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[2]It is far from it, and this is likely the mistake that Fermat originally made.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

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 $\alpha_1, \dots, \alpha_n$ 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. $r/s\in\mathbb{Z}$. $\square$

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. $m\alpha\in\mathcal{O}_K$. $\square$

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

$(1 \Rightarrow 2)$ 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.

$(2 \Rightarrow 1)$ 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. $\square$

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. $\square$

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. $\square$

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. $\square$

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 $N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$. $\square$

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. $\square$

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. $\square$

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. $\square$

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

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 $J \in \Sigma$. $\square$

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. $\square$

[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. $\square$

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. $\square$

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

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

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]

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

But $\operatorname{ord}_{\mathfrak{p}}(\gamma) = k$ (since $\gamma \in \mathfrak{p}^k \setminus \mathfrak{p}^{k+1}$), so $\operatorname{ord}_{\mathfrak{p}}(y) \geq 1$. 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 $\operatorname{ord}_{\mathfrak{p}}(\alpha) = \operatorname{ord}_{\mathfrak{p}}(\mathfrak{a})$ 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 $|N(\alpha)| \le M \cdot N(I)$. Equivalently, α satisfies*

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

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 $m^n \le N(I) < (m+1)^n$. Then define the set

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

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

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

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 $\mathfrak{p}_i \ne 0$ 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 $|N(\alpha)| \le M \cdot N(I)$. Now $(\alpha) = IJ$ for some J, so $[J] = [I]^{-1} = C$, and

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

which proves the desired result. $\square$

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

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 $m\mathcal{O}_K$. $\square$

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. $\square$

5.3 Computation of 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 Computations of Rings of Integers

Lemma 6.1. *Let $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$ 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. $\square$

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 $\mathcal{O}_K = \mathbb{Z}[\alpha]$. $\square$

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 $\mathcal{O}_K/\mathfrak{p} \not\cong \mathbb{Z}/p\mathbb{Z}$. 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 mod 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: $x^2 - d$ mod 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 $p(1+ph) = p + p^2 h$ 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 $0 \leq e_i' \leq e_i$. But $n = \sum e_i' f_i = \sum e_i f_i$, so $e_i' = e_i$ for all i, which completes the proof. $\square$

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. $\square$

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 $p | \Delta(g) \equiv \Delta_K$. $\square$

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 Computations 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 $\mathfrak{a} = \mathfrak{q}_1^{e_1} \ldots \mathfrak{q}_r^{e_r}$ 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 $a^p - a$. $\square$

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 ideas for Fermat's last theorem.