$. Field theory shows that $\{\alpha_i \alpha_{j'}\}$ is a basis for KK' over $\mathbb{Q}$, so we can write

$$\alpha = \sum_{i,j} a_{ij} \alpha_i \alpha'_j, \quad a_{ij} \in \mathbb{Q}.$$

We need to show that $a_{ij} \in \mathbb{Z}$. Let $d = |\Delta_K|, d' = |\Delta_{K'}|$. We will show that $da_{ij} \in \mathbb{Z}$ and $d' a_{ij} \in \mathbb{Z}$, which will imply that $a_{ij} \in \mathbb{Z}$ since $(d, d') = 1$. Let

$$\beta_j = \sum_i a_{ij} \alpha'_i, \quad j = 1, \dots, n.$$

Let T be the $n \times n$ matrix with $T_{\ell j} = \sigma_\ell(\alpha_j)$, where $\sigma_1, \dots, \sigma_n$ are the embeddings of KK' over K', i.e. the elements of $\mathrm{Gal}(KK'/K')$ since K, K' are Galois over $\mathbb{Q}$. Let

$$a = \begin{bmatrix} \sigma_1(\alpha) \\ \vdots \\ \sigma_n(\alpha) \end{bmatrix} \quad \text{and} \quad b = \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix}.$$

Check as an exercise that $a = Tb$. Multiplying this equation by $\operatorname{adj} T$, we find that

$$(\operatorname{adj} T) a = (\det T) b.$$

Now all the entries of T, $\operatorname{adj} T$, and a are algebraic integers, so multiplying the above equation by $\det T$ implies that the entries of db are algebraic integers. Thus $d\beta_j \in \mathcal{O}_{K'}$ for all j. But the $\{\alpha'_i\}$ were an integral basis for $\mathcal{O}_K$ over $\mathbb{Z}$ by assumption, so in fact $da_{i,j} \in \mathbb{Z}$ for all i, j, completing the proof. □

Remark. Let $K_m = \mathbb{Q}(\zeta_m)$. If $(m, m') = 1$, then $(|\Delta_{K_m}|, |\Delta_{K_{m'}}|) = 1$. Additionally, some field theory shows that if $(m, m') = 1$, then $K_m \cap K_{m'} = \mathbb{Q}$ and $K_m K_{m'} = K_{mm'}$ in $\mathbb{C}$.

Using this proposition, along with the previous case that $\mathcal{O}_{\mathbb{Q}(\zeta_m)} = \mathbb{Z}[\zeta_m]$ for $m = p^k$ and the Chinese remainder theorem, one can show that $\mathcal{O}_{\mathbb{Q}(\zeta_m)} = \mathbb{Z}[\zeta_m]$ for any $m \geq 1$.

Corollary 9.3.1. *For all $m \geq 1$, we have $\mathcal{O}_{\mathbb{Q}(\zeta_m)} = \mathbb{Z}[\zeta_m]$.*

9.3 Motivation for Geometry of Numbers

Remark. We will discuss Minkowski's geometry of numbers next. The goals of this are the following:

1. Improve the constant M from the class number computations.
2. Prove the "four squares" theorem, i.e. that every $n \geq 1$ is the sum of 4 integer squares.

Lecture 10

Feb. 6 — Geometry of Numbers

10.1 Complete Lattices and Covolume

Remark. Let K be a number field with $[K:\mathbb{Q}] = n$. Recall that $\mathcal{O}_K \cong \mathbb{Z}^n$ as $\mathbb{Z}$-modules, but we will use a different method. Let $\sigma_1, \dots, \sigma_n : K \hookrightarrow \mathbb{C}$ be the n embeddings of K into $\mathbb{C}$. Call an embedding σ *real* if $\sigma(K) \subset \mathbb{R}$, and *complex* otherwise. Note that if $\sigma : K \hookrightarrow \mathbb{C}$ is complex, then $\overline{\sigma} : K \hookrightarrow \mathbb{C}$ satisfies

$$\operatorname{Re}(\sigma) = \operatorname{Re}(\overline{\sigma}) \quad \text{and} \quad \operatorname{Im}(\sigma) = -\operatorname{Im}(\overline{\sigma}),$$

so $\sigma, \overline{\sigma}$ are kind of dependent. This indicates that we should consider pairs of complex embeddings instead. Suppose we have r_1 real embeddings $\sigma_1, \dots, \sigma_{r_1} : K \hookrightarrow \mathbb{R}$ and r_2 pairs of complex embeddings $\tau_1, \dots, \tau_{r_2} : K \hookrightarrow \mathbb{C}$, so that $r_1 + 2r_2 = n$. Then we have the embedding

$$(\sigma_1, \dots, \sigma_{r_1}, \tau_1, \dots, \tau_{r_2}) : K \overset{i}{\hookrightarrow} \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^{r_1} \times (\mathbb{R}^2)^{r_2} \cong \mathbb{R}^{r_1+2r_2} \cong \mathbb{R}^n. \tag{$*$}$$

Definition 10.1. Let Λ be a complete lattice in $\mathbb{R}^n$. A *fundamental domain* F is a subset $F \subseteq \mathbb{R}^n$ such that for all $x \in \mathbb{R}^n$, there is a unique $y \in F$ such that $x - y \in \Lambda$.

Remark. If $x_1, \dots, x_n$ form a $\mathbb{Z}$-basis for Λ, i.e. $\Lambda = \mathbb{Z}x_1 + \cdots + \mathbb{Z}x_n$, then

$$F = \{a_1x_1 + \cdots + a_nx_n : 0 \le x_i \le 1\}$$

is a fundamental domain, and every fundamental domain arises in this way. In particular, this means that if F, F' are fundamental domains, there exists $T \in \mathrm{GL}_n(\mathbb{Z})$ such that $F' = T(F)$.

Definition 10.2. The *covolume* of a complete lattice $\Lambda \subseteq \mathbb{R}^n$, denoted $\operatorname{covol}(\Lambda)$, is the volume of any fundamental domain. The above discussion says that $\operatorname{covol}(\Lambda)$ is well-defined.[1]

Theorem 10.1. *Let $i : K \to \mathbb{R}^n$ be defined as in $(*)$. Then*

1. *$i(\mathcal{O}_K)$ is a complete lattice in $\mathbb{R}^n$, and*
2. *$\operatorname{covol}(i(\mathcal{O}_K)) = 2^{-r_2}\sqrt{|\Delta_K|}$.*

Proof. One can show that $i(\mathcal{O}_K)$ is discrete, so it is a complete lattice in $\mathbb{R}^n$ (since $\mathcal{O}_K$ is of rank n and i is an embedding). Let $\alpha_1, \dots, \alpha_n$ be an integral basis for $\mathcal{O}_K$. Let

$$B = \begin{bmatrix} \sigma_1(\alpha_1) & \dots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_{r_1}(\alpha_1) & \dots & \sigma_{r_1}(\alpha_n) \end{bmatrix},$$

[1] Note that we can think of $\operatorname{covol}\Lambda$ as $\operatorname{vol}(\mathbb{R}^n/\Lambda)$, which motivates the name "covolume."

and note that $|\det B| = \sqrt{|\Delta_K|}$. Now define the matrix

$$A = \begin{bmatrix} \sigma_1(\alpha_1) & \dots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_{r_1}(\alpha_1) & \dots & \sigma_{r_1}(\alpha_n) \\ \operatorname{Re}\tau_1(\alpha_1) & \dots & \operatorname{Re}\tau_1(\alpha_n) \\ \operatorname{Im}\tau_1(\alpha_1) & \dots & \operatorname{Im}\tau_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \operatorname{Re}\tau_{r_2}(\alpha_1) & \dots & \operatorname{Re}\tau_{r_2}(\alpha_n) \\ \operatorname{Im}\tau_{r_2}(\alpha_1) & \dots & \operatorname{Im}\tau_{r_2}(\alpha_n) \end{bmatrix},$$

and one can compute that $\operatorname{covol}(i(\mathcal{O}_K)) = |\det A| = 2^{-r_2}|\det B| = 2^{-r_2}\sqrt{|\Delta_K|}$. □

Proposition 10.1. *Let $\Lambda' \subseteq \Lambda$ be a finite index sublattice. Then*

$$\operatorname{covol}(\Lambda') = [\Lambda : \Lambda'] \cdot \operatorname{covol}(\Lambda).$$

Proof. A fundamental domain for Λ' contains $[\Lambda : \Lambda']$ copies of a fundamental domain for Λ. □

Corollary 10.1.1. *For an ideal $I \subseteq \mathcal{O}_K$, we have* $\operatorname{covol}(i(I)) = N(I) \cdot 2^{-r_2}\sqrt{|\Delta_K|}$.

Remark. We have seen before that for every ideal I, there exists $\alpha \in I$ such that $|N(\alpha)| \leq M \cdot N(I)$. We will now try to improve this constant M using the above ideas. To do this, we will need to find a norm function on $\mathbb{R}^n$ which is compatible with N on $\mathcal{O}_K$.

Definition 10.3. Define the *norm* $\mathcal{N} : \mathbb{R}^n \to \mathbb{R}$ by

$$\mathcal{N}(a_1, \dots, a_{r_1}, x_1, y_1, \dots, x_{r_2}, y_{r_2}) = a_1 \dots a_{r_1}(x_1^2 + y_1^2) \dots (x_{r_2}^2 + y_{r_2}^2),$$

for $(a_1, \dots, a_{r_1}) \in \mathbb{R}^{r_1}$ and $(x_1, y_1, \dots, x_{r_2}, y_{r_2}) \in \mathbb{C}^{r_2} \cong \mathbb{R}^{2r_2}$. Note that $N(\alpha) = \mathcal{N}(i(\alpha))$.

10.2 Minkowski's Theory of the Geometry of Numbers

Definition 10.4. A set $S \subseteq \mathbb{R}^n$ is *(centrally) symmetric* when $x \in S$ if and only if $-x \in S$.

Lemma 10.1 (Geometric pigeonhole principle)**.** *Let $S \subseteq \mathbb{R}^n$ is a bounded measurable set. If $T : S \to \mathbb{R}^n$ is piecewise volume-preserving and* $\operatorname{vol}(S) > \operatorname{vol}(T(S))$*, then T is not injective.*

Proof. Since T is piecewise volume-preserving, we can write $S = \bigsqcup S_i$ (disjoint union) such that

$$\operatorname{vol}(T(S_i)) = \operatorname{vol}(S_i) \quad \text{for every } i.$$

If T is injective, then $T(S) = \bigsqcup T(S_i)$, which implies that

$$\operatorname{vol}(T(S)) = \sum \operatorname{vol}(T(S_i)) = \sum \operatorname{vol}(S_i) = \operatorname{vol}(S),$$

which contradicts the hypothesis that $\operatorname{vol}(S) > \operatorname{vol}(T(S))$. □

Example 10.4.1. Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice and F be a fundamental domain for Λ. Let $T : \mathbb{R}^n \to F$ send $x \in \mathbb{R}^n$ to the unique $y \in F$ such that $x - y \in \Lambda$. Then T is piecewise volume-preserving.

Theorem 10.2 (Minkowski's convex body theorem)**.** *Let $\Lambda \subseteq \mathbb{R}^n$ be a complete lattice, and let $S \subseteq \mathbb{R}^n$ be a convex, symmetric, bounded set. If $\mathrm{vol}(S) > 2^n \,\mathrm{covol}(\Lambda)$, then S contains a nonzero element of Λ.*[2]

Proof. Consider the lattice $\Lambda' = 2\Lambda \subseteq \Lambda$, so $\mathrm{covol}(\Lambda') = 2^n \,\mathrm{covol}(\Lambda)$. Let F' be a fundamental domain for Λ'. Let $T : \mathbb{R}^n \to F'$ be as in Example 10.4.1, which is piecewise volume-preserving. Then

$$\mathrm{vol}(S) > 2^n \,\mathrm{covol}(\Lambda) = \mathrm{covol}(\Lambda') = \mathrm{vol}(F') \geq \mathrm{vol}(T(S))$$

since $T(S) \subseteq F'$. Thus by the geometric pigeonhole principle, T is not injective, i.e. there exist distinct $x', y' \in S$ such $T(x') = T(y')$. So $p' = x' - y' \in \Lambda'$. Write $p' = 2p$ with $p \in \Lambda \setminus \{0\}$. Since S is symmetric, $-y' \in S$, and convexity implies

$$p = \frac{1}{2}x' + \frac{1}{2}(-y') \in S.$$

Thus p is a nonzero lattice point in S, which completes the proof. □

Remark. The $\mathrm{vol}(S) > 2^n \,\mathrm{covol}(\Lambda)$ condition is sharp: Let $\Lambda = \mathbb{Z}^n$ and $S = (-1, 1)^n$. Note that if S is closed (so compact since S is bounded), then the same conclusion holds when $\mathrm{vol}(S) = 2^n \,\mathrm{covol}(\Lambda)$.

10.3 Applications to Class Group Computations

Remark. We will apply Minkowski's convex body theorem to a compact, convex, symmetric

$$S \subseteq \{x \in \mathbb{R}^n : |\mathcal{N}(x)| \leq 1\}.$$

Note that $\{x \in \mathbb{R}^n : |\mathcal{N}(x)| \leq 1\}$ is not in general convex. For instance, consider the case where $K/\mathbb{Q}$ is a real quadratic field and $\mathcal{N}(x, y) = xy$. One can try to instead consider a subset S with a diamond shape lying inside the hyperbola shape, and consider homogeneous scalings of S. In general, set

$$S = \left\{ x \in \mathbb{R}^n : |a_1| + \cdots + |a_{r_1}| + 2\left(\sqrt{x_1^2 + y_1^2} + \cdots + \sqrt{x_{r_2}^2 + y_{r_2}^2} \leq n\right)\right\},$$

where $x = (a_1, \ldots, a_{r_1}, x_1, y_1, \ldots, x_{r_2}, y_{r_2})$. One can check that $S \subseteq \{x \in \mathbb{R}^n : |\mathcal{N}(x)| \leq 1\}$ (via tools like the AM-GM inequality, etc.), and that S is compact, convex, symmetric. One can also explicitly compute via calculus that

$$\mathrm{vol}(S) = \frac{n^n}{n!} 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2}.$$

Corollary 10.2.1. *Let Minkowski's constant be*

$$M_K = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2} \sqrt{|\Delta_K|}.$$

Then every ideal class in $\mathcal{O}_K$ contains a nonzero ideal of norm $\leq M_K$. Equivalently, every ideal I in $\mathcal{O}_K$ contains an element $\alpha \in I$ with $|N(\alpha)| \leq M_K \cdot N(I)$.

Remark. This is a significant improvement over the old method. For $\mathbb{Q}(\sqrt{-5})$, the old bound gives $M = 10$, whereas this method gives $M_k = 4\sqrt{5}/\pi < 3$.

[2] Note from measure theory that any convex set is (Lebesgue) measurable.

Lecture 11

Feb. 11 — Lagrange's Four Square Theorem

11.1 Lagrange's Four Square Theorem

Theorem 11.1 (Fermat)**.** *If $p \equiv 1 \pmod 4$ is a prime, then there exist $a, b \in \mathbb{Z}$ such that $p = a^2 + b^2$.*

Proof #1. Recall that by Kummer's theorem, factoring (p) in $\mathbb{Z}[i]$ is reduced to considering $x^2 + 1 \bmod p$. Since $p \equiv 1 \pmod 4$, we see that -1 is a square mod p (e.g. this follows by Euler's criterion for the Legendre symbol). So $p\mathbb{Z}[i] = \mathfrak{p}_1\mathfrak{p}_2$, where each $\mathfrak{p}_i$ has norm p. Since $\mathbb{Z}[i]$ is a UFD, we have $\mathfrak{p}_1 = (a + bi)$ and so $p = \mathbb{N}(\mathfrak{p}_1) = N(a + bi) = a^2 + b^2$. This proves the theorem. □

Remark. There is a way to generalize this proof for sums of four squares, but it requires developing unique factorization theory in the integer quaternions $\mathbb{Z}[i, j, k]$. The proof below generalizes more readily.

Proof #2. As above, we know that $x^2 \equiv -1 \pmod p$ has a solution, call it $u \in \mathbb{Z}$. Define $\Lambda \subseteq \mathbb{Z}^2$ by

$$\Lambda = \{(a, b) \in \mathbb{Z}^2 \mid b \equiv au \pmod p\}.$$

Then Λ is a rank 2 lattice, and $|\mathbb{Z}^2/\Lambda| = p$ (e.g. one can write an explicit isomorphism $\mathbb{Z}^2/\Lambda \to \mathbb{Z}/p\mathbb{Z}$ by mapping $[(a, b)] \in \mathbb{Z}^2/\Lambda$ to $a \in \mathbb{Z}/p\mathbb{Z}$, noting that a completely determines $b \bmod p$). Let

$$S = \overline{D}(0, r), \quad \text{where } \pi r^2 = 4p.$$

Then $\mathrm{vol}(S) = 4p = 2^2 \cdot \mathrm{vol}(\Lambda)$, so by Minkowski's theorem, there exists $(a, b) \neq (0, 0)$ in $\Lambda \cap S$. So

$$0 < a^2 + b^2 \leq r^2 = \frac{4}{\pi} \cdot p < 2p$$

since $\pi > 2$. Since $(a, b) \in \Lambda$, we have $b \equiv au \pmod p$, so $b^2 \equiv -a^2 \pmod p$, which implies $p|(a^2 + b^2)$. Then $a^2 + b^2$ is divisible by p but lies strictly between 0 and $2p$, so we must have $a^2 + b^2 = p$. □

Theorem 11.2 (Lagrange's four square theorem)**.** *Every positive integer n is a sum of four squares.*

Lemma 11.1. *It suffices to prove Lagrange's four square theorem when $n = p$ is prime.*

Proof. There is an identity that says the product of two numbers, which are each a sum of four squares, is again a sum of four squares. The idea behind the identity is the following: In the ring $\mathbb{H}_\mathbb{Z}$ of integral quaternions, we have $N(\alpha) = N(\alpha)N(\beta)$, where $N(a + bi + cj + dk) = a^2 + b^2 + c^2 + d^2$. □

Remark. The norm is also multiplicative in $\mathbb{C}$, where $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$ implies that $(a^2 + b^2) = (ac - bd)^2 + (ad + bc)^2$. A similar identity happens in the quaternions.

Lemma 11.2. *If p is an odd prime, then there exist $u, v \in \mathbb{Z}$ such that $u^2 + v^2 \equiv -1 \pmod{p}$.*

Proof. The number of squares in $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is (via the primitive element theorem and Euler's criterion) $(p-1)/2 + 1 = (p+1)/2$. Now define the sets

$$A = \{1 + x^2 : x \in \mathbb{F}_p\} \quad \text{and} \quad B = \{-y^2 : y \in \mathbb{F}_p\}.$$

Each of these sets contains $(p+1)/2$ elements, so $|A| + |B| = p + 1 > \#\mathbb{F}_p$. By the pigeonhole principle, $A \cap B \neq \varnothing$, so there exist $u, v \in \mathbb{F}_p$ such that $1 + u^2 \equiv -v^2 \pmod{p}$, which implies the result. □

Proof of Theorem 11.2. By the first lemma, it suffices to let $n = p$ be prime. As $2 = 1^2 + 1^2 + 0^2 + 0^2$, we can assume that p is an odd prime. By the second lemma, choose u, v such that $u^2 + v^2 \equiv -1 \pmod{p}$. Define $\Lambda \subseteq \mathbb{Z}^4$ by

$$\Lambda = \{(a, b, c, d) \in \mathbb{Z}^4 : c \equiv ua + vb, d = ub - va \pmod{p}\}.$$

Note that $\operatorname{covol}(\Lambda) = |\mathbb{Z}^4/\Lambda| = p^2$ (similarly we find an isomorphism $\mathbb{Z}^4/\Lambda \to (\mathbb{Z}/p\mathbb{Z})^2$ by $(a, b, c, d) \mapsto (a, b)$). Once we can find $(a, b, c, d) \neq 0$ in Λ with norm $< 2p$ (claim), we have

$$\begin{aligned} a^2 + b^2 + c^2 + d^2 &\equiv a^2 + b^2 + (ua + vb)^2 + (ub - va)^2 \\ &\equiv a^2 + b^2 + u^2a^2 + v^2b^2 + u^2b^2 + v^2a^2 \\ &\equiv a^2 + b^2 + (u^2 + v^2)a^2 + (u^2 + v^2)b^2 \\ &\equiv a^2 + b^2 - a^2 - b^2 \\ &\equiv 0 \pmod{p}, \end{aligned}$$

since $u^2 + v^2 \equiv -1 \pmod{p}$. Then as before, $a^2 + b^2 + c^2 + d^2$ is divisible by p but lands strictly between 0 and $2p$, so we must have $a^2 + b^2 + c^2 + d^2 = p$. Given the claim, this proves the result.

So it suffices to find such a point $(a, b, c, d) \neq 0$. Let B_r be the 4-dimensional closed ball of radius r. If $\operatorname{vol}(B_r) = 2^4p^2$, then by Minkowski we get a nonzero lattice point in B_r. We want $r^2 < 2p$. We have

$$\frac{1}{2}\pi^2 r^4 = \operatorname{vol}(B_r) = 16p^2,$$

so $r^2 = \sqrt{32p^2/\pi^2} = (4\sqrt{2}/\pi) \cdot p$. So we need $4\sqrt{2}/\pi < 2$, which happens if and only if $\pi > 2\sqrt{2}$. This is true, since $\pi \approx 3.14$ and $2\sqrt{2} \approx 2.83$, which completes the proof of the theorem. □

11.2 Revisiting Minkowski's Theorem

Remark. Recall that for a number field K, every ideal class is represented by an ideal of norm $\leq M_K$:

$$M_K = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|\Delta_K|}.$$

This implies that $M_K \geq 1$, since an ideal cannot have norm 0. In the above formula, this gives

$$\sqrt{|\Delta_K|} \geq \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{n/2},$$

which is > 1 when $n \geq 2$ and goes to ∞ as $n \to \infty$. This implies that if $K \neq \mathbb{Q}$ is any number field, then some p ramifies in $\mathcal{O}_K$. This then means that $\mathbb{Z}$ has no unramified covers, which means that $\mathbb{Z}$ has trivial "arithmetic fundamental group." The subject discussing this is called *étale cohomology*.

Theorem 11.3 (Tate?)**.** *If $E/\mathbb{Q}$ is an elliptic curve, then there is some prime of bad reduction.*

Remark. The above theorem from the theory of elliptic curves has a similar flavor to our discussion above. Fontaine greatly generalizes this result to an abelian variety $A/\mathbb{Q}$.

11.3 Introduction to Dirichlet's Unit Theorem

Remark. Let K be a number, $\mathcal{O}_K$ its ring of integers, and $\mathcal{O}_K^\times$ the *unit group.*

Theorem 11.4 (Dirichlet, weak)**.** *The unit group $\mathcal{O}_K^\times$ is finitely generated. In particular,*

$$\mathcal{O}_K \cong \mathbb{Z}^r \times (\textit{finite abelian group}),$$

where the finite abeliain group is the roots of unity in K.

Example 11.0.1. Suppose $[K:\mathbb{Q}] = 2$. If K is imaginary, then $K = \mathbb{Q}(\sqrt{-d})$, where $d > 0$ is square free. Then $u \in \mathcal{O}_K$ is a unit if and only if $N(u) = 1$, Since u is either $a + b\sqrt{-d}$ or $a + b\sqrt{-d}/2$, One can use $N(a + b\sqrt{-d}) = a^2 + db^2 = 1$ to easily find the units. The conclusion is

$$\mathcal{O}_K^\times = \begin{cases} \{\pm 1, \pm i\}, & \text{if } d = 1, \\ \{\pm 1, \pm\omega \pm \omega^2\}, & \text{if } d = 3, \\ \{\pm 1\}, & \text{otherwise,} \end{cases}$$

so $\mathcal{O}_K$ has rank 0. Now consider a real quadratic field $K = \mathbb{Q}(\sqrt{d})$. For $\mathbb{Q}(\sqrt{2})$, notice that

$$(\sqrt{2} - 1)(\sqrt{2} + 1) = 1.$$

In particular, this means that $(\sqrt{2} - 1)^k$ is a unit for each $k \in \mathbb{Z}$, yielding a rank 1 subgroup. In fact,

$$\mathbb{Z}[\sqrt{2}]^\times \cong \{\pm 1\} \times \mathbb{Z} \cong \{\pm 1\} \times \langle \sqrt{2} - 1 \rangle.$$

One can also view this from the perspective of Diophantine equations. Note that $a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ is a unit if and only if $a^2 - 2b^2 = \pm 1$. The set of solutions to this equation form a group under multiplication, and that group is of rank 1. This is the *generalized Pell equation*, $a^2 - db^2 = \pm 1$. It is known for certain d modulo 4, this equation has infinitely many solutions, which are generated by a single fundamental solution. This result follows as a special case of Dirichlet's unit theorem.

Remark. The above Pell equations are difficult to solve, even for relatively small values of d. For instance, the smallest solution to $a^2 - 61b^2 = 1$ is $a \approx 10^6$, $b \approx 10^8$.

Example 11.0.2. Let $K = \mathbb{Q}(\zeta_m)$, where $m = p^k$. Then the unit group $\mathcal{O}_K^\times$ contains

$$\left\{ \frac{1 - \zeta_m^a}{1 - \zeta_m} : 1 \le a \le p - 1 \right\}.$$

This generates a subgroup of rank $\phi(m)/2 - 1 = r_1 + r_2 - 1$ (here r_1 is the number of real embeddings and r_2 is $1/2$ the number of complex embeddings). Note that this is compatible with the quadratic case, since $r_1 + r_2 - 1$ is 1 if K is real and 0 if K is complex.

Lecture 12

Feb. 13 — Dirichlet's Unit Theorem

12.1 Dirichlet's Unit Theorem and Proof

Theorem 12.1 (Dirichlet's unit theorem)**.** *For a number field K of degree n, we have*

$$\mathcal{O}_K^\times \cong \mathbb{Z}^r \times (\textit{finite abelian group})$$

where the finite abelian group is the roots of unity in K and $r = r_1 + r_2 - 1$ ($\leq n-1$, with equality if and only if $K/\mathbb{Q}$ is totally real), where r_1, r_2 are the number of real and (pairs of) complex embeddings of K.

Remark. The strategy is the following: Let $L : K^\times \to \mathbb{R}^{r_1+r_2}$ be the homomorphism given by

$$L(\alpha) = (\log|\sigma_1(\alpha)|, \dots, \log|\sigma_{r_1}(\alpha)|, \log|\tau_1(\alpha)|, \dots, \log|\tau_{r_2}(\alpha)|),$$

where $\sigma_1, \dots, \sigma_{r_1} : K \hookrightarrow \mathbb{R}$ are the real embeddings and $\tau_1, \dots, \tau_{r_2} : K \hookrightarrow \mathbb{C}$ are half of the complex embeddings. We will want to show that $L(\mathcal{O}_K)$ is a lattice.

Lemma 12.1. *We have* $\ker L|_{\mathcal{O}_K^\times} = \mu_K$ *and* $L(\mathcal{O}_K^\times) \subseteq H = \{\sum x_i = 0\}$.

Proof. We can write the kernel of $L_{\mathcal{O}_K^\times}$ as

$$\ker L|_{\mathcal{O}_K^\times} = \left\{\alpha \in \mathcal{O}_K^\times : \begin{matrix}\text{absolute values of the conjugates} \\ \alpha_1, \dots, \alpha_m \text{ of } \alpha \text{ are all } 1\end{matrix}\right\} = \mu_K$$

by Kronecker's theorem. Now if $\alpha \in \mathcal{O}_K^\times$, then $|N_{\mathbb{Q}}^K(\alpha)| = 1$, so

$$\left|\prod_i \sigma_i(\alpha) \cdot \prod_j \tau_j(\alpha)^2\right| = 1,$$

which implies that $\sum \log|\sigma_i(\alpha)| + \sum \log|\tau_j(\alpha)|^2 = 0$, i.e. $L(\alpha) \in H$. □

Corollary 12.1.1. *We have* $\mathcal{O}_K^\times/\mu_K \subseteq H \cong \mathbb{R}^{r_1+r_2-1}$.

Lemma 12.2. *For any closed ball B around 0 in $\mathbb{R}^{r_1+r_2}$, $L(\mathcal{O}_K^\times) \cap B$ is finite, i.e. $L(\mathcal{O}_K^\times)$ is discrete.*

Proof. We can write the intersection via

$$L(\mathcal{O}_K^\times) \cap B = \{\alpha \in \mathcal{O}_K^\times : \text{all conjugates of } \alpha \text{ have norm bounded by } C\}.$$

For any element of the set, there are only finitely many possible minimal polynomials, each with only a finite number of roots, so the set itself must be finite. □

Lemma 12.3. *Let $A = (a_{ij})$ be an $r \times r$ real matrix such that:*

1. *the entries in each row sum to 0,*
2. *the diagonal entries $a_{ii} > 0$, and*
3. *the off-diagonal entries $a_{ij} < 0$ for $i \neq j$.*

Then $\operatorname{rank} A = r - 1$.

Proof. It suffices to show that the first $r-1$ columns $v_1, \dots, v_{r-1}$ are linearly independent. Suppose otherwise that we can write

$$\sum_{i=1}^{r-1} c_i v_i = 0,$$

where the c_i are not all zero. Without loss of generality, assume $c_k = 1$ and $c_j \leq 1$ for all $j \neq k$. Then $a_{kj} < 0$ implies that $c_j a_{jk} \geq a_{jk}$, and $\sum_{j=1}^{r-1} a_{kj} > \sum_{j=1}^{r} a_{kj}$ since $k \neq r$. Then

$$0 = \sum_{j=1}^{r-1} c_j a_{kj} \geq \sum_{j=1}^{r-1} a_{kj} > \sum_{j=1}^{r} a_{kj} = 0,$$

which is a contradiction. Since (1) imposes one linear condition, we have $\operatorname{rank} A = r - 1$. □

Lemma 12.4. *Fix k with $1 \leq k \leq r$. Then there is a constant C (depending only on K) such that given $\alpha \in \mathcal{O}_K \setminus \{0\}$, there exists $\beta \in \mathcal{O}_K \setminus \{0\}$ with:*

1. *$|N(\beta)| \leq C$, and*
2. *if $L(\alpha) = (a_1, \dots, a_r)$ and $L(\beta) = (b_1, \dots, b_r)$, then $b_i < a_i$ for all $i \neq k$.*

Proof. We claim that taking

$$C = \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|\Delta_K|}$$

works. For convenience, let

$$\epsilon_i = \begin{cases} 1 & \text{if } 1 \leq i \leq r_1, \\ 2 & \text{if } r_1 + 1 \leq i \leq r = r_1 + r_2. \end{cases}$$

Choose $a_1', \dots, a_r'$ with $a_i' < a_i$ for each i. Define the region

$$E = \{x \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} : |x_i|^{\epsilon_i} \leq C_i\},$$

where $C_i = e^{a_i'}$ for $i \neq k$ and $\prod_i C_i = C$. It is clear that E is symmetric, compact, convex, and

$$\operatorname{vol}(E) = 2^{r_1} \pi^{r_2} \prod_i C_i = 2^{r_1} \pi^{r_2} C = 2^n \operatorname{covol} i(\mathcal{O}_K)$$

So by Minkowski's theorem, $E \cap i(\mathcal{O}_K) \neq \{0\}$. Thus taking $p \in E \cap i(\mathcal{O}_K)$ and $\beta = i^{-1}(p)$ works. □

Proof of Theorem 12.1. Choose $\alpha_0 \in \mathcal{O}_K$ arbitrarily and fix k. By Lemma 12.4, we can find a sequence $\alpha_1, \alpha_2, \alpha_3, \dots \in \mathcal{O}_K \setminus \{0\}$ such that if $L(\alpha_j) = (a_1(j), \dots, a_r(j))$, then $|N(\alpha_j)| \leq C$ for $j \geq 1$ and $a_i(j) < a_i(j-1)$ for $j \geq 1$, for all $i \neq k$. There are only a finite number of ideals of norm $\leq C$, so there

exists $j_1 > j_2$ such that $(\alpha_{j_1}) = (\alpha_{j_2})$. So $u^{(k)} = \alpha_{j_1}/\alpha_{j_2} \in \mathcal{O}_K^\times$. If $L(u^{(k)}) = (a_1, \dots, a_r)$, then $a_i < 0$ for $i \neq k$, since $a_i = a_i(j_1) - a_i(j_2) < 0$. Then $a_k > 0$ since $L(u) \in H$.

Now applying Lemma 12.3 to $u^{(1)}, \dots, u^{(k)}$, we see that $\mathcal{O}_K^\times/\mu_K$ is full rank in $H \cong \mathbb{R}^{r_1+r_2-1}$. □

Remark. Next time, we will compute the class group and unit group of $\mathbb{Q}(\sqrt[3]{11})$.

12.2 Real Quadratic Fields and Continued Fractions

Example 12.0.1. Let $K = \mathbb{Q}(\sqrt{d})$, where $d > 0$ is square-free. We know that the unit group $\mathcal{O}_K^\times$ has rank 1, and (if $d \equiv 2, 3 \pmod 4$) the units correspond to the integer solutions to $x^2 - dy^2 = \pm 1$.

To solve this equation, one computes the continued fraction expansion for $\sqrt{d}$. A *continued fraction* is

$$\alpha = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \dots}}$$

for some positive integers a_i, also denoted $[a_1, a_2, a_3, \dots]$. The *nth convergent* for $[a_1, a_2, a_3, \dots]$ is

$$[a_1, a_2, \dots, a_n] = a_1 + \cfrac{1}{a_2 + \cfrac{1}{\dots + \cfrac{1}{a_n}}} = \frac{p_n}{q_n}$$

The reason for the name convergent is because $p_n/q_n \to \alpha$ as $n \to \infty$.

Theorem 12.2. *Every $\alpha > 1$ has a unique continued fraction expansion.*

Theorem 12.3. *We have the following:*

1. *The continued fraction expansion of α is finite if and only if $\alpha \in \mathbb{Q}$.*
2. *The continued fraction expansion of α is pre-periodic if and only if $[\mathbb{Q}(\alpha) : \mathbb{Q}] \leq 2$.*[1]

Theorem 12.4. *Let $d \equiv 2, 3 \pmod 4$ be square-free and positive. Let $\varepsilon > 1$ be the fundamental unit of $\mathbb{Z}[\sqrt{d}]$, i.e. the unique unit which generates the unit group and is > 1. Let k be the period of the continued fraction expansion of $\sqrt{d}$. Then $\varepsilon = p_k + q_k\sqrt{d}$.*

Example 12.0.2. Let $K = \mathbb{Q}(\sqrt{19})$. One can compute that

$$\sqrt{19} = [4, \overline{2, 1, 3, 1, 2, 8}],$$

which has period 6. The 6th convergents are $p_6 = 170$ and $q_6 = 39$. This says that

$$\sqrt{19} \approx \frac{170}{39}.$$

In fact, $170^2 - 19 \cdot 39^2 = 1$. This also means that $170 + 39\sqrt{19}$ is the fundamental unit in K.

Remark. For $\mathbb{Q}(\sqrt{94})$, the fundamental unit is $2143295 + 221064\sqrt{94}$. Furthermore, in $\mathbb{Q}(\sqrt{9199})$, the first coefficient for the fundamental unit has 88 decimal digits.

[1] A continued fraction expansion is *pre-periodic* if it is periodic after some finite prefix.

Lecture 13

Feb. 18 — Computing Unit Groups

13.1 Computing Unit Groups

Exercise 13.1. Show that the sign of Δ_K is $(-1)^{r_2}$.

Remark. If $n = 3$ and $r_1 = r_2 = 1$, then by Dirichlet's unit theorem we know that $\mathcal{O}_K^\times$ has rank 1. The *fundamental unit* is the unique generator $\varepsilon \in \mathcal{O}_K^\times$ with $\varepsilon > 1$. This means that

$$\mathcal{O}_K^\times = \{\pm\varepsilon^k : k \in \mathbb{Z}\}.$$

(Note that when K has a real embedding, the only roots of unity are ± 1.) We want a lower bound for ε.

Lemma 13.1. *Let K be a cubic number field with negative discriminant. Then*

$$\varepsilon > \sqrt[3]{\frac{|\Delta_K| - 24}{4}}.$$

Equivalently, $|\Delta_K| < 4\varepsilon^3 + 24$.

Proof. Let $\varepsilon = \varepsilon_1$ and $\varepsilon_2, \varepsilon_3$ be its other two conjugates. Since K has a pair of complex embeddings, we have $\varepsilon_3 = \overline{\varepsilon_2}$. Write $\varepsilon = u^2$ with $u > 1$ in $\mathbb{R}$. Then since $N(\varepsilon) = 1$, we have

$$|\varepsilon_2|^2 = \frac{1}{\varepsilon} = u^{-2}.$$

Thus $\varepsilon_2 = u^{-1}e^{i\theta}$, with $0 \le \theta \le \pi$ (by exchanging the two conjugates, if necessary). Then

$$|\Delta(\varepsilon)|^{1/2} = |\Delta(1, \varepsilon, \varepsilon^2)|^{1/2} = \det \begin{bmatrix} 1 & \varepsilon & \varepsilon^2 \\ 1 & \varepsilon_2 & \varepsilon_2^2 \\ 1 & \varepsilon_3 & \varepsilon_3^2 \end{bmatrix} = 2(u^3 + u^{-3} - 2\cos\theta)\sin\theta.$$

Note that $K = \mathbb{Q}(\varepsilon)$, so $|\Delta_K| \le |\Delta(\varepsilon)|$. Thus it suffices to bound $|\Delta(\varepsilon)|$. We claim that

$$2(u^3 + u^{-3} - 2\cos\theta)\sin\theta \le (4\varepsilon^3 + 24)^{1/2} = (4u^6 + 24)^{1/2},$$

which would prove the lemma. Set $2a = u^3 + u^{-3}$, so that

$$|\Delta(\varepsilon)|^{1/2} = 4(a - \cos\theta)\sin\theta.$$

For fixed a, this is maximized when $a\cos\theta = 2\cos^2\theta - 1$. Let $x = \cos\theta$ and $g(x) = 2x^2 - ax - 1$, so that $\cos\theta$ is a root of g. Note that $u > 1$, so $a > 1$ and thus $g(1) = 1 - a < 0$. Clearly, $g(x) > 0$ for x

sufficiently large, so g has a root > 1. But this is not the root we want. We also have $g(-1/2u^3) < 0$ and $g(-1) > 0$, where $-1/2u^3 \in (-1/2, 0)$, so this gives a root $x_0 \in (-1, -1/2u^3) \subseteq (0, 1)$. Then

$$|\Delta(\varepsilon)|^{1/2} \leq 4(a - x_0)(1 - x_0^2)^{1/2},$$

which gives the bound

$$|\Delta(\varepsilon)| \leq 16(a^2 + 1 - x_0^2 - x_0^4) < 4u^6 + 24$$

since $x_0 \in (-1, -1/2u^3)$. This proves the claim. □

Remark. The smallest value of $|\Delta_K|$ over all cubic number fields K is 23.

Example 13.0.1. We will find the unit group for $K = \mathbb{Q}(\sqrt[3]{2})$. Let $\alpha = \sqrt[3]{2}$, which satisfies

$$1 + \alpha + \alpha^2 = \frac{\alpha^3 - 1}{\alpha - 1} = \frac{1}{\alpha - 1}.$$

In particular, $u = 1 + \alpha + \alpha^2 \in \mathcal{O}_K^\times$, and we claim that $\varepsilon = u$. Note that

$$\Delta_K = \Delta(x^3 - 2) = -108.$$

So the lemma implies that $\varepsilon^3 > (108 - 24)/4 = 21$, i.e. $\varepsilon > \sqrt[3]{21}$. One can compute that

$$1 < u < 7 < (21)^{2/3},$$

which implies that $1 < u < \varepsilon^2$. Since $u = \varepsilon^m$ for $m \geq 1$ (as u is positive), we must have $m = 1$.

Example 13.0.2. Let $K = \mathbb{Q}(\sqrt[3]{11})$. We will find $\mathcal{O}_K^\times$ and $\mathrm{Cl}(\mathcal{O}_K)$. Note that the calculus argument (lower bound for ε) will not work here: It only tells us that a certain unit u is either ε or ε^2. Note that

$$11^2 \not\equiv 1 \pmod 9,$$

so $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{11}]$. Also note that $\Delta_K = -3 \cdot 11^2$, so Minkowski's constant is

$$M_K = \frac{3!}{3^3}\left(\frac{4}{\pi}\right)\sqrt{3^3 \cdot 11^2} < 17.$$

Thus we want to factor $2, 3, 5, 7, 11, 13$ in $\mathcal{O}_K$. We can factor $x^3 - 11 \pmod p$ by:

p	$x^3 - 11 \pmod p$
2	$(x-1)(x^2+x+1)$
3	$(x+1)^3$
5	$(x-1)(x^2+x+1)$
7	$x^3 - 4$
11	x^3
13	$x^3 - 2$

Thus by Kummer's theorem, we have $(2) = \mathfrak{p}_2\mathfrak{p}_2'$ with $N(\mathfrak{p}_2) = 2$ and $N(\mathfrak{p}_2') = 4$, $(3) = \mathfrak{p}_3^3$, $(5) = \mathfrak{p}_5\mathfrak{p}_5'$ with $N(\mathfrak{p}_5) = 5$, and $(11) = \mathfrak{p}_{11}^3$ where $\mathfrak{p}_{11} = (\alpha)$ for $\alpha = \sqrt[3]{11}$. Thus the class group is generated via

$$\mathrm{Cl}(\mathcal{O}_K) = \langle [\mathfrak{p}_2], [\mathfrak{p}_3], [\mathfrak{p}_5] \rangle.$$

Now we want to find some elements of $\mathcal{O}_K$ with small norm.

Note that α has minimal polynomial $x^3 - 11$, so $\alpha - t$ has minimal polynomial $(x-t)^3 - 11$ for $t \in \mathbb{Z}$, so $N(\alpha - t) = t^3 - 11$. For $t = 1$,

$$N(\alpha - 1) = -10,$$

so $(\alpha - 1)$ has norm 10. Thus $(\alpha - 1) = \mathfrak{p}_2\mathfrak{p}_5$, which allows us to remove $\mathfrak{p}_5$ as a generator. For $t = 2$,

$$N(\alpha - 2) = -3,$$

so $(\alpha - 2) = \mathfrak{p}_3$ and we can remove $\mathfrak{p}_3$ as a generator. So $\mathrm{Cl}(\mathcal{O}_K) = \langle [\mathfrak{p}_2] \rangle$, and it suffices to find the order of $\mathfrak{p}_2$. Set $t = -1$, so

$$N(\alpha + 1) = -12.$$

Thus $(\alpha + 1) = \mathfrak{p}_3\mathfrak{p}_2^2$ or $\mathfrak{p}_3\mathfrak{p}_2'^2$. But $\mathfrak{p}_2 = (2, \alpha - 1)$ contains $\alpha + 1$, so $\mathfrak{p}_2$ divides $(\alpha + 1)$. Thus

$$(\alpha + 1) = \mathfrak{p}_3\mathfrak{p}_2^2,$$

so $\mathfrak{p}_2^2$ is principal. So $\mathfrak{p}_2$ has order dividing 2, and $\mathrm{Cl}(\mathcal{O}_K) \cong \mathbb{Z}/2\mathbb{Z}$ or $\{1\}$.

To see which one it is, we will need some information about the unit group. We begin by finding some nontrivial unit. To do this, note that $\mathfrak{p}_3 = (\alpha - 2)$ and $\mathfrak{p}_3\mathfrak{p}_2^2 = (\alpha + 1)$. Then $\mathfrak{p}_2^2 = (\beta)$ for

$$\beta = \frac{\alpha + 1}{\alpha - 2} = \alpha^2 + 2\alpha + 5.$$

Using $t = 3$ from before, we have $N(\alpha - 3) = 16$, so $(\alpha - 3) = \mathfrak{p}_2^4$ or $\mathfrak{p}_2^2\mathfrak{p}_2'^2$ since $\alpha - 3 \in \mathfrak{p}_2$. But $\mathfrak{p}_2\mathfrak{p}_2'^2 = (2)$ and 2 does not divide $\alpha - 3$, so we must have $(\alpha - 3) = \mathfrak{p}_2^4$. Then $\mathfrak{p}_2^4 = (\beta^2)$, so

$$u = -\frac{\beta^2}{\alpha - 3} \approx 266.99 > 1$$

is a unit. The lower bound gives $\varepsilon > 9.34$, so $\varepsilon^3 > u$. Thus either $u = \varepsilon$ or ε^2.

The new idea from this point is the following: We will construct a homomorphism $\mathbb{Z}[\alpha] \to \mathbb{F}_p$ for suitable p, such that the image of u is not a square (this will imply that u itself cannot be a square). Try

$$\mathfrak{p}_5 = (5, \alpha - 1)$$

with norm 5, so reduction mod $\mathfrak{p}_5$ gives a homomorphism $\mathbb{Z}[\alpha] \to \mathbb{F}_5 = \mathbb{Z}[\alpha]/\mathfrak{p}_5$ which maps $\alpha \mapsto 1$. Using $u = -\beta^2/(\alpha - 3) = -(\alpha^2 + 2\alpha + 5)/(\alpha - 3)$, we have $u \mapsto 2$, which is not a square. So $\varepsilon = u$.

Now we claim that $\mathfrak{p}_2$ is not principal. If it were, then $\mathfrak{p}_2 = (\gamma)$ and

$$(\beta) = \mathfrak{p}_2^2 = (\gamma^2).$$

Then for $v = u^{-1} = -2\alpha^2 + 4\alpha + 1$, we can write $\pm v^m \beta = \gamma^2$ for some m. Without loss of generality, we can assume $m = 0$ or 1 (by absorbing powers of v into γ). So one of β, $-\beta$, $v\beta$, or $-v\beta$ is a square in $\mathcal{O}_K$. As before, we can find homomorphisms $\mathbb{Z}[\alpha] \to \mathbb{F}_p$ for various p such that each of these elements map to non-squares, which will give a contradiction. Note that 19 splits completely in K, so we get three homomorphisms $\mathbb{Z}[\alpha] \to \mathbb{F}_{19}$, with $\alpha \mapsto \{5, -3, -2\}$. Choose the one which maps $\alpha \mapsto 5$. This one sends $\beta \to 2$ and $v\beta \to -1$, which are non-squares. Choosing the one with $\alpha \mapsto -2$, we find $-\beta \mapsto -5$ and $-v\beta \mapsto -1$, which are non-squares mod 19. Thus $\mathfrak{p}_2$ is not principal, so $\mathfrak{p}_2$ has order 2.

This shows that $\mathrm{Cl}(\mathcal{O}_K) \cong \mathbb{Z}/2\mathbb{Z}$ and $\mathcal{O}_K^\times = \{\pm\langle v \rangle\}$.

Lecture 14

Feb. 20 — Localization

14.1 Motivation for Localization

Remark. So far we have been dealing with the following scenario of a number field K:

$$\begin{array}{ccc} K & \text{---} & \mathcal{O}_K \\ \Big|{\scriptstyle n} & & \Big|{\scriptstyle n} \\ \mathbb{Q} & \text{---} & \mathbb{Z} \end{array}$$

We would now like to consider relative extensions, for a finite extension L/K:

$$\begin{array}{ccc} L & \text{---} & \mathcal{O}_L \\ \Big|{\scriptstyle n} & & \Big|{\scriptstyle n} \\ K & \text{---} & \mathcal{O}_K \end{array}$$

For instance, that if prime ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_r \subseteq \mathcal{O}_L$ lie over $\mathfrak{p} \subseteq \mathcal{O}_K$, then $[L : K] = \sum_{i=1}^{r} e_i f_i$. One of our goals will be to show that a Noetherian domain R is Dedekind if and only if $R_\mathfrak{p}$ is a PID for every prime ideal $\mathfrak{p}$. The second goal will be to prove "Dirichlet's S-unit theorem."

14.2 Localization

Definition 14.1. Let R be a domain and K its field of fractions. Let S be a *multiplicative subset* of R, i.e. $0 \notin S$, $1 \in S$, and $a, b \in S$ implies $ab \in S$. Then the *localization of R by S* is the subring

$$S^{-1}R = \left\{ \frac{a}{b} : a \in R, b \in S \right\} \subseteq K.$$

Remark. The equivalence relation of $a/b \sim c/d$ if $ad = bc$ is included by default since $S^{-1}R \subseteq K$.

Remark. Note that $R \subseteq S^{-1}R \subseteq K$. The idea is that $S^{-1}R$ will have some of the nice properties of K while still retaining enough of the information of R.

Example 14.1.1. For $S = R \setminus \{0\}$, we have $S^{-1}R = K$, and for $S = \{1\}$, we have $S^{-1}R = R$.

Example 14.1.2. If $\mathfrak{p} \subseteq R$ is a prime ideal, then $S = R \setminus \mathfrak{p}$ is a multiplicative subset. Thus we can define $R_\mathfrak{p} = S^{-1}R$, which we will call the *localization of R at $\mathfrak{p}$*.

Remark. One can definition localization in a more general context, e.g. for a ring which is not a domain. This is necessary for algebraic geometry, but we do not need this, so we will avoid it.

Proposition 14.1. *The prime ideals of $S^{-1}R$ are in (inclusion-preserving) bijection with the prime ideals of R disjoint from S.*

Proof. Denote by $\operatorname{Spec} R$ the set of prime ideals of R. We will show the following bijection:

$$\begin{aligned} \{\mathfrak{q} \in \operatorname{Spec}(R) : \mathfrak{q} \cap S = \varnothing\} &\longleftrightarrow \operatorname{Spec}(S^{-1}R) = \operatorname{Spec}(R') \\ \mathfrak{q} &\longmapsto S^{-1}\mathfrak{q} = \left\{ \frac{a}{b} : a \in \mathfrak{q}, b \in S \right\} \\ \mathfrak{q}' \cap R &\longmapsto \mathfrak{q}' \end{aligned}$$

First we claim that $S^{-1}\mathfrak{q}$ is a prime ideal in R'. Note that $\mathfrak{q} \cap S = \varnothing$ is equivalent to $1 \notin S^{-1}\mathfrak{q}$. Check as an exercise that $S^{-1}\mathfrak{q}$ is in fact an ideal in R'. To see that it is prime, suppose that $(a_1/b_1)(a_2/b_2) \in S^{-1}\mathfrak{q}$, where $a_1, a_2 \in R$ and $b_1, b_2 \in S$. Then we can see that

$$\frac{a_1 a_2}{b_1 b_2} = \frac{a}{b}, \quad a \in \mathfrak{q}, b \in S,$$

so $a_1 a_2 b = a b_1 b_2 \in \mathfrak{q}$. As $b \in S$ and $q \cap S = \varnothing$, we have $b \notin \mathfrak{q}$. Thus $a_1 \in \mathfrak{q}$ or $a_2 \in \mathfrak{q}$, i.e. $S^{-1}\mathfrak{q}$ is prime.

The other direction is easier and is mostly left as an exercise. To see that $(\mathfrak{q}' \cap R) \cap S = \varnothing$, suppose that $s \in S \cap \mathfrak{q}'$. Then $s \cdot (1/s) = 1 \in \mathfrak{q}'$, where $s \in \mathfrak{q}'$ and $(1/s) \in R$, which is impossible since $\mathfrak{q}' \neq R$.

It only remains to show that these maps are inverses of each other, which is left as an exercise. □

Corollary 14.0.1. *The prime ideals of $R_\mathfrak{p}$ are in bijection with the prime ideals of R contained in $\mathfrak{p}$.*

Corollary 14.0.2. *The localization $R_\mathfrak{p}$ is a local ring, i.e. it has a unique maximal ideal.*

Example 14.1.3. We can write the localization $\mathbb{Z}_{(2)}$ as

$$\mathbb{Z}_{(2)} = \left\{ \frac{a}{b} \in \mathbb{Q} : b \text{ is odd} \right\}.$$

The unique maximal ideal is $2\mathbb{Z}_{(2)} = \{2a/b : b \text{ is odd}\}$, and $\mathbb{Z}_{(2)} \setminus 2\mathbb{Z}_{(2)} = \mathbb{Z}_{(2)}^\times$. We also have

$$\mathbb{Z}_{(2)}/2\mathbb{Z}_{(2)} = \mathbb{Z}/2\mathbb{Z}.$$

In general, we will see that $\mathcal{O}_K/\mathfrak{p}^m\mathcal{O}_K \cong (\mathcal{O}_K)_\mathfrak{p}/\mathfrak{p}^m(\mathcal{O}_K)_\mathfrak{p}$, so we can study the localization instead.

Lemma 14.1. *Let R be a ring and $\mathfrak{m}$ a maximal ideal in R. If $s \notin \mathfrak{m}$, then $\mathfrak{m}^n + (s) = (1)$ for all $n \geq 1$. Equivalently, $\overline{s}$ is a unit in $R/\mathfrak{m}^n$ for every $n \geq 1$.*

Proof. We induct on n. The case $n = 1$ is clear since $\mathfrak{m}$ is maximal. Now suppose $(1) = \mathfrak{m}^{n-1} + (s)$, so

$$\mathfrak{m} = \mathfrak{m}^n + s\mathfrak{m} \subsetneq \mathfrak{m}^n + (s)$$

since $s \notin \mathfrak{m}$. But $\mathfrak{m}$ is a maximal ideal, so we must have $\mathfrak{m}^n + (s) = (1)$. □

Remark. We will denote $\mathfrak{m}_\mathfrak{p} = \mathfrak{p}R_\mathfrak{p}$, the unique maximal ideal in the localization $R_\mathfrak{p}$.

Lemma 14.2. *Let R be an integral domain and $\mathfrak{p}$ a maximal ideal. Then for all $n \geq 1$, the natural map*

$$\phi : R/\mathfrak{p}^n \to R_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}^n$$

is an isomorphism. (In particular, $R/\mathfrak{p} \cong R_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}$.)

Proof. The natural map is the map induced by the inclusion $R \hookrightarrow R_\mathfrak{p}$ on the quotient $R/\mathfrak{p}^n$.

First we show that ϕ is injective. Suppose $x \in R \cap \mathfrak{m}_\mathfrak{p}^n$, and we will show that $x \in \mathfrak{p}^n$. Write

$$x = \frac{y}{s}, \quad y \in \mathfrak{p}^n, s \notin \mathfrak{p}.$$

By the lemma, we have $\overline{s} \in (R/\mathfrak{p}^n)^\times$. But $sx = y \in \mathfrak{p}^n$, which implies that $\overline{s} \cdot \overline{x} = 0$ in $R/\mathfrak{p}^n$. Since $\overline{s}$ is a unit, this means that $\overline{x} = 0$, so $x \in \mathfrak{p}^n$. This shows that ϕ is injective.

Now we show that ϕ is surjective. Let $r/s \in R_\mathfrak{p}$ with $r \in R$ and $s \notin \mathfrak{p}$. By the lemma, there exists $r' \in R$ such that $r \equiv r's \pmod{\mathfrak{p}^n}$ (e.g. take $r' = s^{-1}r \in R/\mathfrak{p}^n$). Then $r/s \equiv r' \pmod{\mathfrak{m}_\mathfrak{p}^n}$, so we have

$$\phi(r') = \frac{r}{s} + \mathfrak{m}_\mathfrak{p}^n.$$

Since $r/s \in R_\mathfrak{p}$ was arbitrary, this shows surjectivity. Thus ϕ is an isomorphism. □

14.3 Dedekind Domains and Localization

Lemma 14.3. *If R is a Noetherian domain, then so is $S^{-1}R$.*

Proof. The key observation is that every ideal of $S^{-1}R$ is of the form $S^{-1}I$ for some ideal I of R (check this as an exercise). So if I is generated by $x_1, \ldots, x_r$, then $S^{-1}I$ is generated by $x_1/1, \ldots, x_r/1$. □

Lemma 14.4. *If R is integrally closed, then $S^{-1}R$ is also integrally closed.*

Proof. Suppose $\alpha = a/b \in K$ satisfies a monic polynomial $f \in (S^{-1}R)[x]$. Then we need to show that $\alpha \in S^{-1}R$. Write

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0, \quad a_i = \frac{r_i}{s_i} \in S^{-1}R.$$

Let $s = s_0 s_1 \ldots s_{n-1}$ and multiply the equation $f(\alpha) = 0$ by s^n to get

$$(s\alpha)^n + a_{n-1}s(s\alpha)^{n-1} + \cdots + a_1 s^{n-1}(s\alpha) + a_0 s^n = 0.$$

The coefficients $a_{n-1}s, \ldots, a_0 s^n$ are in R, so $s\alpha$ is integral over R. But R is integrally closed, so $s\alpha \in R$. Since $s \in S$, we have $\alpha \in S^{-1}R$, which proves that $S^{-1}R$ is integrally closed. □

Proposition 14.2. *If R is a Dedekind domain and S is a multiplicative set, then $S^{-1}R$ is either a Dedekind domain or a field.*

Proof. From the above lemmas, it suffices to show $\dim(S^{-1}R) \leq 1$. There is an bijection from chains of prime ideals in $S^{-1}R$ to chains of prime ideals in R disjoint from S, so $\dim(S^{-1}R) \leq \dim R = 1$. □

Corollary 14.0.3. *If R is Dedekind, then $R_\mathfrak{p}$ is a PID for every nonzero prime ideal $\mathfrak{p}$.*

Proof. Note that $R_\mathfrak{p}$ is a local Dedekind ring with prime ideals (0) and $\mathfrak{m}_\mathfrak{p}$. By unique factorization, every nonzero ideal of $R_\mathfrak{p}$ is of the form $\mathfrak{m}_\mathfrak{p}^k$. So it suffices to show that $\mathfrak{m}_\mathfrak{p}$ is principal.

To do this, choose any $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$, and we claim that $\mathfrak{m}_\mathfrak{p} = \pi R_\mathfrak{p}$. Since $\pi R_\mathfrak{p}$ is an ideal, we have $\pi R_\mathfrak{p} = \mathfrak{m}_\mathfrak{p}^k$ for some $k \geq 1$. If $k \geq 2$, then $\pi \in \mathfrak{m}_\mathfrak{p}^2 \cap R = (\mathfrak{m}_\mathfrak{p} \cap R)^2 = \mathfrak{p}^2$, a contradiction. So $k = 1$. □

Definition 14.2. A local PID is called a *discrete valuation ring (DVR)*.

Lecture 15

Feb. 25 — Localization, Part 2

15.1 Valuations

Example 15.0.1. Recall that $R_{\mathfrak{p}}$ is a local PID, also known as a discrete valuation ring. Consider

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} : p \nmid b \right\} \subseteq \mathbb{Q}.$$

There is a *p-adic valuation* $v_p : \mathbb{Z}_{(p)} \to \mathbb{N} \cup \{\infty\}$ given by $v_p(x) = k$ if $x = p^k \cdot a/b$ where $a, b \in \mathbb{Z}$, $p \nmid a$, $p \nmid b$, and $v_p(0) = \infty$. Now v_p extends to $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$, and we can recover $\mathbb{Z}_{(p)}$ as

$$\mathbb{Z}_{(p)} = \{x \in \mathbb{Q} : v_p(x) \geq 0\}.$$

This is known as the *valuation ring* associated to v_p. This is discrete since $\mathbb{Z} \cup \{\infty\}$ is discrete.

Definition 15.1. A *(real) valuation* on a field k is a function $v : k \to \mathbb{R} \cup \{\infty\}$ such that

- $v(x) = \infty$ if and only if $x = 0$;
- $v(ab) = v(a) + v(b)$;
- $v(a + b) \geq \min\{v(a), v(b)\}$.

Given such a valuation v, there *valuation ring associated to* v is $\mathcal{O}_v = \{x \in k : v(x) \geq 0\}$.

Lemma 15.1. *For all $x \in k$, either $x \in \mathcal{O}_v$ or $x^{-1} \in \mathcal{O}_v$.*

Definition 15.2. A *valuation ring* is a subring $\mathcal{O}$ of a field k such that for all $x \in k$, $x \in \mathcal{O}$ or $x^{-1} \in \mathcal{O}$.

15.2 Dedekind Domains and Localization, Continued

Lemma 15.2. *If R is an integral domain, then*

$$R = \bigcap_{\mathfrak{p} \text{ prime}} R_{\mathfrak{p}} = \bigcap_{\mathfrak{m} \text{ maximal}} R_{\mathfrak{m}}.$$

Proof. Since every maximal ideal is prime, we prove the statement for maximal ideals. We need to show that $\bigcap_{\mathfrak{p}} R_{\mathfrak{p}} \subseteq R$. Choose $a/b \in \bigcap_{\mathfrak{p}} R_{\mathfrak{p}}$. Define the ideal

$$I = \{y \in R : ay \in bR\}$$

We will show that $I = R$, which implies that $a \in bR$ and thus $a/b \in R$ since $1 \in I$. Check as an exercise that I is indeed an ideal. Now since $a/b \in R_{\mathfrak{p}}$, we can write $a/b = x/y$ with $x, y \in R$ and $y \notin \mathfrak{p}$. Then

$ay = bx$, so $y \in I$. Since $y \notin \mathfrak{p}$, this means that $I \not\subseteq \mathfrak{p}$. We can do this for every maximal ideal $\mathfrak{p}$. But every $I \neq R$ is contained in a maximal ideal, so we must have $I = R$. □

Theorem 15.1. *If R is a Noetherian integral domain, then R is Dedekind if and only if $R_\mathfrak{p}$ is a PID for every nonzero prime ideal $\mathfrak{p}$ of R.*

Proof. ($\Rightarrow$) This was Corollary 14.0.3.

($\Leftarrow$) The tricky part to show is that R is integrally closed. This part follows from Lemma 15.2 since the intersection of integrally closed subrings is again integrally closed. □

15.3 S-Integers and S-Units

Definition 15.3. Let S be a finite set of nonzero prime ideals in a domain R and $K = \operatorname{Frac} R$. Define

$$R^S = \left\{ \frac{x}{y} \in K : x, y \in R,\ y \notin \mathfrak{p} \text{ for all } \mathfrak{p} \notin S \right\} = T^{-1}R,$$

where $T = \{x \in R : x \notin \bigcup_{\mathfrak{p} \notin S} \mathfrak{p}\}$.

Remark. If R is Dedekind, this means (y) is divisible only by primes in S.

Example 15.3.1. Let $S = \{(2), (3)\} \subseteq \operatorname{Spec} \mathbb{Z}$. Then

$$\mathbb{Z}^S = \left\{ \frac{x}{y} \in \mathbb{Q} : x, y \in \mathbb{Z},\ y = \pm 2^a 3^b \right\}.$$

In some sense, $\mathbb{Z}_{(2)}$ is close to $\mathbb{Q}$ while $\mathbb{Z}^{(2)}$ is close to $\mathbb{Z}$. Note that $(\mathbb{Z}^{(2)})^\times = \pm\{2^k\}$, which is of rank 1.

Remark. The following are some facts and definitions regarding R^S:

- R^S is Dedekind.
- $\operatorname{Cl}(R^S)$ is finite.
- $(R^S)^\times$ is finitely generated of rank $|S| + r_1 + r_2 - 1$.

Exercise 15.1. Let K be a number field, $R = \mathcal{O}_K$, and S a finite set of nonzero prime ideals. Show that

$$1 \longrightarrow R^\times \longrightarrow (R^S)^\times \longrightarrow \bigoplus_{\mathfrak{p} \in S} (K^\times / R_\mathfrak{p}^\times) \longrightarrow \operatorname{Cl}(R) \longrightarrow \operatorname{Cl}(R^S) \longrightarrow 0$$

is an exact sequence, where $K^\times / R_\mathfrak{p}^\times \cong \mathbb{Z}$.

Remark. Note that the above shows that $\operatorname{Cl}(R^S)$ is in fact a quotient of $\operatorname{Cl}(R)$, hence it must be finite.

Proposition 15.1. *If K is a number field, then there exists a finite set S of nonzero prime ideals such that $\mathcal{O}_K^S$ is a PID (equivalently, $\operatorname{Cl}(\mathcal{O}_K^S) = \{0\}$).*

Proof. There is a map $\rho : \operatorname{Cl}(R) \to \operatorname{Cl}(R^S)$ given by $[I] \mapsto [IR^S]$, which one can verify as an exercise is surjective. Let $I_1, \ldots, I_t$ be ideals which generate $\operatorname{Cl}(R)$. Define

$$S = \text{all prime ideals of } R \text{ dividing some } I_k.$$

For $\mathfrak{p} \in S$, we have $\mathfrak{p}R^S = (1)$. So $\rho([I_k]) = 0$ for all k. Thus we must have $\operatorname{Cl}(R^S) = 0$. □

Remark. The above proposition says that we may get a PID $\mathcal{O}_K^S$ in place of $\mathcal{O}_K$ (which is often not a PID), at the cost of increasing the rank of the unit group by $|S|$.

15.4 Applications to Elliptic Curves

Theorem 15.2 (Siegel)**.** *Let K be a number field and S a finite set of nonzero primes in $\mathcal{O}_K$. Let $f(x) \in K[x]$ be a separable polynomial of degree ≥ 3. Then the Diophantine equation*

$$Y^2 = f(X)$$

has only finitely many solutions with $X, Y \in \mathcal{O}_K^S$. (As a special case, this holds when $S = \varnothing$, so that $\mathcal{O}_K^S = \mathcal{O}_K$. In particular, if $K = \mathbb{Q}$ and $S = \varnothing$, then $\mathcal{O}_K^S = \mathbb{Z}$. The case $\deg f = 3$ is an elliptic curve.)

Proof. We will use the following result without proof:

> **Theorem** (Siegel, Mahler)**.** Let K, S as before. Then the equation $x + y = 1$ has only finitely many solutions with $x, y \in (\mathcal{O}_K^S)^\times$.[1]

Without loss of generality, assume that f splits over K (by enlarging K if necessary), so

$$f(X) = a(X - \alpha_1) \dots (X - \alpha_n), \quad a, \alpha_j \in K$$

for distinct $\alpha_1, \dots, \alpha_n$ and $n \geq 3$. Let $K^S = (\mathcal{O}_K^S)^\times$. By enlarging S if necessary, we can assume:

1. $a \in K^S$, $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K^S$;
2. $\alpha_i - \alpha_j \in K^S$ for all $i \neq j$;
3. $\mathcal{O}_K^S$ is a PID.

By Dirichlet's S-unit theorem, K^S is finitely generated, and so $K^S/(K^S)^2$ is finite. So if

$$L = \text{compositum of } K(\sqrt{u}) \text{ for all } u \in K^S,$$

then L/K is finite. Now define the set

$$T = \text{prime ideals of } \mathcal{O}_L \text{ containing some element of } S.$$

We will work with $\mathcal{O}_L^T$, the T-integers in $\mathcal{O}_L$. Now suppose $y^2 = f(x)$ with $x, y \in \mathcal{O}_K^S$, so that

$$y^2 = a(x - \alpha_1) \dots (x - \alpha_n).$$

Then any prime ideal $\mathfrak{p}$ of $\mathcal{O}_K^S$ divides at most one of these terms (otherwise it divides $\alpha_i - \alpha_j$ for $i \neq j$, which we assumed lies in K^S). Since $\mathfrak{p}$ must divides y^2, it must divide y^2 twice, and since

$$(x - \alpha_1) \dots (x - \alpha_n) = a^{-1} y^2,$$

we must have $x - \alpha_i = u_i a_i^2$ for each i, where $u_i \in K^S$ and $a_i \in \mathcal{O}_K^S$. Then $(x - \alpha_i) = \mathfrak{a}_i^2$, where $\mathfrak{a}_i = (a_i)$. Let $u_i = v_i^2$ with $v_i \in L^T$, then

$$x - \alpha_i = v_i^2 a_i^2 = w_i^2, \quad w_i \in \mathcal{O}_L^T.$$

[1] For instance, $x + y = 1$ has finitely solutions with $x, y \in \pm\{2^a 3^b\}$. This is not obvious, e.g. $1 = 3^2 - 2^3 = 3 - 2 = 2^2 - 3 = \dots$.

The trick is then the following: We can write

$$\alpha_j - \alpha_i = w_i^2 - w_j^2 = (w_i - w_j)(w_i + w_j).$$

Since $\alpha_j - \alpha_i \in K^S$, we must have $w_i - w_j, w_i + w_j \in L^T$. Because $n \geq 3$, we have *Siegel's identities*:

$$\frac{w_1 - w_2}{w_1 - w_3} + \frac{w_2 - w_3}{w_1 - w_3} = 1 \quad \text{and} \quad \frac{w_1 + w_2}{w_1 - w_3} - \frac{w_2 + w_3}{w_1 - w_3} = 1.$$

All of the above quotients lie in L^T, so there are only finitely many choices for the quotients by the theorem of Siegel and Mahler. One can show that there are then only finitely many choices for w_1, hence there can only be finitely many choices for $x = \alpha_1 + w_1^2$, since α_1 is fixed. □

Lecture 16

Feb. 27 — Factorization and Galois Theory

16.1 Factorization of Ideals in Relative Extensions

Remark. Let L/K be a finite extension of number fields with $[L:K] = n$. Note that we also have an extension of number rings of the form $\mathcal{O}_K \subseteq \mathcal{O}_L$.

Exercise 16.1. Show the following:

- $\mathcal{O}_L \cap K = \mathcal{O}_K$;
- $\mathcal{O}_L$ is a finitely generated $\mathcal{O}_K$-module, generated by n elements.

Remark. Let L/K be a finite separable extension of fields of degree n, and let B, A be Dedekind domains such that $A \subseteq K$ and $A \subseteq B \subseteq L$. We will assume that

- B is integral over A;
- $B/\mathfrak{q}$ and $A/\mathfrak{p}$ are finite fields for all nonzero prime ideals $\mathfrak{q}, \mathfrak{p}$.

Definition 16.1. A prime ideal $\mathfrak{q}$ of B *lies over* $\mathfrak{p}$ of A if $\mathfrak{q}$ contains $\mathfrak{p}$ (if and only if $\mathfrak{q} | \mathfrak{p}B$).

Lemma 16.1. *In the above setting, $\mathfrak{q}$ lies over $\mathfrak{p}$ if and only if $\mathfrak{q} \cap A = \mathfrak{p}$.*

Proof. The key point is that if $\mathfrak{q} \supseteq \mathfrak{p}$, then $\mathfrak{q} \cap A$ is a prime ideal containing $\mathfrak{p}$. But A is Dedekind, so it is 1-dimensional, so we must have $\mathfrak{q} \cap A = \mathfrak{p}$. □

Lemma 16.2. *If $\mathfrak{p}$ is a nonzero prime ideal of A, then $\mathfrak{p}B \neq B$, i.e. $\mathfrak{p}B$ is a proper ideal of B.*

Proof. Choose $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$. Since $\pi \in \mathfrak{p}$, we have $\pi A = \mathfrak{p}\mathfrak{a}$ for some ideal $\mathfrak{a}$ with $\mathfrak{p} \nmid \mathfrak{a}$. Thus $(\mathfrak{p}, \mathfrak{a}) = 1$, so

$$1 = b + a, \quad b \in \mathfrak{p}, a \in \mathfrak{a}.$$

Suppose otherwise that $\mathfrak{p}B = B$. Then $aB = a\mathfrak{p}B \subseteq \pi B$. This means that $a = \pi x$ for some $x \in B$, so $x = a/\pi \in K$. But then $x \in B \cap K = A$, so $a \in \pi A \subseteq \mathfrak{p}$. This implies $1 = b + a \in \mathfrak{p}$, a contradiction. □

Theorem 16.1. *Let $\mathfrak{p} \subseteq A$ be a prime ideal. If $\mathfrak{p}B = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r} \subseteq B$, then*

$$\sum_{i=1}^{r} e(\mathfrak{q}_i/\mathfrak{p}) f(\mathfrak{q}_i/\mathfrak{p}) = [L:K],$$

where $e(\mathfrak{q}_i/\mathfrak{p}) = e_i$ and $f(\mathfrak{q}_i/\mathfrak{p}) = [B/\mathfrak{q}_i : A/\mathfrak{p}]$.

Proof. Let $S = A \setminus \mathfrak{p} \subseteq A \subseteq B$. We claim that we can replace B by $S^{-1}B = B'$ and A by $S^{-1}A = A'$ without changing any of the above numerical invariants (e or f). This is because we have $A/\mathfrak{p} \cong A'/\mathfrak{p}'$ and $B/\mathfrak{q}' \cong B'/\mathfrak{q}_i'$, and if $\mathfrak{p}B = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$, then $\mathfrak{p}B' = \mathfrak{q}_1'^{e_1} \cdots \mathfrak{q}_r'^{e_r}$.

Then A' is a PID, so the same argument we used over $\mathbb{Z}$ will work. □

Corollary 16.1.1. *Let $\mathfrak{p} \subseteq \mathcal{O}_K$ be a prime ideal. If $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r} \subseteq \mathcal{O}_L$, then*

$$\sum_{i=1}^{r} e(\mathfrak{q}_i/\mathfrak{p}) f(\mathfrak{q}_i/\mathfrak{p}) = n,$$

where $e(\mathfrak{q}_i/\mathfrak{p}) = e_i$ and $f(\mathfrak{q}_i/\mathfrak{p}) = [\mathcal{O}_L/\mathfrak{q}_i : \mathcal{O}_K/\mathfrak{p}]$.

16.2 Connections to Galois Theory

Proposition 16.1. *If L/K is Galois, then $\mathrm{Gal}(L/K)$ acts transitively on the set $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_r\}$ of prime ideals of B lying over $\mathfrak{p}$.*

Proof. It is clear to see that $\mathrm{Gal}(L/K)$ acts on $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_r\}$: If $\mathfrak{q} \cap A = \mathfrak{p}$ and $\sigma \in \mathrm{Gal}(L/K)$, then

$$\sigma(\mathfrak{q}) \cap A = \sigma(\mathfrak{q} \cap A) = \sigma(\mathfrak{p}) = \mathfrak{p}.$$

To see that the action is transitive, let $\mathfrak{q}_i, \mathfrak{q}_j$ be two distinct prime ideals of B lying over $\mathfrak{p}$, and assume otherwise that $\mathfrak{q}_i \neq \mathfrak{q}_j$ for every $\sigma \in \mathrm{Gal}(L/K)$. By the Chinese remainder theorem, we can solve

$$x \equiv 0 \pmod{\mathfrak{q}_j}, \quad x \equiv 1 \pmod{\sigma(\mathfrak{q}_i)}$$

for all $\sigma \in \mathrm{Gal}(L/K)$, with $x \in B$. Now we have

$$N_{L/K}(x) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x) \in B \cap K = A.$$

Thus $N_{L/K}(x) \in \mathfrak{q}_j \cap A = \mathfrak{p}$. Note that $x \notin \sigma(\mathfrak{q}_i)$ for all σ, so $\sigma(x) \notin \mathfrak{q}_i$ for all σ. Since $\mathfrak{p}B \subseteq \mathfrak{q}_i$,

$$\prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x) \in \mathfrak{p}B \subseteq \mathfrak{q}_i,$$

which implies $\sigma(x) \in \mathfrak{q}_i$ for some $\sigma \in \mathrm{Gal}(L/K)$ since $\mathfrak{q}_i$ is a prime ideal. Contradiction. □

Corollary 16.1.2. *If L/K is Galois, then*

$$e(\mathfrak{q}_1/\mathfrak{p}) = \cdots = e(\mathfrak{q}_r/\mathfrak{p}) = e \quad \textit{and} \quad f(\mathfrak{q}_1/\mathfrak{p}) = \cdots = f(\mathfrak{q}_r/\mathfrak{p}) = f,$$

so we have the equality $efr = n$.

Proof. Applying σ to $\mathfrak{p}B = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$, we have $\mathfrak{p}B = \sigma(\mathfrak{q}_1)^{e_1} \cdots \sigma(\mathfrak{q}_r)^{e_r}$. For any i, j, we can find σ with $\sigma(\mathfrak{q}_i) = \mathfrak{q}_j$, so by unique factorization we have $e_i = e_j$. For f, note that we have an induced map

$$\sigma : B/\mathfrak{q}_i \to B/\mathfrak{q}_j.$$

Since σ is an automorphism, it is easy to see that σ is an isomorphism, so that $f_i = f_j$. □

Remark. Let L/K be Galois, and B, A be Dedekind domains with $A \subseteq K$ and $A \subseteq B \subseteq L$. Fix a prime ideal $\mathfrak{p} \subseteq A$ and let $S = \{\mathfrak{q}_1, \dots, \mathfrak{q}_r\}$ be the set of prime ideals lying over $\mathfrak{p}$. Then $G = \mathrm{Gal}(L/K)$ acts transitively on S, with $|G| = n = efr$ and $|S| = r$.

So by the orbit-stabilizer theorem, the stabilizer of any $\mathfrak{q}_i$ has order ef. Fix some $\mathfrak{q} \in S$, define the *decomposition group* $D_{\mathfrak{q}} = D_{\mathfrak{q}/\mathfrak{p}}$ of $\mathfrak{q}/\mathfrak{p}$ to be the stabilizer of $\mathfrak{q}$, i.e.

$$D_{\mathfrak{q}/\mathfrak{p}} = \{\sigma \in G : \sigma(\mathfrak{q}) = \mathfrak{q}\}.$$

Let $\ell = B/\mathfrak{q}$ and $k = A/\mathfrak{p}$, so that $|\mathrm{Gal}(\ell/k)| = f$.

Theorem 16.2 (Frobenius)**.** *There is a natural surjective homomorphism*

$$D_{\mathfrak{q}/\mathfrak{p}} \twoheadrightarrow \mathrm{Gal}(\ell/k).$$

Proof. Let $\sigma \in D_{\mathfrak{q}/\mathfrak{p}}$. We want to define $\overline{\sigma} \in \mathrm{Gal}(\ell/k)$. Take $\overline{x} \in \ell$ and lift it to some $x \in B$. Define

$$\overline{\sigma}(\overline{x}) = \sigma(x) \bmod q.$$

To see that this is well-defined, note that if x_1, x_2 are two lifts, then $x_1 - x_2 \in \mathfrak{q}$, so

$$\sigma(x_1) - \sigma(x_2) \in \sigma(\mathfrak{q}) = \mathfrak{q}.$$

Let $\overline{\alpha}$ be a primitive element for ℓ/k (recalling that we are assuming ℓ/k is finite separable). To prove surjectivity, it suffices to show that every Galois conjugate of $\overline{\alpha}$ is of the form $\overline{\sigma}(\overline{\alpha})$ for some $\sigma \in D_{\mathfrak{q}/\mathfrak{p}}$. Let $\alpha \in B$ be a lift of $\overline{\alpha}$ such that $\alpha \in \mathfrak{q}'$ for all $\mathfrak{q}' \in S$, $\mathfrak{q}' \neq \mathfrak{q}$. This follows by the Chinese remainder theorem, which gives a solution to the following system of congruences:

$$\alpha \equiv \overline{\alpha} \pmod{\mathfrak{q}}, \quad \alpha \equiv 0 \pmod{\mathfrak{q}'} \text{ for } \mathfrak{q}' \neq \mathfrak{q}.$$

Let $f \in A[x]$ be the minimal polynomial of α and $\overline{g} \in k[x]$ be the minimal polynomial of $\overline{\alpha}$. We have

$$f(x) = \prod_{\sigma \in H} (x - \sigma(\alpha))$$

for some subset $H \subseteq G$. Let $H' = H \cap D_{\mathfrak{q}}$. We claim that $\sigma(\alpha) \in \mathfrak{q}$ whenever $\sigma \in G$ and $\sigma \notin D_{\mathfrak{q}}$. This is because $\sigma \notin D_{\mathfrak{q}}$ gives $\sigma^{-1} \notin D_{\mathfrak{q}}$, so $\sigma^{-1}(\mathfrak{q}) \neq \mathfrak{q}$, hence $\alpha \in \sigma^{-1}(\mathfrak{q})$ and $\sigma(\alpha) \in \mathfrak{q}$. Let $\overline{f} = f \bmod \mathfrak{q}$, so

$$\overline{f}(x) = \prod_{\sigma \in H} (x - \overline{\sigma(\alpha)}) = \prod_{\sigma \in H'} (x - \overline{\sigma(\alpha)}) \prod_{\sigma \notin H'} (x - \overline{\sigma(\alpha)}) = x^m \prod_{\sigma \in H'} (x - \overline{\sigma}(\overline{\alpha})).$$

So all nonzero roots of $\overline{f}(x)$ have the form $\overline{\sigma}(\overline{\alpha})$ for some $\sigma \in D_{\mathfrak{q}}$. Finally, note that

$$\overline{f}(\overline{\alpha}) = \overline{f(\alpha)} = 0,$$

so $\overline{g} | \overline{f}$. Note that 0 is not a root of $\overline{g}$ (since $\overline{g}$ is the minimal polynomial of a nonzero element), so

$$\overline{g} \mid \prod_{\sigma \in H'} (x - \overline{\sigma(\alpha)}).$$

This shows the result for any root of $\overline{g}$, which completes the proof. □

Corollary 16.2.1. *Let the* inertia group $I_{\mathfrak{q}/\mathfrak{p}}$ *be the kernel of the above map. Then* $|I_{\mathfrak{q}/\mathfrak{p}}| = e$.

Proof. This is by the first isomorphism theorem, since $|D_{\mathfrak{q}/\mathfrak{p}}| = ef$ and $|\mathrm{Gal}(\ell/k)| = f$. □

Lecture 17

Mar. 4 — More Galois Theory

17.1 Frobenius Elements

Remark. Recall that last class, we showed that $|D_\mathfrak{q}| = e_\mathfrak{q} f_\mathfrak{q} = ef$, $|I_\mathfrak{q}| = e_\mathfrak{q} = e$, and $D_\mathfrak{q}/I_\mathfrak{q} \cong \mathrm{Gal}(\ell/k)$. This is useful because $\mathrm{Gal}(L/K)$ is in general a complicated group; in fact, any finite group can arise as $\mathrm{Gal}(L/K)$ for some extension L/K. On the other hand, ℓ, k are finite fields, and thus $\mathrm{Gal}(\ell/k)$ is cyclic. In particular, $\mathrm{Gal}(\ell/k) = \langle \tau \rangle$ where $\tau(x) = x^{|k|}$ is the *Frobenius automorphism.*

Corollary 17.0.1. *If $\mathfrak{q}/\mathfrak{p}$ is unramified (i.e. $p \nmid \Delta_{L/K}$, or $e_\mathfrak{q} = 1$), then $D_\mathfrak{q}$ is cyclic.*

Definition 17.1. The generator of $D_\mathfrak{q}$ is called the *Frobenius element* and is denoted $\mathrm{Frob}_\mathfrak{q}$.[1]

Remark. What is the dependence of $\mathrm{Frob}_\mathfrak{q}$ on the choice of $\mathfrak{q}/\mathfrak{p}$?

Lemma 17.1. *Suppose $\mathfrak{q}, \mathfrak{q}'$ are prime ideals of $\mathcal{O}_L$ lying over $\mathfrak{p}$. Choose $\sigma \in G$ such that $\sigma\mathfrak{q} = \mathfrak{q}'$ Then*

$$D_{\mathfrak{q}'} = \sigma D_\mathfrak{q} \sigma^{-1} \quad \textit{and} \quad I_{\mathfrak{q}'} = \sigma I_\mathfrak{q} \sigma^{-1}.$$

If $\mathfrak{q}/\mathfrak{p}$ is unramified, then so is $\mathfrak{q}'/\mathfrak{p}$ and $\mathrm{Frob}_{\mathfrak{q}'} = \sigma \,\mathrm{Frob}_\mathfrak{q}\, \sigma^{-1}$.

Proof. We will prove the statement only for $D_{\mathfrak{q}'}$, the rest is left as an exercise. We can write

$$\begin{aligned} D_{\mathfrak{q}'} = \{\tau \in G : \tau\mathfrak{q}' = \mathfrak{q}'\} = \{\tau \in G : \tau\sigma\mathfrak{q} = \sigma\mathfrak{q}\} = \{\tau \in G : (\sigma^{-1}\tau\sigma)\mathfrak{q} = \mathfrak{q}\} \\ = \sigma\{\sigma^{-1}\tau\sigma : \tau \in G\}\sigma^{-1} = \sigma D_\mathfrak{q} \sigma^{-1}. \end{aligned}$$

The proof of the other statements are similar. □

Remark. When L/K is Galois and $\mathfrak{p}$ is unramified, the above lemma allows us to define the Frobenius conjugacy class $\mathrm{Frob}_\mathfrak{p} \subseteq \mathrm{Gal}(L/K)$ (the set of all $\mathrm{Frob}_\mathfrak{q}$ where $\mathfrak{q}/\mathfrak{p}$ is unramified).

Example 17.1.1. Consider $K/\mathbb{Q}$, let $G = \mathrm{Gal}(K/\mathbb{Q})$ and Frob_p be the conjugacy class corresponding to a prime p not dividing Δ_K. The *Chebotarev density theorem* then says that if we fix a conjugacy class $C \subseteq G$, then the density of primes p with $\mathrm{Frob}_p = C$ is $|C|/|G|$.

Example 17.1.2. Consider $K = \mathbb{Q}(\zeta_n)$, so $G \cong (\mathbb{Z}/n\mathbb{Z})^\times$ is abelian (so that the Frobenius conjugacy classes are singletons and can therefore be identified with elements). If we fix $\sigma_a \in G$ with $(a, n) = 1$, then we will show shortly that $\mathrm{Frob}_p = \sigma_p$ for $p \nmid n$. So if we fix a conjugacy class (element) $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, then $\mathrm{Frob}_p = a$ if and only if $p \equiv a \pmod{n}$. The Chebotarev density theorem then says that the density of such p is $1/\phi(n)$ (this is Dirichlet's theorem on primes in arithmetic progressions).

[1] Note that $\mathrm{Frob}_\mathfrak{q}$ depends on the choice of $\mathfrak{q}$ and only makes sense when $\mathfrak{q}$ is unramified.

17.2 Fixed Fields

Remark. Let L/K be Galois and fix $\mathfrak{q}/\mathfrak{p}$. Let $D = D_{\mathfrak{q}/\mathfrak{p}}$ and $I = I_{\mathfrak{q}/\mathfrak{p}}$. Then for an intermediate field $K \subseteq K' \subseteq L$ (e.g. $K = L^H$, the fixed field of some subgroup $H \subseteq G$), we have some $\mathfrak{p}'$ lying over $\mathfrak{p}$:

$$\begin{array}{ccc} L & & \mathfrak{q} \\ | & & | \\ L^H = K' & & \mathfrak{p}' = \mathfrak{q} \cap \mathcal{O}_{K'} \\ | & & | \\ K & & \mathfrak{p} \end{array}$$

Lemma 17.2. *Let $D' = D_{\mathfrak{q}/\mathfrak{p}'}$ and $I' = I_{\mathfrak{q}/\mathfrak{p}'}$. Then $D' = D \cap H$ and $I' = I \cap H$.*

Proof. We only prove the statement for D', the other for I' is similar. Note that

$$D = \text{stabilizer of } \mathfrak{q} \text{ in } G \quad \text{and} \quad D' = \text{stabilizer of } \mathfrak{q} \text{ in } H,$$

from which it is clear that $D' = D \cap H$. □

Remark. The following is a fact from Galois theory that we will use:

If H, H' are subgroups of $G = \mathrm{Gal}(L/K)$, then $L^{H \cap H'} = L^H L^{H'}$.

In the above, $L^H L^{H'}$ is compositum of L^H and $L^{H'}$.

Proposition 17.1. *Call L^D the* decomposition field *and L^I the* inertia field. *Then*

1. *L^D is the largest intermediate field K' such that $e(\mathfrak{p}'/\mathfrak{p}) = f(\mathfrak{p}'/\mathfrak{p}) = 1$;*
2. *L^I is the largest intermediate field K' such that $e(\mathfrak{p}'/\mathfrak{p}) = 1$.*

Proof. Again, we only prove the statement for L^D. We first claim that if $K' = L^D$, then we in fact have $e(\mathfrak{p}'/\mathfrak{p}) = f(\mathfrak{p}'/\mathfrak{p}) = 1$. By the lemma, we have $D' = D$, so we have

$$e(\mathfrak{q}/\mathfrak{p}')f(\mathfrak{q}/\mathfrak{p}') = e(\mathfrak{q}/\mathfrak{p})f(\mathfrak{q}/\mathfrak{p}).$$

But by a homework problem, e and f are multiplicative in towers, so $e(\mathfrak{p}'/\mathfrak{p}) = f(\mathfrak{p}'/\mathfrak{p}) = 1$.

To see that it is the largest such extension, let K' be any intermediate field with $e(\mathfrak{p}'/\mathfrak{p}) = f(\mathfrak{p}'/\mathfrak{p}) = 1$. We want to show that $K' \subseteq L^D$. We can write $K' = L^H$ for some $H \leq G$. Then $D' = D \cap H$, so

$$L^{D'} = L^D K'$$

by Galois theory. The hypothesis implies $|D| = |D'|$, which combined with $D' \subseteq D$ implies $D' = D$. Then we have $L^D = L^{D'} = L^D K'$, which implies that $K' \subseteq L^D$. This proves the result. □

Corollary 17.0.2. *Let $\mathfrak{p} \subseteq \mathcal{O}_K \subseteq K \subseteq M, M' \subseteq L$ (not necessarily Galois). Then $\mathfrak{p}$ splits completely (resp. is unramified) in both M and M' if and only if $\mathfrak{p}$ splits completely (resp. is unramified) in MM'.*

Proof. Take a Galois closure L' of L/K. If $\mathfrak{p}$ splits completely in L, then $e = 1$ in both K and L, so $e = 1$ in M, M' as well since e is multiplicative in towers. On the other hand, if $\mathfrak{p}$ splits completely in both M and M', then $(L')^D$ contains both M and M', so $MM' \subseteq (L')^D$ and $\mathfrak{p}$ splits completely in MM'. □

Corollary 17.0.3. *Suppose L/K is finite (but not necessarily Galois). Let M be the Galois closure of L/K. Then $\mathfrak{p}$ is unramified (resp. splits completely) in L if and only if $\mathfrak{p}$ is unramified (resp. splits completely) in M.*

Proof. This is because M is the compositum of L^σ over $\sigma \in \mathrm{Gal}(M/K)$. □

Remark. The above corollaries imply that we can reduce many questions to the Galois case (many extensions of number fields, e.g. $\mathbb{Q}(\sqrt[3]{2})$, are not Galois, but we can still work with them by embedding them in a Galois closure).

17.3 A Non-Monogenic Number Ring

Remark. We will show that if $K = \mathbb{Q}(\sqrt{7}, \sqrt{10})$, then $\mathcal{O}_K$ is not monogenic, i.e. there is no $\alpha \in \mathcal{O}_K$ such that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. In fact, we will show that for all $\alpha \in \mathcal{O}_K$ such that $K = \mathbb{Q}(\alpha)$, we have $3 \mid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$. In particular, this means that Kummer's theorem will not help us factor (3) in $\mathcal{O}_K$, even when trying some change of variables.

We will actually do this more generally: Let $K_1 = \mathbb{Q}(\sqrt{d_1})$ and $K_2 = \mathbb{Q}(\sqrt{d_2})$ with $d_1, d_2 \equiv 1 \pmod 3$. Kummer's theorem says that 3 splits completely in K_i $(i = 1, 2)$ if and only if

$$x^2 - d_i \equiv x^2 - 1 \pmod 3$$

splits into linear factors (which it does). By our previous results, this implies that 3 splits completely in the compositum $K = K_1 K_2$.

Now suppose otherwise that $\mathcal{O}_K = \mathbb{Z}[\alpha]$ (or even $3 \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$). Then Kummer's theorem applies to K as well, so the minimal polynomial f_α of α over $\mathbb{Z}$ factors into distinct linear factors mod 3. But $\deg f_\alpha = 4$ and there are only 3 linear polynomials in $\mathbb{F}_3[x]$, so this cannot possibly happen.

Lecture 18

Mar. 6 — Factorization in Cyclotomic Fields

18.1 Factorization in Cyclotomic Fields

Remark. Let $\mathbb{Z}[\zeta_m] \subseteq \mathbb{Q}(\zeta_m)$ and $p \nmid m$ prime. We can factor

$$p\mathbb{Z}[\zeta_m] = \mathfrak{p}_1 \dots \mathfrak{p}_r,$$

where $p \nmid m$ implies that the $\mathfrak{p}_i$ are distinct, i.e. $e_i = 1$ for each i. Since $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ is Galois, we have $f_1 = \cdots = f_r = f$ and thus $fr = \phi(m)$.

Proposition 18.1. *In the above situation, we have f = order of $[p]$ in $(\mathbb{Z}/m\mathbb{Z})^\times$.*

Proof. Note that $G = \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$ by the isomorphism

$$\begin{aligned}(\mathbb{Z}/m\mathbb{Z})^\times &\longrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \\ a &\longmapsto (\sigma_a : \zeta_m \mapsto \zeta_m^a).\end{aligned}$$

We have $f = [\mathbb{Z}[\zeta_m]/\mathfrak{p} : \mathbb{F}_p]$, but this is hard to deal with. Instead, Kummer's theorem says that

$$f = \text{degree of any irreducible factor of } \Phi_m \bmod p.$$

Let $g(x)$ be an irreducible factor of $\overline{\Phi_m(x)}$, so that $\deg g = f$. Then $\mathbb{F}_p[x]/(g(x))$ is a finite field of order p^f, so its Galois group over $\mathbb{F}_p$ is generated by $x \mapsto x^p$. By the proof of Kummer's theorem,

$$\mathbb{Z}[\zeta_m]/\mathfrak{p} \cong \mathbb{F}_p[x]/(g(x)),$$

so the Galois group of $\mathbb{F}_p[x]/(g(x))$ is $\mathrm{Gal}(\ell/k)$, where ℓ is $\mathbb{Z}[\zeta_m]/\mathfrak{p}$ and k is $\mathbb{F}_p$. Then $D_\mathfrak{p} \cong \mathrm{Gal}(\ell/k)$ is a subgroup of G, and the generator $x \mapsto x^p$ in $\mathrm{Gal}(\ell/k)$ corresponds to $p \in (\mathbb{Z}/m\mathbb{Z})^\times$. Since ℓ has order p^f (so $x \mapsto x^p$ has order f in $\mathrm{Gal}(\ell/k)$), we see that the order of $[p]$ in $(\mathbb{Z}/m\mathbb{Z})^\times$ is f. □

Example 18.0.1. Let $m = 15$, so that $\phi(15) = 8$. Then

$$\Phi_{15}(x) = \frac{(x^{15}-1)(x-1)}{(x^5-1)(x^3-1)} = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1.$$

Mod 2, we can factor

$$\Phi_{15}(x) \equiv (x^4 + x^3 + 1)(x^4 + x + 1) \pmod 2,$$

and notice that $2^4 \equiv 1 \pmod{15}$. On the other hand, we have $31 \equiv 1 \pmod{15}$ and

$$\Phi_{15}(x) \equiv (x+3)(x+11)(x+12)(x+13)(x+17)(x+21)(x+22)(x+24) \pmod{15}.$$

18.2 Law of Quadratic Reciprocity

Remark. Let p be an odd prime and let $K_p = \mathbb{Q}(\zeta_p)$. Note that since $\mathrm{Gal}(K_p/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$ and p is odd, $\mathrm{Gal}(K/\mathbb{Q})$ is cyclic of even order, hence there is a unique subgroup H of index 2. By Galois theory, this subgroup corresponds to a unique quadratic subfield $L = K_p^H \subseteq K_p$.

Lemma 18.1. *The unique subgroup H of index 2 is the subgroup of squares mod p.*

Proof. Half of the residues mod p are squares, so this is a subgroup of index 2, hence it is H. □

Remark. One way to calculate L is to use Gaussian periods (Gauss sums). We will do this later, and we proceed with a different method for now. Because the ramification index e is multiplicative in towers, and because p is the only prime ramifying in K_p, it follows that p is the only prime ramifying in L.

We know that $L = \mathbb{Q}(\sqrt{d})$ where d is square-free. We have previously seen that

$$\Delta_{\mathbb{Q}(\sqrt{d})} = \begin{cases} d & \text{if } d \equiv 1 \pmod 4, \\ 4d & \text{if } d \equiv 2, 3 \pmod 4. \end{cases}$$

Note that we have to be in the first case since 2 does not ramify in L, and so $d = \pm p$ since d is square-free and p is the only prime dividing it. We also have $d \equiv 1 \pmod 4$, so $d = p^*$, where

$$p^* = (-1)^{(p-1)/2} p = \begin{cases} p & \text{if } p \equiv 1 \pmod 4, \\ -p & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Now suppose that p, q are distinct odd primes (so q is unramified in L). We will figure out how q factors in L, i.e. how $q\mathcal{O}_L$ factors into prime ideals. We will do this in two different ways.

We first use Kummer's criterion. We look at $x^2 - p^* \pmod q$ (note that $q \nmid [\mathcal{O}_L : \mathbb{Z}[\sqrt{p^*}]] = 2$ since q is an odd prime), which splits into linear factors if and only if $(\frac{p^*}{q}) = 1$.

On the other hand, let $\mathfrak{q}$ be a prime ideal of $\mathbb{Z}[\zeta_p]$ lying over q. Let $D = D_{\mathfrak{q}/q} \subseteq (\mathbb{Z}/p\mathbb{Z})^\times$, where D corresponds to $\langle q \rangle$. Then K_p^D is the largest subfield of K_p in which q splits completely (since $K_p/\mathbb{Q}$ is Galois). But $L = K_p^H$, so Galois theory implies that

$$q \text{ splits in } L \iff L \subseteq K_p^D \iff D \subseteq H \iff q \in H \iff \left(\frac{q}{p}\right) = 1.$$

Corollary 18.0.1 (Law of quadratic reciprocity)**.** *Let p, q be distinct odd primes. Then*

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

Proof. Recall Euler's criterion that $(\frac{a}{q}) \equiv a^{(q-1)/2} \pmod q$. Then by the above calculation,

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

which is the desired formula. □

Remark. The above argument can be generalized more readily than other more elementary proofs of quadratic reciprocity. Let L/K be a finite abelian extension of number fields (i.e. $\mathrm{Gal}(L/K)$ is abelian). One can embed L into some analogue M of K_p (this is called a *ray class field*), so $K \subseteq L \subseteq M$.

One then analyzes how $\mathfrak{p}$ factors directly in L/K and also using the $L = M^H$ perspective. This results in *Artin's reciprocity law*, which is a result of *class field theory*. As a subject, class field theory tries to understand the abelian extensions of a number field.

Theorem 18.1 (Hilbert)**.** *Let K be a number field. Then there exists a maximal finite abelian extension H of K which is unramified at all primes (and ∞). Moreover,*

$$\mathrm{Gal}(H/K) \cong \mathrm{Cl}(\mathcal{O}_K).$$

18.3 Gauss Sums

Definition 18.1. Let $\zeta = \zeta_p = e^{2\pi i/p}$. Define the *Gauss sum*

$$g = \sum_{t \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{t}{p}\right) \zeta_p^t.$$

Lemma 18.2. *We have $g^2 = p^*$.*

Proof. We sketch the proof. Define

$$g_a = \sum_{t \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{t}{p}\right) \zeta_p^{at}.$$

Note that we have the identity $g_a = (\frac{a}{p})g$:

$$g = \sum_{b \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{b}{p}\right) \zeta_p^b = \sum_{t \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{at}{p}\right) \zeta_p^{at} = \left(\frac{a}{p}\right) \sum_{t \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{t}{p}\right) \zeta_p^{at}$$

since multiplication by a is a permutation on $(\mathbb{Z}/p\mathbb{Z})^\times$. Now we calculate $\sum_a g_a g_{-a}$ in two different ways:

$$g_a g_{-a} = \left(\frac{a}{p}\right)\left(\frac{-a}{p}\right) g^2 = \left(\frac{-1}{p}\right) g^2,$$

so that $\sum_a g_a g_{-a} = (\frac{-1}{p})(p-1)g^2$. On the other hand, we can also write

$$g_a g_{-a} = \sum_{x,y} \left(\frac{xy}{p}\right) \zeta_p^{a(x-y)},$$

so $\sum_a g_a g_{-a} = \sum_{x,y} (\frac{xy}{p}) \sum_a \zeta_p^{a(x-y)} = p(p-1)$. Comparing the two formulas gives $g^2 = p^*$. □

Proof of Corollary 18.0.1 using Gauss sums. Let p, q be distinct primes. First we have

$$g^q \equiv g_q = \left(\frac{q}{p}\right) g \pmod{q\mathbb{Z}[\zeta_p]},$$

so we have

$$p^*(g^2)^{(q-1)/2} = g^2 (g^2)^{(q-1)/2} = g^{q+1} \equiv \left(\frac{q}{p}\right) g^2 = \left(\frac{q}{p}\right) p^* \pmod{q\mathbb{Z}[\zeta_p]}.$$

Since $(g^2)^{(q-1)/2} = (\frac{p^*}{q})$, comparing the above expressions yields $(\frac{p^*}{q}) = (\frac{q}{p})$, as desired. □

Corollary 18.1.1. *We have* $\mathbb{Q}(\sqrt{p^*}) \subseteq \mathbb{Q}(\zeta_p)$.

Remark. Gauss actually computed the value of g, in addition to g^2. Gauss found that

$$g = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \pmod 4, \\ i\sqrt{p} & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

One can also formulate a similar question for cubes, but the answer is much more complicated.