Harvard University Math 129

Notes for *Number Fields*

Reuben Stern

Spring Semester 2017

Contents

0.1 Preliminaries

These notes were taken during the Spring semester of 2017, in Harvard's Math 129, *Number Fields*. The course was taught by Mark Kisin, and met Monday/Wednesday/Friday from 12 to 1 pm. Allow me to elucidate the process for taking these notes: I take notes by hand during lecture, which I transfer to LaTeX at night. It is an unfortunate consequence of this method that these notes do not capture the unique lecturing style of the professor. Indeed, I take full responsibility for any errors in exposition or mathematics, but all credit for genuinely clever remarks, proofs, or exposition will be due to the professor (and not to the scribe). In an appendix at the end of this document, you will find the collected homework problems (with solutions). I make no promises regarding the correctness of these solutions; consider yourself warned. Please send any and all corrections to reuben_stern@college.harvard.edu. They will be most appreciated.

0.2 Administrative Stuff

Office hours for Professor Kisin will be Mondays, 1–2 pm, in Science Center 234. Homework will be due on Wednesdays, and posted on the course website. There will be an in-class midterm exam on 3/8; questions on the exam will be almost directly taken from homeworks.

> Kisin: *"I don't believe in exam surprises."*

The textbook for the course is "Algebraic Theory of Numbers" by Pierre Samuel, and a good reference is "Algebraic Number Theory" by Neukirch. In the class, we will be discussing the structure of number fields, and their applications. This includes:

- Unique factorization
- Class groups, unit groups
- Local fields, adeles
- Applications to Diophantine equations mixed in, such as
  1. Fermat's Theorem: if $p \equiv 1 \mod 4$, then $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.
  2. Pell's Equation: if $d \in \mathbb{Z}$ is squarefree, then find the solutions to $a^2 - db^2 = \pm 1$.

1 January 23, 2017

1.1 Characteristic Polynomials

This was the first meeting of the class. We begin by introducing the most critical definition in the course:

Definition 1.1. A **number field** is a field $K \supseteq \mathbb{Q}$ (therefore, char $K = 0$) such that K is finite-dimensional as a $\mathbb{Q}$-vector space.

Lemma 1.2. *If K is a number field and $\alpha \in K$, then there exists a monic polynomial $f \in \mathbb{Q}[x]$ such that $f(\alpha) = 0$.*

Easy Proof. If $d = \dim_{\mathbb{Q}} K$, then the elements $1, \alpha, \alpha^2, \dots, \alpha^d$ must be linearly dependent. Therefore there exist $a_0, a_1, \dots, a_d$ not all zero such that $a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_d\alpha^d = 0$. Let i be the largest integer such that $a_i \neq 0$; we then take

$$f(x) = a_i^{-1}\left(a_0 + a_1x + a_2x^2 + \cdots + a_dx^d\right).$$

This is monic, and $f(\alpha) = 0$, concluding the proof. □

Proof. ("A more learned proof."[1]) Suppose L is any field, V a finite-dimensional L-vector space, and consider an L-linear map $\varphi : V \to V$. Recall[2] the **characteristic polynomial** $P_\varphi(x) \in L[x]$ of φ is a (the) monic polynomial of degree $\dim_L V$, such that $P_\varphi(\varphi) = 0$ (Cayley-Hamilton Theorem). But what exactly do we mean by evaluating the polynomial at an operator? If $P_\varphi(x) = x^n + a_{n-1}x^n + \cdots + a_0$, then $P_\varphi(\varphi) = \varphi^n + a_{n-1}\varphi^{n-1} + \cdots + a_0 \in \mathrm{End}_L(V)$. The statement is then that $P_\varphi(\varphi)$ is the zero endomorphism.

Consider now the $L[x]$-module given by $V \otimes_L L[X]$. If $V \cong L^n$ (with a choice of basis), then

$$V \otimes_L L[x] \cong L[x]^n \qquad \text{(free module with the same basis.)}$$

Look at the map $x - \varphi : V \otimes L[x] \to V \otimes L[x]$. The map x is defined by left-multiplication by x, i.e. $(v \otimes f) \mapsto v \otimes (xf)$, and the map φ is more precisely $\varphi \otimes \mathbf{1}_{L[x]}$.

Kisin: *"If you're a real purist, you refrain from choosing a basis."*

We now define

$$P_\varphi(x) := \det(x - \varphi | V \otimes L[x]),$$

which we can define more precisely as the unique $P \in L[x]$ such that $x - \phi$ is multiplication by P, when acting on $\bigwedge^n(V \otimes L[x])$.

[1] Quote Mark Kisin, 2017.

[2] Kisin (paraphrased): *This is a very pretentious word that mathematicians use.*

Remark 1.3. Everything we just did works just as well for a free, finitely-generated module M over an arbitrary ring R: with $\varphi : M \to M$, we can define $P_\varphi(x)$.

Back to the lemma: we consider the map $\widetilde{\alpha} : K \to K$ given by $x \mapsto \alpha x$. Then take

$$f(x) = \det(x - \widetilde{\alpha}|K) = P_{\widetilde{\alpha}}(x).$$

Cayley-Hamilton then tells us $f(\widetilde{\alpha}) = 0$, so we're *basically* done. We have to be a little bit more rigorous though: in general, $f(\widetilde{\alpha})$ (for arbitrary f) is the multiplication by $f(\alpha)$ endomorphism[3], so if $f(\widetilde{\alpha}) = 0$, then in particular $f(\alpha) \cdot 1 = 0$, so $f(\alpha) = 0$. □

1.2 The Ring of Integers

Now, we come to the second most important definition in the course:

Definition 1.4. If K is a number field, the **ring of integers** $\mathcal{O}_K \subseteq K$ is the set of all $\alpha \in K$ which are the root of a monic polynomial in $\mathbb{Z}[x]$. It needs to be proved that $\mathcal{O}_K$ actually *is* a ring, but for now we'll just take it on faith.

Lemma 1.5. *If $\alpha \in K$, the following are equivalent: i) $\alpha \in \mathcal{O}_K$, and ii) if $f_0(x) \in \mathbb{Q}[x]$ is the minimal polynomial of α, then $f_0(x) \in \mathbb{Z}[x]$.*

Proof. Recall that $f_0(x) \in \mathbb{Q}[x]$ is the monic polynomial of least degree such that $f_0(\alpha) = 0$. Moreover, if $f(x) \in \mathbb{Q}[x]$ and $f(\alpha) = 0$, then f_0 divides f.

ii) ⇒ i) is obvious from the definition — if $f_0(x)$ is in $\mathbb{Z}[x]$, then there is a monic polynomial in $\mathbb{Z}[x]$ which vanishes at α; just take $f_0(x)$.

i) ⇒ ii) Suppose $f \in \mathbb{Z}[x]$ and $f(\alpha) = 0$. Then $f = f_0 \cdot g$, with $g \in \mathbb{Q}[x]$. It is a consequence of Gauss' Lemma (which we will prove on the first homework, see Appendix A) that if $f \in \mathbb{Z}[x]$ factors as $f_0 \cdot g$ where $f_0, g \in \mathbb{Z}[x]$, then both f_0 and g are in $\mathbb{Z}[x]$ too. With this fact, we are done. □

Example 1.6. As a good (and standard) second example of a number field — after $\mathbb{Q}$, of course — let's take $K = \mathbb{Q}[\sqrt{2}]$. As an abstract vector space, this is the quotient $\mathbb{Q}[x]/(x^2 - 2)$. A basis for K is the set $\{1, \sqrt{2}\}$, so every $\alpha \in K$ can be written $\alpha = a + b\sqrt{2}$, for $a, b \in \mathbb{Q}$. What is the ring of integers $\mathcal{O}_K$? The minimal polynomial for $\alpha = a + b\sqrt{2}$ is

$$f(x) = (x - (a + b\sqrt{2}))(x - (a - b\sqrt{2})) = x^2 - (2a)x + (a^2 - 2b^2).$$

Therefore $\alpha \in \mathcal{O}_K$ if and only if $2a, a^2 - 2b^2 \in \mathbb{Z}$. Thus $a \in \frac{1}{2}\mathbb{Z}$, which implies $2b^2 \in \frac{1}{4}\mathbb{Z}$, i.e., $b^2 \in \frac{1}{8}\mathbb{Z}$. But if b^2 is a multiple of $1/8$, then b must be a multiple of $1/2$, so $b^2 \in \frac{1}{4}\mathbb{Z}$.

[3] Exercise: check this!

This implies $a^2 \in \frac{1}{2}\mathbb{Z}$, which gives $a \in \mathbb{Z}$; then we also get $b \in \mathbb{Z}$. Thus

$$\mathcal{O}_K = \mathbb{Z}[\sqrt{2}].$$

Note that this isn't always the case! If we take $K = \mathbb{Q}[\sqrt{5}]$, we see that $\mathcal{O}_K$ is strictly larger than $\mathbb{Z}[\sqrt{5}]$.

2 January 25, 2017

We began the class with Kisin working through the example from last time again, and once again presenting the example that for $K = \mathbb{Q}(\sqrt{5})$,

$$\mathbb{Z}[\sqrt{5}] \subset \mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right].$$

Now let's work out this theory in more generality, i.e., for an arbitrary quadratic extension.

2.1 Quadratic Extensions

Definition 2.1. A **quadratic extension** of $\mathbb{Q}$ is a number field $K/\mathbb{Q}$ such that $\dim_{\mathbb{Q}} K = 2$. A few properties are immediate from this definition: first, if $\alpha \in K$ and $\alpha \notin \mathbb{Q}$, then $\mathbb{Q}(\alpha) \subseteq K$ and $\mathbb{Q} \subsetneq \mathbb{Q}(\alpha)$. By a dimensional argument, it follows that $\mathbb{Q}(\alpha) = K$. Second, if $f(x) = \det(x - \alpha|_K) = x^2 + ax + b$ with $a, b \in \mathbb{Q}$ and $f(\alpha) = 0$, then by the quadratic formula, we get

$$K = \mathbb{Q}(\sqrt{d}), \quad d \in \mathbb{Q}.$$

Multiplying d by the square of an integer, we may as well assume that $d \in \mathbb{Z}$, and that d is squarefree.

We move on now to computing $\mathcal{O}_K$. It is immediate that $\mathbb{Z}[\sqrt{d}] \subseteq \mathcal{O}_K$. If we write $\alpha = a + b\sqrt{d}$, $a, b \in \mathbb{Q}$, when is $\alpha \in \mathcal{O}_K$?

The characteristic polynomial of α is given by

$$f_0(x) = (x-\alpha)(x-\overline{\alpha}) = x^2 - 2ax + (a^2 - db^2).$$

It follows that $\alpha \in \mathcal{O}_K$ if and only if $2a, a^2 - b^2 d \in \mathbb{Z}$. Write $a = A/2$ for some $A \in \mathbb{Z}$; then $4(a^2 - b^2 d) = A^2 - 4b^2 d \in 4\mathbb{Z}$. We have a few cases:

(i) If A is odd, then $A^2 \equiv 1 \mod 4$, which implies $4b^2 d$ is an integer $\equiv 1 \mod 4$. This implies that $4b^2 = (2b)^2 \in \frac{1}{d}\mathbb{Z}$. Because d is squarefree, we get $2b \in \mathbb{Z}$. But $4b^2 d \equiv 1$ mod 4 means $b = B/2$, but $b \notin \mathbb{Z}$. Also, $d \equiv 1 \mod 4$.

(ii) If $d \cong 3 \mod 4$, then by contrapositive to (i), A is even. Thus $a \in \mathbb{Z}$ and $b^2 d \in \mathbb{Z}$, so $b^2 \in \frac{1}{d}\mathbb{Z}$ and $b \in \mathbb{Z}$. This means that $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$.

(iii) If $d \cong 1 \mod 4$, and $\alpha \notin \mathbb{Z} + \mathbb{Z} \cdot \sqrt{d}$, then $\alpha = a + b\sqrt{d} = \frac{A}{2} + \frac{B}{2}\sqrt{d}$, both A and B odd. This is equal to

$$\frac{1+\sqrt{d}}{2} + \frac{(A-1)}{2} + \frac{(B-1)}{2}\sqrt{d}.$$

But we note that the latter two terms are in $\mathbb{Z}[\sqrt{d}]$, so $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$.

2.2 The Ring of Integers is a Ring

The ultimate goal of this section is to prove the lemma

Lemma 2.2. *If K is any number field, $\mathcal{O}_K \subseteq K$ is a subring.*

Definition 2.3. Suppose $A \subseteq R$ are commutative rings with unity. An element $\alpha \in R$ is said to be **integral over** A if there exists a monic polynomial $f(x) \in A[x]$ such that $f(\alpha) = 0$. The ring R is called **integral over** A if all $\alpha \in R$ are integral over A.

To prove the lemma, we will prove a stronger result:

Proposition 2.4. *If $A' = \{\alpha \in R : \alpha$ is integral over $A\}$, then A' is a subring of R (called the **integral closure**).*

We will assemble a few technical lemmas along the way to the proof of the proposition.

Lemma 2.5. *Let A be a ring and M be a finitely generated A-module, and let $\alpha : M \to M$ be an A-linear map. Then there exists a monic polynomial $f(x) \in A[x]$ such that $f(\alpha) = 0$.*

Proof. Assume M is free. Then the theory of last time comes into play: we can take $f(x) = \det(x - \alpha|_M)$, and apply Cayley-Hamilton. In general, a finitely-generated module is the quotient of a free module, so we have a surjection $A^n \to M$. Then lift α to a map $\alpha' : A^n \to A^n$ such that the diagram

$$\begin{tikzcd}
A^n \arrow[r, two heads] \arrow[d, "\alpha'"'] & M \arrow[d, "\alpha"] \\
A^n \arrow[r, two heads] & M
\end{tikzcd}$$

commutes. We then choose some $f(x)$ such that $f(\alpha') = 0$, which gives $f(\alpha) = 0$. □

Lemma 2.6. *If $A \subseteq R$ and $\alpha \in R$, the following are equivalent:*

(i) $f(\alpha) = 0$ *for some monic polynomial* $f(x) \in A[x]$.

(ii) $A[\alpha] \subseteq R$ *is a finitely-generated A-module.*

(iii) $A[\alpha]$ *is contained in* some *finitely-generated A-module.*

Proof. (*i) ⇒ ii)*) If α satisfies $f(\alpha) = 0$, then the map $A[x]/f(x) \longrightarrow\!\!\!\!\rightarrow A[\alpha]$ sending $x \mapsto \alpha$ is surjective, and $A[x]/f(x)$ is already finitely generated.

(*ii) ⇒ iii)*) Obvious.

(*iii) ⇒ i)*) We use the previous lemma: if $A[\alpha] \subseteq M$ is finitely generated, apply the lemma to the map $\widetilde{\alpha}$ given by $m \mapsto \alpha \cdot m$. Then there exists a monic $f(x) \in A[x]$ such that $f(\widetilde{\alpha}) = 0$, which implies (in the same way as last class) $f(\alpha) = 0$. □

Proof of Proposition. Recall the notation $A' = \{\alpha \in R : \alpha \text{ is integral over } A\}$. If $\alpha, \beta \in A'$, we want to show that $\alpha + \beta, \alpha \cdot \beta \in A'$ as well. We will show something more general: consider the ring $A[\alpha, \beta]$. This is a finitely generated $A[\alpha]$-module, because if $\{a_1, \ldots, a_n\}$ are A-module generators of $A[\beta]$, they are also a set of $A[\alpha]$-module generators of $A[\alpha, \beta]$.

Symmetrically, if $\{b_1, \ldots, b_m\}$ is a set of A-module generators for $A[\alpha]$, then they are $A[\beta]$-module generators of $A[\alpha, \beta]$. Thus, the set $\{a_i, b_j\}_{i,j}$ is a set of A-module generators for $A[\alpha, \beta]$, and $A[\alpha, \beta]$ is a finitely-generated A-module. If $\gamma \in A[\alpha, \beta]$, $A[\gamma] \subseteq A[\alpha, \beta]$, so the lemma gives us that γ is integral over A. In particular, $A[\alpha, \beta]$ is closed under sums and products. □

3 January 27, 2017

The ultimate goal of this lecture is to show that if K is a number field, $\mathcal{O}_K$ is finitely generated over $\mathbb{Z}$.

3.1 More on Integrality

The proof techniques of last time give us the following corollary:

Corollary 3.1. *If $A \subseteq B \subseteq C$ are rings and subrings, with B integral over A and C integral over B, then C is integral over A.*

Proof. If $\alpha \in C$, let $f(x) \in B[x]$ be monic with $f(\alpha) = 0$. If we write

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

then α is integral over $B_1 = A[a_0, \ldots, a_{n-1}]$. It follows that $B_1[\alpha]$ is finitely generated over B_1, and B_1 is obtained by adjoining coefficients in B. We get that B_1 is finitely generated over A, so $B_1[\alpha]$ is finitely generated over A. Thus α is integral over A. □

In our quest to show that $\mathcal{O}_K$ is finitely generated over $\mathbb{Z}$, we will in fact show that $\mathcal{O}_K \cong \mathbb{Z}^n$, where $n = [K : \mathbb{Q}]$.

3.2 The Norm and Trace Functions

Definition 3.2. Suppose $B \supseteq A$ are rings, and B is a finitely generated, free A-module (that is, $B \cong A^n$). If $\alpha \in B$, we can look at the map $\widetilde{\alpha} : B \to B$, $x \mapsto \alpha \cdot x$. We then define the **trace** of α as

$$\mathrm{Tr}_{B/A}(\alpha) := \mathrm{tr}(\widetilde{\alpha}|_B) \in A,$$

and the **norm** of α as

$$N_{B/A} := \det(\widetilde{\alpha}|_B) \in A.$$

Recall that $\mathrm{tr}(\widetilde{\alpha}|_B)$ is -1 times the first coefficient of $\det(x - \widetilde{\alpha}|_B)$.

Remark 3.3. If L/K is a finite field extension, then this definition applies. If furthermore L/K is Galois, then

$$N_{L/K}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha) \quad \text{and}$$
$$\mathrm{Tr}_{L/K}(\alpha) = \sum_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha).$$

We will prove these later.

Lemma 3.4. *If* $\alpha \in \mathcal{O}_K$*, then* $\det(x - \widetilde{\alpha}|_K) \in \mathbb{Z}[x]$.

Proof. If $K = \mathbb{Q}[\alpha]$, then this determinant *is* the minimal polynomial of α. To see this, we see that there is a map

$$\begin{tikzcd} \mathbb{Q}[x]/f_0(x) \arrow[r, two heads] & \mathbb{Q}(\alpha) \end{tikzcd}$$

which is surjective. But because $f_0(x)$ is minimal, the quotient is a field. Thus the map is injective as well. It follows that $\deg f_0(x) = [\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(\det(x - \widetilde{\alpha}|_K))$, so $f_0(x) = \det(x - \widetilde{\alpha}|_K)$.

Clarify this part of the proof

For the general case, $\widetilde{\alpha} : K \to K$ restricts to $\widetilde{\alpha} : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$. We can identify $K \cong \mathbb{Q}(\alpha)^s$, such that $\widetilde{\alpha}$ acts component-wise. The matrix of $\widetilde{\alpha}$ is block diagonal with all blocks given by the matrix of $\widetilde{\alpha} : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$.

This implies that $\det(x - \widetilde{\alpha}|_K) = f_0(x)^{[K:\mathbb{Q}(\alpha)]} \in \mathbb{Z}[x]$. □

Kisin: *"Sorry about the bases... usually if someone chooses a basis, they've taken a wrong turn."*

This lemma implies that if $\alpha \in \mathcal{O}_K$, then $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$.

3.3 The Trace Pairing

Definition 3.5. The **trace pairing** is the pairing of $\mathbb{Q}$-vector spaces defined by

$$K \times K \to \mathbb{Q}, \qquad (x, y) \mapsto \langle x, y \rangle := \mathrm{Tr}_{K/\mathbb{Q}}(xy).$$

This is evidently bilinear, and gives a map

$$\begin{tikzcd} K \arrow[r] & \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{Q}) = K^* \\ \alpha \arrow[r, mapsto] & (x \mapsto \mathrm{Tr}_{K/\mathbb{Q}}(\alpha x)) =: \varphi_\alpha. \end{tikzcd}$$

The map $\alpha \mapsto \varphi_\alpha$ is injective: indeed, if $\alpha \neq 0$, it is immediate that $\varphi_\alpha(\alpha^{-1}) = \mathrm{Tr}_{K/\mathbb{Q}}(1) = [K : \mathbb{Q}] \neq 0$. This crucially uses the fact that we're in characteristic zero; we will see an example at the end of lecture where, in characteristic p, we have a nonzero α where φ_α is the zero map.

Definition 3.6. For any additive subgroup $L \subseteq K$, we define the **dual subgroup** $L^\vee$ of L by

$$L^\vee := \{\alpha \in K : \mathrm{Tr}_{K/\mathbb{Q}}(\alpha \cdot x) \in \mathbb{Z}, \forall x \in L\}.$$

If $e_1, \ldots, e_n$ is a $\mathbb{Q}$-basis for K, and $L = \mathbb{Z}\langle e_1, \ldots, e_n\rangle$, we define $e_i^\vee \in K$ as follows: the trace pairing gives an isomorphism $K \xrightarrow{\simeq} K^*$; let $e_i^\vee$ be such that $e_i^\vee(e_j) = \delta_{ij}$, where we consider $e_i^\vee$ as its image under the isomorphism. This is obviously another $\mathbb{Q}$-basis for K.

For any $\beta \in K$, write $\beta = \sum a_i \cdot e_i^\vee$. Then

$$\langle \beta, e_j\rangle = a_j.$$

Thus $L^\vee = \mathbb{Z}\langle e_1^\vee, \ldots, e_n^\vee\rangle$.

Proposition 3.7. *We have an isomorphism $\mathcal{O}_K \cong \mathbb{Z}^n$, where $n = [K : \mathbb{Q}]$.*

Proof. Take a $\mathbb{Q}$-basis for K $e_1, \ldots, e_n$, where each $e_i \in \mathcal{O}_K$. How do we know that this is possible? If $\alpha \in K$, write the minimal polynomial for α as $f_0(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, with the $a_i \in \mathbb{Q}$. Note that if $m \in \mathbb{Z}$, $m \cdot \alpha$ has minimal polynomial

$$(mx)^n + m \cdot a_{n-1}(mx)^{n-1} + \cdots + m^n \cdot a_0.$$

If we take $m = \operatorname{lcm}(a_1, \ldots, a_n)$, then $m\alpha \in \mathcal{O}_K$, and things work.

Let $L = \mathbb{Z}\langle e_1, \ldots, e_n\rangle \subseteq \mathcal{O}_K$. Recall that $\operatorname{Tr}_{K/\mathbb{Q}}(\mathcal{O}_K) \subseteq \mathbb{Z}$, or equivalently

$$\langle \cdot, \cdot \rangle : \mathcal{O}_K \times \mathcal{O}_K \longrightarrow \mathbb{Z}.$$

This implies that $\mathcal{O}_K \subseteq \mathcal{O}_K^\vee$, so $L \subseteq \mathcal{O}_K^V$. By the inclusion reversal of the $\vee$ operation, we have the inclusion $\mathcal{O}_K^\vee \subseteq L^\vee$. This finishes the proof, because $\mathcal{O}_K$ is sandwiched between two free abelian groups of rank n. Thus $\mathcal{O}_K \cong \mathbb{Z}^n$. □

Example 3.8. We look at some of our examples of quadratic extensions (or rather the one general example), and show that they agree with this proposition. If $K = \mathbb{Q}(\sqrt{d})$ where $d \in \mathbb{Z}$ is squarefree, then

$$\begin{aligned} \mathcal{O}_K &= \mathbb{Z}[\sqrt{d}] \cong \mathbb{Z}^2, && d \equiv 3 \mod 4 \\ \mathcal{O}_K &= \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] \cong \mathbb{Z}^2, && d \equiv 1 \mod 4 \end{aligned}$$

Remark 3.9. Let $\mathbb{F}_p$ be the field with p elements, p a prime. With the inclusion $\mathbb{F}_p[x] \subseteq \mathbb{F}_p(x)$, we can introduce "$p$-th roots of x" and take $\mathbb{F}_p[x^{1/p}] \subseteq \mathbb{F}_p(x^{1/p})$. This is an example of a "ring of integers" in characteristic p.

In this way, we can look at the trace pairing on $\mathbb{F}_p(x^{1/p})$:

Example 3.10. *(Trace pairing is zero.)* The field extension $\mathbb{F}_p(x^{1/p}) \supseteq \mathbb{F}_p(x)$ is a degree p extension with basis $1, x^{1/p}, \dots, x^{(p-1)/p}$. It is clear that $x^{i/p}$ acts by $x^{j/p} \mapsto x^{(i+j)/p}$.

Thus if $i = 1, \dots, p-1$, this is a nontrivial cyclic permutation, so the matrix representing it has zeros on the diagonal (zero trace). Because we are working in characteristic p, $\operatorname{tr}(1) = p = 0$. Thus the trace pairing itself is zero.

4 January 30, 2017

4.1 The Discriminant

Recall from last time: if K is a number field and $\mathcal{O}_K$ is its ring of integers, then $\mathcal{O}_K \cong \mathbb{Z}^n$, where $n = [K : \mathbb{Q}]$. In general, $\mathcal{O}_k$ does not equal its dual module $\mathcal{O}_K^\vee$, unless $K = \mathbb{Q}$. We can then ask:

Question 4.1. What is $|\mathcal{O}_K^\vee/\mathcal{O}_K|$? This is called the **discriminant** of K, and it comes up in various calculations.

Lemma 4.2. *Let $\alpha_1, \ldots, \alpha_n$ be a $\mathbb{Z}$-basis for $\mathcal{O}_K$. Then*

$$\det \operatorname{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j) = [\mathcal{O}_K^\vee : \mathcal{O}_K] = \left|\frac{\mathcal{O}_K^\vee}{\mathcal{O}_K}\right|,$$

where the trace is taken element-wise in the matrix $(\alpha_i\alpha_j)$.

Before we prove this lemma (which will take the entire lecture), let's give an example.

Example 4.3. Let K be a quadratic extension, that is, $K = \mathbb{Q}(\sqrt{d})$ for some squarefree $d \in \mathbb{Z}$. We have two cases to deal with: if $d \equiv 3\ (4)$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$; and if $d \equiv 1\ (4)$, then $\mathcal{O}_K = \left[\frac{1+\sqrt{d}}{2}\right]$. In the first case, we have a $\mathbb{Z}$-basis for $\mathcal{O}_K$ given by $\{1, \sqrt{d}\}$, so we want to compute

$$\det\left(\operatorname{Tr}_{K/\mathbb{Q}}\begin{pmatrix} 1 & \sqrt{d} \\ \sqrt{d} & d \end{pmatrix}\right).$$

Remember that $\operatorname{Tr}_{K/\mathbb{Q}}(\alpha) = \operatorname{tr}(\alpha : K \to K)$. Also, $\operatorname{Tr}_{K/\mathbb{Q}}(\sqrt{d}) = 0$, so

$$|\mathcal{O}_K^\vee/\mathcal{O}_K| = \det\begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} = 4d$$

In the other case, we want to compute

$$\det\left(\operatorname{Tr}_{K/\mathbb{Q}}\begin{pmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ \frac{1+\sqrt{d}}{2} & \frac{1+2\sqrt{d}+d}{2} \end{pmatrix}\right),$$

which equals

$$\det\begin{pmatrix} 2 & 1 \\ 1 & \frac{1+d}{2} \end{pmatrix} = 1 + d - 1 = d.$$

We now return to the proof of the lemma: Suppose $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n \in K$ (where $n = [K : \mathbb{Q}]$). Write

$$\alpha = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}, \quad \beta = \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}.$$

Then $\mathrm{Tr}_{K/Q}(\alpha_i \beta_j) = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha \cdot \beta^t)$. Now for a technical lemma:

Lemma 4.4. *If $M \in M_n(\mathbb{Q})$, and $\alpha' = M \cdot \alpha$, then*

$$\det \left(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha' \cdot \beta^t \right) = \det M \cdot \det \mathrm{Tr}_{K/\mathbb{Q}}(\alpha \cdot \beta^t).$$

Proof. We know $\det(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha' \cdot \beta^t)) = \det(\mathrm{Tr}_{K/\mathbb{Q}}(M \cdot \alpha \cdot \beta^t))$. Because trace is $\mathbb{Q}$-linear, we get that this is equal to

$$\det(M \cdot \mathrm{Tr}_{K/\mathbb{Q}}(\alpha \cdot \beta^t)) = \det(M) \cdot \det(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha \cdot \beta^t)).$$

□

Corollary 4.5. *Suppose α, β are $\mathbb{Q}$-bases for K. Then up to sign,* $\det(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha \cdot \beta^t))$ *depends only on $\sum_i \mathbb{Z} \cdot \alpha_i$ and $\sum_j \mathbb{Z} \cdot \beta_j$.*

Proof. Suppose $\alpha' = (\alpha'_1, \ldots, \alpha'_n)^t$ is another basis with $\mathbb{Z}\langle \alpha' \rangle = \mathbb{Z}\langle \alpha \rangle$. We have a matrix M such that $\alpha' = M \cdot \alpha$. We know that $M \in \mathrm{GL}_n(\mathbb{Z})$, and $M^{-1} \in \mathrm{GL}_n(\mathbb{Z})$, so $M \in \mathrm{SL}_n(\mathbb{Z})$. □

Corollary 4.6. $\det(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i \alpha_j))$ *depends only on $\sum \mathbb{Z} \cdot \alpha_i$.*

Proof. Previous proof shows $\alpha \mapsto \alpha'$ changes $\det \mathrm{Tr}(-)$ by $\det(M)^2 = (\pm 1)^2 = 1$. □

Lemma 4.7. *With the same notation, let $\alpha = (\alpha_1, \ldots, \alpha_n)^t$ be a $\mathbb{Q}$-basis K, $\alpha' = M \cdot \alpha$ for some $M \in M_n(\mathbb{Z})$,* $\det(M) \neq 0$. *Let*

$$L = \sum \mathbb{Z} \cdot \alpha_i, \qquad L' = \sum \mathbb{Z} \cdot \alpha'_i.$$

Then $[L : L'] = \pm \det(M)$.

Proof. (first) Truth of the lemma depends only on L, L', not on α and α', as changing α and α' while keeping L and L' fixed changes M by multiplication by $\mathrm{GL}_n(\mathbb{Z})$ (which have determinant ± 1). For a more "enlightened" proof, let us record the following fact:

Lemma 4.8. *There exists a $\mathbb{Z}$-basis $e_1, \dots, e_n$ of L such that $L = \sum \mathbb{Z} f_i e_i$, $f_i \in \mathbb{Z}$.*

Proof. In Samuel. The idea is that L/L' is a finitely-generated abelian group, and $L/L' = \prod(\mathbb{Z}/n_i)$. □

With this fact, we can take $M = \begin{pmatrix} f_1 & & \\ & \ddots & \\ & & f_n \end{pmatrix}$, so $\det(M) = \prod f_i = |L/L'|$.

(second) We have $L' \subseteq L$ by assumption. Write $V = L \otimes \mathbb{R} = \mathbb{R} \cdot \alpha_1 + \cdots + \mathbb{R} \cdot \alpha_n = \mathbb{R} \cdot \alpha_1' + \cdots + \mathbb{R} \cdot \alpha_n'$, so $L' \subseteq L \subseteq V$. We're going to discuss volumes. Take, for concreteness, a volume form on $V = L \otimes \mathbb{R}$. We have the composition

$$\begin{tikzcd} L/L' \arrow[r] & V/L' \arrow[r, two heads] & V/L, \end{tikzcd}$$

which gives $\mathrm{Vol}(V/L') = |L/L'|\mathrm{Vol}(V/L)$. Remember that M is by definition $\alpha' = M \cdot \alpha$. As a linear map $V \to V$, M induces an isomorphism $M : L \xrightarrow{\simeq} L'$, so we get an isomorphism

$$M : V/L \xrightarrow{\simeq} V/L'.$$

To the volume form, this tells us

$$\mathrm{Vol}(V/L') = |\det(M)|\mathrm{Vol}(V/L),$$

so $[L : L'] = \pm \det M$. □

Proof of Lemma 4.2. Take $\alpha_1^\vee, \dots, \alpha_n^\vee$ the dual basis; write $\alpha = M \cdot \alpha^\vee$. Then $\det(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha \cdot \alpha^t)) = \det(\mathrm{Tr}_{K/\mathbb{Q}}(M \cdot \alpha^\vee \cdot \alpha^t))$

$$= \det(M) \cdot \det(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^\vee \cdot \alpha^t)) = \pm[\mathcal{O}_K^\vee : \mathcal{O}_K].$$

□

5 February 1, 2017

This lecture will be guided by the following proposition:

Proposition 5.1. *Let K, L be linearly disjoint number fields; write $D_K = \operatorname{disc}(K)$ and $D_L = \operatorname{disc}(L)$. Then*

$$\mathcal{O}_K \cdot \mathcal{O}_L \subseteq \mathcal{O}_{K \cdot L} \subseteq \frac{1}{\gcd(D_K, D_L)} \mathcal{O}_K \cdot \mathcal{O}_L.$$

In particular, if $\gcd(D_K, D_L) = 1$, then $\mathcal{O}_K \cdot \mathcal{O}_L = \mathcal{O}_{K \cdot L}$.

5.1 Linear Disjointness

Let us first clarify what is meant by *linear disjointness*:

Definition 5.2. We say that two extensions $K/\mathbb{Q}$ and $L/\mathbb{Q}$ are **linearly disjoint** if $[K \cdot L : \mathbb{Q}] = [K : \mathbb{Q}] \cdot [L : \mathbb{Q}]$, which is the same as saying the natural map

$$K \otimes_{\mathbb{Q}} L \xrightarrow{\simeq} K \cdot L,$$

where $\dim_{\mathbb{Q}}(K \otimes_{\mathbb{Q}} L) = \dim_{\mathbb{Q}} K \cdot \dim_{\mathbb{Q}} L$. Equivalently, $K \otimes_{\mathbb{Q}} L$ is a field.

Example 5.3. Suppose that K and L are quadratic fields, and $K \neq L$. We have the following field diagram:

$$\begin{tikzcd}
 & K \cdot L \arrow[dl, dash, "2"'] \arrow[dr, dash, "2"] \arrow[dd, dash, "4"] & \\
K \arrow[dr, dash, "2"'] & & L \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

From this, we see that K and L are linearly disjoint ($4 = 2 \cdot 2$).

Example 5.4. The above allows us to compute the ring of integers of a biquadratic field, as the next lemma will make precise:

$$\mathcal{O}_{\mathbb{Q}(\sqrt{5},\sqrt{7})} = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}, \sqrt{7}\right].$$

Lemma 5.5. *Suppose $L \supseteq K$ are number fields. Then*

$$\mathcal{O}_L \cap K = \mathcal{O}_K.$$

Proof. Simply note that an integral element in K is integral in L, and that any integral element in $L \cap K$ is integral in K. □

Lemma 5.6. *Let $\alpha \in \mathcal{O}_L$, and let $P_{0,K}$ be the minimal polynomial of α over K. Then $P_{0,K} \in \mathcal{O}_K[x]$.*

Proof. (Kisin stares at board in silence.) Consider $P_{0,\mathbb{Q}}$, the minimum polynomial of α over $\mathbb{Q}$. This lives in $\mathbb{Z}[x]$. Then $P_{0,K}$ divides $P_{0,\mathbb{Q}}$ in $K[x]$. Now choose an extension $L' \supseteq L$ such that $P_{0,\mathbb{Q}}$ factors completely over L' :

$$P_{0,\mathbb{Q}} = (x-\alpha_1)\cdots(x-\alpha_n),$$

and $\alpha_i \in \mathcal{O}_{L'}$ for all i. Thus $P_{0,K} \in \mathcal{O}_{L'}[x] \cap K[x] = \mathcal{O}_K[x]$. □

Corollary 5.7. $\mathrm{Tr}_{L/K}(\mathcal{O}_L) \subseteq \mathcal{O}_K$. *In fact, if $\alpha \in \mathcal{O}_L$, then $P_\alpha(x) \in \mathcal{O}_K[x]$.*

Proof. Consider L as a $K(\alpha)$-vector space. In the case $K(\alpha) = L$, the previous lemma handles it for us. Suppose then that we have an identification $L \cong K(\alpha)^n$. Then the map $\tilde{\alpha} : L \to L$, $x \mapsto \alpha x$, is given by a block diagonal matrix where all blocks are of the form $\tilde{\alpha} : K(\alpha) \to K(\alpha)$. Thus,

$$P_\alpha(x) = P_{0,K}(\alpha)^{[L:K(\alpha)]}.$$

□

Corollary 5.8. *If $f = gh$ are monic polynomials in $\mathcal{O}_K[x]$, then $g, h \in \mathcal{O}_K[x]$.*

Proof. Choose $K' \supseteq K$ such that f factors completely over K'. Any zero of f is in $\mathcal{O}_{K'}$, and so for g and h. Thus $g, h \in \mathcal{O}_{K'}[x] \cap K[x] = \mathcal{O}_K[x]$. □

5.2 Some Trace Stuff, Some Galois Stuff

Lemma 5.9. *Let $\overline{K}$ be a fixed algebraic closure of K. If $\alpha \in L$, then*

$$\mathrm{Tr}_{L/K}(\alpha) = \sum_{\sigma : L \hookrightarrow \overline{K}} \sigma(\alpha).$$

That is to say, taking the trace is the same as taking the sum of Galois conjugates.

Proof. Suppose $L = K(\alpha)$. The minimal polynomial $P_{0,K}(\alpha)$ of alpha factorizes over $\overline{K}$ as

$$P_{0,K}(\alpha) = \det(x - \widetilde{\alpha}|_L) = (x - \alpha_1) \cdots (x - \alpha_n), \quad \alpha_i \in \overline{K}.$$

Thus $\mathrm{Tr}_{L/K}(\alpha) = \alpha_1 + \alpha_2 + \cdots + \alpha_n$. What are the embeddings $L \hookrightarrow \overline{K}$? In the case that $L = K(\alpha)$, we have $L = K[x]/(P_{0,K})$, so □

Definition 5.10. For any extension of number fields K'/K and $\mathcal{O}_K$-submodule $L \subseteq K'$, we define

$$L^{\vee_k} = \{\alpha \in K' : \mathrm{Tr}_{K'/K}(\alpha \cdot \beta) \in \mathcal{O}_K \ \forall \ \beta \in L\}.$$

The claim, which we will prove next time, is that if K and L are linearly disjoint number fields,

$$(\mathcal{O}_K \otimes \mathcal{O}_L)^{\vee_K} = \mathcal{O}_K \otimes \mathcal{O}_L^{\vee} = \mathcal{O}_K \cdot \mathcal{O}_L^{\vee}.$$

6 February 3, 2017

6.1 Finishing the Proposition of Last Time

Kisin: *"We could just have class in my office at this point."*

Remark 6.1. If $\alpha_1, \ldots, \alpha_n$ is a $\mathbb{Z}$-basis for $\mathcal{O}_K$, then

$$\det \operatorname{Tr}(\alpha_i \alpha_j) = \pm[\mathcal{O}_K^\vee : \mathcal{O}_K].$$

The point is that the *determinant* carries the sign, while the order of $\mathcal{O}_K^\vee / \mathcal{O}_K$ doesn't.

Recall the proposition from last time:

Proposition 6.2. *If L and K are linearly disjoint number fields, then*

$$\mathcal{O}_{K \cdot L} \subseteq \frac{1}{\gcd(D_K, D_L)} \mathcal{O}_K \cdot \mathcal{O}_L.$$

In particular, there is equality if D_K and D_L are coprime.

If $\mathscr{L} \subseteq K \subseteq K'$, and $\mathscr{L}$ is an $\mathcal{O}_K$ submodule, recall the definition from last time:

$$\mathscr{L}^{\vee_K} = \{\alpha \in K' : \operatorname{Tr}_{K'/K}(\alpha \cdot \beta) \in \mathcal{O}_K \quad \forall\, \beta \in \mathscr{L}\}.$$

The claim, which we will prove, is the following:

Lemma 6.3. $(\mathcal{O}_K \otimes \mathcal{O}_L)^{\vee_K} = \mathcal{O}_K \otimes \mathcal{O}_L^\vee \subseteq L \otimes K = L \cdot K$.

Proof. Note that if $\alpha \in L$, then $\det_K(x - \alpha|_{K \cdot L}) = \det_{\mathbb{Q}}(x - \alpha|_L)$, since a $\mathbb{Q}$-basis for L is a K basis for $K \cdot L$. This implies that $\operatorname{Tr}_{K \cdot L/K}(\alpha) = \operatorname{Tr}_{L/\mathbb{Q}}(\alpha)$.

Choose $e_1, \ldots, e_s$ a $\mathbb{Z}$-basis for $\mathcal{O}_K$; thus

$$\mathcal{O}_K \otimes \mathcal{O}_L = \bigoplus_i e_i \mathcal{O}_L.$$

So for any $\alpha \in K \cdot L$, we can write

$$\alpha = e_1 \alpha_1 + \cdots + e_s \alpha_s, \quad \alpha_i \in \mathcal{O}_L.$$

For any $\beta \in L$, K-linearity of the trace gives

$$\begin{aligned} \mathrm{Tr}_{K\cdot L/K}(\alpha \cdot \beta) &= \sum_i e_i \,\mathrm{Tr}\, K \cdot L/K(\alpha_i \cdot \beta) \\ &= \sum_i e_i \,\mathrm{Tr}_{L/\mathbb{Q}}(\alpha_i \cdot \beta). \end{aligned}$$

Suppose $\beta \in \mathcal{O}_L$. Then

$$\mathrm{Tr}_{K\cdot L/K}(\alpha \cdot \beta) \in \mathcal{O}_K \iff \mathrm{Tr}_{L/\mathbb{Q}}(\alpha_i \cdot \beta) \in \mathbb{Z}, \forall\, i.$$

Recall that we are tasked with trying to understand when $\mathrm{Tr}_{K\cdot L/K}(\alpha \cdot \beta) \in \mathcal{O}_K$ for all $\beta \in \mathcal{O}_K \otimes \mathcal{O}_L$. This holds if and only if

$$\mathrm{Tr}\, K \cdot L/K(\alpha \cdot \beta) \in \mathcal{O}_K \quad \forall\, \beta \in \mathcal{O}_L,$$

which is equivalent to saying

$$\begin{aligned} \mathrm{Tr}_{K\cdot L/K}(\alpha_i \cdot \beta) \in \mathbb{Z} &\iff \alpha_i \in \mathcal{O}_L^\vee \;\; \forall\, i \\ &\iff \alpha \in \mathcal{O}_L^\vee \otimes \mathcal{O}_K \end{aligned}$$

□

6.2 Cyclotomic Extensions

Definition 6.4. A **cyclotomic field** is a number field $K = \mathbb{Q}(\zeta_n)$, where ζ_n is a primitive n-th root of unity.

Consider the case of ζ_p, where p is prime. This satisfies $\zeta_p^p - 1 = 0$. What is the degree of this extension?

Let $f(x) = \frac{x^p - 1}{x - 1}$. It is clear that $f(\zeta_p) = 0$, because $\zeta_p \neq 1$.

Lemma 6.5. *$f(x)$ as defined is irreducible over $\mathbb{Q}$.*

To prove this, we will make use of the following sublemma:

Lemma 6.6. *Suppose $f(x) \in \mathbb{Z}[x]$ is monic. If $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, where $p|a_i$, $p^2 \not| a_0$ for some prime p, then $f(x)$ is irreducible.*

Proof. Suppose $f(x) = g(x)h(x)$, where $g, h \in \mathbb{Q}[x]$ are monic. Then by Gauss's lemma, $g, h \in \mathbb{Z}[x]$. We now pass to the quotient, $\mathbb{Z}[x] \mapsto \mathbb{Z}/p[x]$ via $b \mapsto \overline{b}$. From this,

$$\overline{f}(x) = x^n = \overline{g}\overline{h},$$

so $\overline{g}(x) = x^i$ and $\overline{h}(x) = x^j$ for some $i + j = n$. Because p^2 does not divide a_0, $\overline{h}(0)$ and $\overline{g}(0)$ are not both zero. Thus either i or j are zero. □

Back to the Lemma. It can be shown easily that $f(x) = x^{p-1} + x^{p-2} + \cdots + 1$. The trick here is to make the substitution $x \mapsto x + 1$. It is clear that $f(x)$ is irreducible if and only if $f(x+1)$ is. We have then

$$g(x) = f(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + \binom{p}{p-1} x^{p-2} + \cdots + \binom{p}{1}.$$

Since $\binom{p}{n}$ is divisible by p for all n, and $\binom{p}{1} = p$, the conditions of Eisenstein's criterion (Lemma 6.6) hold. □

Corollary 6.7. $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$ *and* $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p)^\times$.

Proof. The first part follows directly from $\mathbb{Q}(\zeta_p) \cong \mathbb{Q}[x]/f(x)$. For the second, consider the map $\zeta_p \mapsto \zeta_p^i$, where $i = 1, 2, \ldots, p-1$. This map gives rise to an automorphism $\mathbb{Q}(\zeta_p) \longrightarrow \mathbb{Q}(\zeta_p)$. We thus get a map

$$(\mathbb{Z}/p)^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$$

which can be seen immediately to be a homomorphism. □

Next class, we will look at the following:

Proposition 6.8. $\mathcal{O}_{\mathbb{Q}(\zeta_p)} = \mathbb{Z}[\zeta_p]$.

Question 6.9. Corresponding to the inclusion $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_p)$, we have the field diagram

$$\begin{tikzcd}
\mathbb{Q}(\zeta_p) \arrow[d, dash, "p-1"] \\
\mathbb{Q}.
\end{tikzcd}$$

If $p \neq 2$, then $p - 1$ is even. Recall that there is an isomorphism $(\mathbb{Z}/p)^\times \cong \mathbb{Z}/(p-1)$, so $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is cyclic of even order. There is thus a unique map

$$\varphi : \mathbb{Z}/(p-1) \longrightarrow \mathbb{Z}/2,$$

with kernel $2\mathbb{Z}/(p-1) =: H$. By Galois theory, we know that the fixed field $\mathbb{Q}(\zeta_p)^H$ is a degree 2 (i.e., quadratic) extension. What is this extension?

7 February 6, 2017

7.1 More on Cyclotomic Extensions

Recall from last time: let $K = \mathbb{Q}(\zeta_p)$. We showed that $\text{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/p)^\times \cong \mathbb{Z}/(p-1)$. As Kisin mentioned at the end of last class, we will prove the following proposition:

Proposition 7.1. $\mathcal{O}_{\mathbb{Q}(\zeta_p)} = \mathbb{Z}[\zeta_p]$.

To begin the proof, let $f(x) = x^{p-1} + x^{p-2} + \cdots + 1$. For some fixed algebraic closure $\overline{K}$ of K, we can factor $f(x)$ as

$$f(x) = \prod_{\sigma:\mathbb{Q}\hookrightarrow\overline{K}} (X - \sigma(\zeta_p)) = \prod_{i=1}^{p-1} (x - \zeta_p^i).$$

Note that $\text{Tr}_{K/\mathbb{Q}}(\zeta_p) = -1$, and $\text{Tr}_{K/\mathbb{Q}}(\zeta_p^i) = -1$ for all $i = 1, \dots, p-1$. This implies that

$$\text{Tr}_{K/\mathbb{Q}}(1 - \zeta_p^i) = (p-1) + 1 = p,$$

because $\text{Tr}_{K/\mathbb{Q}}(1) = p - 1$. Using the expression of the norm as the product of Galois conjugates, we also have

$$N_{K/\mathbb{Q}}(1 - \zeta_p^i) = \prod_{i=1}^{p-1} (1 - \zeta_p^i) = f(1) = p.$$

Lemma 7.2. $\mathcal{O}_K \cdot (1 - \zeta_p) \cap \mathbb{Z} = p \cdot \mathbb{Z}$.

Proof. Note that $p = f(1) \in \mathcal{O}_K \cdot (1 - \zeta_p)$, so $p \cdot \mathbb{Z} \subseteq \mathcal{O}_K \cdot (1 - \zeta_p) \cap \mathbb{Z}$. If the containment is strict, then $\mathcal{O}_K \cdot (1 - \zeta_p) \cap \mathbb{Z} = \mathbb{Z}$, because there is no proper ideal of $\mathbb{Z}$ containing $p \cdot \mathbb{Z}$ other than the entire ring. Thus, $1 - \zeta_p \in \mathcal{O}_K^\times$. By Galois conjugation, $1 - \zeta_p^i \in \mathcal{O}_K^\times$ for all $i = 1, \dots, p-1$ as well, so $f(1) \in \mathcal{O}_K^\times$, which implies $p^{-1} \in \mathcal{O}_K^\times$. But this is a contradiction, as the minimum polynomial for p^{-1} in $\mathcal{O}_K$ is $x - p^{-1}$, so $p^{-1} \notin \mathcal{O}_K$. □

Corollary 7.3. *If* $y \in \mathcal{O}_K$*, then* $\text{Tr}_{K/\mathbb{Q}}(y \cdot (1 - \zeta_p)) \in p \cdot \mathbb{Z}$.

Proof.

$$\text{Tr}_{K/\mathbb{Q}}(y \cdot (1 - \zeta_p)) = \sum_{\sigma:\mathbb{Q}\hookrightarrow\overline{K}} \sigma(y)(1 - \sigma(\zeta_p)) \in \mathcal{O}_K \cdot (1 - \zeta_p) \cap \zeta = p \cdot \mathbb{Z} \text{ by lemma.}$$

□

Back to Proposition. Suppose $x = a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2} \in \mathcal{O}_K$, $a_i \in \mathbb{Q}$[4]. Multiply x by $(1-\zeta_p)$:

$$x(1-\zeta_p) = a_0(1-\zeta_p) + a_1(1-\zeta_p)\zeta_p + \cdots + a_{p-2}(1-\zeta_p)\zeta_p^{p-2},$$

and take the trace: since $(1-\zeta_p)\zeta_p = \zeta_p - \zeta_p^2$ (and in general, $(1-\zeta_p^i)\zeta_p = \zeta_p - \zeta_p^{i+1}$), those terms go to zero under the trace, so

$$\mathrm{Tr}_{K/\mathbb{Q}}(x(1-\zeta_p)) = p \cdot a_0,$$

and $a_0 \in \mathbb{Z}$ by the lemma.

For the other coefficients, multiply by ζ_p^{-1}:

$$\zeta_p^{-1}x = a_1 + a_2\zeta_p + \cdots + a_{p-2}\zeta_p^{p-3} + a_0\zeta_p^{-1}.$$

Since we know $a_0\zeta_p^{-1} \in \mathcal{O}_K$, we can subtract it off, and apply the argument again to see $a_1 \in \mathbb{Z}$; by induction, we see that $a_0, \ldots, a_{p-2} \in \mathbb{Z}$. □

7.2 Quadratic Subfields of Cyclotomic Extensions

We return now to our question from last time: recall that by Galois theory, the fixed field of the group of automorphisms corresponding to $2\mathbb{Z}/(p-1)$ is a quadratic subextension of $\mathbb{Q}(\zeta_p)$.

Question 7.4. What is this subfield *really*?

To answer this, we need two propositions. We state them now, and will give complete proofs next time.

Proposition 7.5. *Let $L = \mathbb{Q}(\zeta_p)$. Then the discriminant* $\mathrm{disc}(L)$ *is*

$$\mathrm{disc}(L) = (-1)^{\frac{(p-1)(p-2)}{2}} \cdot p^{p-2}$$

Proposition 7.6. *If $\mathbb{Q} \subseteq K \subseteq L$ are number fields, then*

$$\mathrm{disc}(K) \mid \mathrm{disc}(L).$$

Assuming the propositions, we may answer our question. Let $K \subseteq L = \mathbb{Q}(\zeta_p)$ be the quadratic subfield; we know $K = \mathbb{Q}(\sqrt{d})$ for d a squarefree integer. We also know $\mathrm{disc}(K) = d$ if $d \equiv 1$ (4), or $4d$ if $d \not\equiv 1$ (4). By the proposition (and that d is squarefree),

$$d | p^{p-2} \Longrightarrow d|p \Longrightarrow d = \pm p.$$

[4] Because $\{1, \zeta_p, \ldots, \zeta_p^{p-2}\}$ forms a $\mathbb{Q}$-basis for $\mathcal{O}_K$

So

$$d = \begin{cases} p & p \equiv 1\ (4) \\ -p & p \equiv 3\ (4) \end{cases}.$$

But of course this hinges on the propositions.

8 February 8, 2017

Recall the two propositions from last time, that we used in computing the quadratic subfield of a cylotomic extension:

Proposition 8.1. *If p is an odd prime,*

$$\operatorname{disc}(\mathbb{Q}(\zeta_p)) = (-1)^{\frac{(p-1)(p-2)}{2}} p^{p-2}$$

Proposition 8.2. *If $\mathbb{Q} \subseteq K \subseteq L$ are number fields, then*

$$d_K | d_L.$$

8.1 Discriminants of Subfields

Proof of Proposition 8.2. We claim that $\mathcal{O}_K^\vee \subseteq \mathcal{O}_L^\vee$. If $\alpha \in \mathcal{O}_K^\vee$, then $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha \cdot \beta) \in \mathbb{Z}$ for all $\beta \in \mathcal{O}_K$. We must check that if $\beta \in \mathcal{O}_L$,

$$\mathrm{Tr}_{L/\mathbb{Q}}(\alpha \cdot \beta) \in \mathbb{Z}.$$

By transitivity of the trace, $\mathrm{Tr}_{L/\mathbb{Q}} = \mathrm{Tr}_{K/\mathbb{Q}} \circ \mathrm{Tr}_{L/K}$. Thus

$$\begin{aligned}\mathrm{Tr}_{L/\mathbb{Q}}(\alpha \cdot \beta) &= \mathrm{Tr}_{K/\mathbb{Q}}(\mathrm{Tr}_{L/K}(\alpha \cdot \beta)) \\ &= \mathrm{Tr}_{K/\mathbb{Q}}(\alpha \cdot \mathrm{Tr}_{L/K}(\beta)).\end{aligned}$$

Since $\mathrm{Tr}_{L/K}(\beta) \in \mathcal{O}_K$ by definition, we get $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha \cdot \mathrm{Tr}_{L/K}(\beta)) \in \mathbb{Z}$ because $\alpha \in \mathcal{O}_K^\vee$.

By the inclusion $K \hookrightarrow L$, we get an inclusion $\mathcal{O}_K^\vee \hookrightarrow \mathcal{O}_L^\vee$, which (because $\mathcal{O}_K \subset \mathcal{O}_L$) gives a map

$$\mathcal{O}_K^\vee / \mathcal{O}_K \longrightarrow \mathcal{O}_L^\vee / \mathcal{O}_L.$$

Because $\mathcal{O}_L \cap K = \mathcal{O}_K$, this map is an injection, exhibiting $\mathcal{O}_K^\vee / \mathcal{O}_K$ as a subgroup of $\mathcal{O}_L^\vee / \mathcal{O}_L$.

Aside 8.3. We saw the following diagram in class:

$$\begin{tikzcd}
\mathcal{O}_K^\vee \arrow[r, hook] \arrow[d, dashed] & \mathcal{O}_L^\vee \arrow[d] \\
\mathcal{O}_K^\vee / \mathcal{O}_K \arrow[r, hook] & \mathcal{O}_L^\vee / \mathcal{O}_L
\end{tikzcd}$$

By Lagrange's theorem from group theory, we get that

$$|d_K| = \left|\frac{\mathcal{O}_K^\vee}{\mathcal{O}_K}\right| \quad \text{divides} \quad \left|\frac{\mathcal{O}_L^\vee}{\mathcal{O}_L}\right| = |d_L|.$$

□

8.2 Discriminant of Cyclotomic Extensions

Let's fix some notation: let L/K be a finite extension of fields, and $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n)^t$ a K-basis for L, expressed as a column vector. Also let

$$D(\underline{\alpha}) := \det(\mathrm{Tr}_{L/K}(\underline{\alpha} \cdot \underline{\alpha}^t)) \in K.$$

If $M \in M_n(K)$, let $\underline{\beta} = M \cdot \underline{\alpha}$. Then

$$D(\underline{\beta}) = (\det M)^2 D(\underline{\alpha}),$$

which we've proved before.

Lemma 8.4. *Suppose* $\mathrm{char} K = 0$*, and let* $\overline{K}$ *be a fixed algebraic closure of* K*. Let*

$$\sigma_1, \ldots, \sigma_n : L \hookrightarrow \overline{K}$$

be the $n = [L : K]$ *distinct embeddings*[a] $L \hookrightarrow \overline{K}$*. Then*

$$D(\underline{\alpha}) = \det(\sigma_k(\alpha_i))^2.$$

[a] These come from the fact that the extension L/K is separable.

Proof. The proof is a chain of computations:

$$\begin{aligned}
D(\underline{\alpha}) &= \det(\mathrm{Tr}_{L/K}(\alpha_i \cdot \alpha_j)) \\
&= \det\left(\sum_{\sigma_k} \sigma_k(\alpha_i \cdot \alpha_j)\right) \\
&= \det\left(\sum_{\sigma_k} \sigma_k(\alpha_i) \cdot \sigma_k(\alpha_j)\right) \\
&= \det\left((\sigma_k(\alpha_i))_{k,i} \cdot (\sigma_k(\alpha_j))_{k,j}^t\right) \\
&= \det((\sigma_k(\alpha_i))) \cdot \det((\sigma_k(\alpha_j))^t) \\
&= \det((\sigma_k(\alpha_i)))^2.
\end{aligned}$$

The fourth equality comes from factoring the sum into the product of two matrices (one can work this out by calculation). □

Corollary 8.5. *Suppose $L = K(\alpha)$, where α has minimum polynomial $f(x)$ of degree n. Then*

$$D(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_{L/K}(f'(\alpha)).$$

Proof. By the Lemma, $D(1, \alpha, \ldots, \alpha^{n-1}) = \det(\sigma_k(\alpha^j))^2$. This is just equal to

$$\det(\alpha_i^j)^2,$$

where $\alpha_1, \ldots, \alpha_n \in \overline{K}$ are the roots of $f(x)$. So, we must compute

$$\det \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ & & \vdots & & \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{pmatrix}^2 .$$

This is called a **Vandermonde determinant**, and there is a nice general form for computing it:

$$\begin{aligned} \det(\alpha_i^j)^2 &= \left(\prod_{i<j} (\alpha_i - \alpha_j) \right)^2 \\ &= (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j} (\alpha_i - \alpha_j). \end{aligned}$$

If we fix i, we claim

$$= (-1)^c \cdot \prod_j f'(\alpha_j). \tag{8.1}$$

We know that $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$, so

$$f'(x) = \sum_i (x - \alpha_1) \cdots \widehat{(x - \alpha_i)} \cdots (x - \alpha_n),$$

where the hat means to omit that factor from the product. Thus

$$f'(\alpha_i) = \prod_{i \neq j} (\alpha_i - \alpha_j).$$

So Eq. (8.1) is

$$\begin{aligned} &= (-1)^c \cdot \prod_k f'(\sigma_k(\alpha)) \\ &= (-1)^c \cdot \prod_k \sigma_k(f'(\alpha)) \\ &= (-1)^c \cdot N_{L/K}(f'(\alpha)), \end{aligned}$$

where $c = \frac{n(n-1)}{2}$, proving the proposition. □

Finally, Proof of Proposition 8.1. If $L = \mathbb{Q}(\zeta_p)$, $K = \mathbb{Q}$, we know $\mathcal{O}_L = \mathbb{Z}[\zeta_p]$, which has a $\mathbb{Z}$-basis $1, \zeta_p, \ldots, \zeta_p^{p-2}$. Recall that the cyclotomic polynomial $f(x)$ is

$$f(x) = \frac{x^p - 1}{x - 1}.$$

By the Lemma,

$$d_L = (-1)^{\frac{(p-2)(p-1)}{2}} N_{L/\mathbb{Q}}(f'(\zeta_p)).$$

Writing

$$(x-1)f(x) = x^p - 1$$

and differentiating both sides, we see

$$f'(\zeta_p) = \frac{p\zeta_p^{p-1}}{\zeta_p - 1}.$$

Thus

$$N_{L/\mathbb{Q}}(f'(\zeta_p)) = N_{L/\mathbb{Q}}\left(\frac{p\zeta_p^{p-1}}{\zeta_p - 1}\right).$$

Because the norm is multiplicative,

$$\begin{aligned} N_{L/\mathbb{Q}}(f'(\zeta_p)) &= p^{p-1}\frac{N_{L/\mathbb{Q}}(\zeta_p^{p-1})}{N_{L/\mathbb{Q}}(\zeta_p - 1)} \\ &= \frac{p^{p-1}}{N_{L/\mathbb{Q}}(\zeta_p - 1)} = p^{p-2}. \end{aligned}$$

□

9 February 10, 2017

Recall that last time, we found d such that $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(\zeta_p)$:

$$d = \begin{cases} p & p \equiv 1(4) \\ -p & p \equiv 3(4) \end{cases}.$$

Today, we wish to find this in a more "organic" way, using a fair bit more theory.

9.1 The Legendre Symbol

Definition 9.1. Let us define the **Legendre Symbol** $\left(\frac{-}{p}\right)$ by the composition

$$\left(\frac{-}{p}\right) : \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \xrightarrow{\simeq} (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow\!\!\!\!\rightarrow \{\pm 1\},$$

where the last map is thought of as the canonical map $\mathbb{Z}/(p-1)\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$.

Our task now is to write expicitly $\sqrt{d} \in \mathbb{Q}(\zeta_p)$. If $g \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, we see that

$$g(\sqrt{d}) = \begin{cases} \sqrt{d} & g \in \ker\left(\frac{-}{p}\right) \\ -\sqrt{d} & g \notin \ker\left(\frac{-}{p}\right) \end{cases}.$$

That is to say,

$$g(\sqrt{d}) = \left(\frac{g}{p}\right)\sqrt{d}.$$

For notational concision, write G to refer to $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. Let us now define an element $h \in \mathbb{Q}(\zeta_p)$ by

$$h = \sum_{\sigma \in G} \left(\frac{\sigma}{p}\right) \cdot \sigma(\zeta_p).$$

Note that if $\tau \in G$,

$$\tau(h) = \sum_{\sigma \in G} \left(\frac{\sigma}{p}\right) \tau\sigma(\zeta_p) = \left(\sum_{\sigma \in G} \left(\frac{\sigma}{p}\right)\left(\frac{\tau}{p}\right) \tau\sigma(\zeta_p)\right) \left(\frac{\tau}{p}\right)^{-1}.$$

As the Legendre symbol is a homomorphism, and for fixed τ, $\sigma\tau$ runs over all elements of G, this just gives

$$\tau(h) = h\left(\frac{\tau}{p}\right)^{-1} = h\left(\frac{\tau}{p}\right),$$

as the Legendre symbol of τ is its own inverse. This already implies that $\mathbb{Q}(h) \subseteq \mathbb{Q}(\zeta_p)$ is a quadratic subfield.

9.2 More on the Quadratic Subfield of a Cyclotomic Field

As a further calculation, we compute h^2.

> Kisin: *"This is kind of a cool computation."*

Via the isomorphism $G \cong (\mathbb{Z}/p\mathbb{Z})^\times$, we have

$$h^2 = \sum_{a,b \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\zeta_p^a \cdot \zeta_p^b.$$

We can change variables to rewrite this as

$$h^2 = \sum_{a,t \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{a}{p}\right)\left(\frac{ta}{p}\right)\zeta_p^a \cdot \zeta_p^{ta}$$

Because the Legendre symbol is a homomorphism, this is

$$\sum_{a,t}\left(\frac{a}{p}\right)^2\left(\frac{t}{p}\right)\zeta_p^{a(1+t)} = \sum_t\left(\frac{t}{p}\right)\sum_a \zeta_p^{a(1+t)}.$$

If $t \neq -1$ in $(\mathbb{Z}/p\mathbb{Z})^\times$, then

$$\sum_a \zeta_p^{a(1+t)} = \sum_a \zeta_p^a = \mathrm{Tr}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p) = 1,$$

by a computation we have done before.

If $t = -1$, then

$$\sum_a \zeta_p^{a(1+t)} = p - 1.$$

Note that

$$\sum_t \left(\frac{t}{p}\right) = 0.$$

Thus

$$h^2 = \left(\frac{-1}{p}\right)(p-1) - \sum_{t \neq -1}\left(\frac{t}{p}\right) = \left(\frac{-1}{p}\right)p.$$

So $h^2 = \left(\frac{-1}{p}\right)p$, and $h = \sqrt{\pm p}$. Let us now show precisely when $h = \sqrt{+p}$ and when $h = \sqrt{-p}$. We know that $\left(\frac{-1}{p}\right) = 1$ if and only if -1 is a quadratic residue in $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$. This is true if and only if $(-1)^{\frac{p-1}{2}} = 1 \in (\mathbb{Z}/p\mathbb{Z})^\times$. (Why? If $\gamma \in (\mathbb{Z}/p\mathbb{Z})^\times$ is a generator, then $(-1) = \gamma^i$. Thus i is even if and only if $(\gamma^i)^{\frac{p-1}{2}} = 1$.) Because $(-1)^{\frac{p-1}{2}} = 1$ if and only if $p \equiv 1(4)$, this gives us precisely the same answer as before:

$$g^2 = \begin{cases} p & p \equiv 1(4) \\ -p & p \equiv 3(4). \end{cases}$$

9.3 Motivation for Dedekind Domains

We have been discussing number fields K and their rings of integers, $\mathcal{O}_K \subseteq K$. In one particularly nice example, $\mathbb{Z} \subseteq \mathbb{Q}$, we have *unique factorization into prime numbers*, the so-called "Fundamental Theorem of Arithmetic."

Recall that in any domain D, $f \in D$ is called **irreducible** if one cannot write $f = f_1 \cdot f_2$ for $f_1, f_2 \notin D^\times$. In a Dedekind domain, we do not quite have unique factorization into irreducibles:

Example 9.2. Consider the number field $K = \mathbb{Q}(\sqrt{-5})$. Its ring of integers $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ is a Dedekind domain, but

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

are two factorizations of 6 into irreducibles.

In a Dedekind domain, we *do* have factorization of ideals into unique prime *ideals*. Moreover, we have a group structure on ideals (with inverses).

Definition 9.3. As a stray definition, we say the **class group** of a number field is the group $\mathrm{Cl}_K := \{\text{group of nonzero ideals of } \mathcal{O}_K\}/\{\text{principal ideals}\}$. It is a theorem that this group is finite for any number field.

10 February 13, 2017

10.1 Dedekind Domains: Definitions and First Examples

Definition 10.1. A **Dedekind domain** is a [commutative unital] ring A such that

1. A is **Noetherian**
2. Any nonzero prime ideal $\mathfrak{p} \subseteq A$ is maximal
3. A is a domain integrally closed in its field of fractions frac$A$.

Remark 10.2. Recall that a ring is **Noetherian** if any increasing sequence of ideals stabilizes. Also recall that an ideal $\mathfrak{p}$ is **prime** if for $a, b \in A$, $ab \in \mathfrak{p}$ implies $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.

Proposition 10.3. *Let K be a number field. Then $\mathcal{O}_K$ is a Dedekind domain.*

Proof. (1) We know $\mathcal{O}_K \cong \mathbb{Z}^n$, where n is the degree $[K : \mathbb{Q}]$ of the field extension. Since $\mathbb{Z}^n$ is a finitely-generated $\mathbb{Z}$-module, and $\mathbb{Z}$ is Noetherian, $\mathbb{Z}^n$ is Noetherian as well. One way to see this is by invoking the Hilbert Basis Theorem, and writing $\mathbb{Z}^n$ as $\mathbb{Z}[x_1, \dots, x_n]/(x_1 - 1, x_2 - 1, \dots, x_n - 1)$, noting that the quotient of a Noetherian ring is Noetherian.

(3) We know that $\mathcal{O}_K$ is a domain, and by the homework, $\mathcal{O}_K$ is integrally closed in K. Quick reminder as to how that proof works: if $\alpha \in K$ is integral over $\mathcal{O}_K$, then $\mathcal{O}_K[\alpha]$ is integral over $\mathcal{O}_K$, which is integral over $\mathbb{Z}$. Thus $\mathcal{O}_K[\alpha]$ is integral over $\mathbb{Z}$, so α is in $\mathcal{O}_K$.

(2) This property is the strongest of the three, so it will be the most interesting to verify. Let's begin with a definition: an **order** $B \subseteq K$ is a subring which is finitely generated as a $\mathbb{Z}$-module, such that $B \otimes_{\mathbb{Z}} \mathbb{Q} \cong K$, i.e., frac $B = K$.

Lemma 10.4. *If $B \subseteq K$ is an order and $I \subseteq B$ is a nonzero ideal, then $|B/I|$ is finite.*

Proof. Let $\alpha \in I$ be nonzero. Then $P_\alpha(x) = \det_{\mathbb{Z}}(x - \tilde{\alpha}|_B)$, so $P_\alpha(\alpha) = 0$. (*Note*: B is free because it is a subring of a field, so there is no torsion.) Write

$$P_\alpha(\alpha) = \alpha^d + a_{d-1}\alpha^{d-1} + \cdots + a_0,$$

where $a_0 = \pm N_{K/\mathbb{Q}}(\alpha)$. Therefore, $N_{K/\mathbb{Q}}(\alpha) \in I$, which is an integer $m \in \mathbb{Z}$, so $I \supseteq m \cdot B$. Thus, B/mB surjects onto B/IB, and $B/mB \cong \mathbb{Z}^n/m\mathbb{Z}^n$, which has finite order. □

Now suppose $\mathfrak{p} \subseteq \mathcal{O}_K$ is a prime ideal. By the Lemma, $\mathcal{O}_K/\mathfrak{p}$ is a finite domain.

Lemma 10.5. *A finite domain C is a field.*

Proof. Let $\alpha \in C$ be nonzero. Observe that the map $C \xhookrightarrow{\alpha\cdot -} C$ is injective because C is a domain. By the pigeon-hole principle, $\widetilde{\alpha}$ is surjective as well. In particular, there exists some $x \in C$ such that $\alpha x = 1$. □

This finishes our proof: $\mathcal{O}_K/\mathfrak{p}$ is a field, so $\mathfrak{p}$ is maximal. □

10.2 Unique Factorization in Dedekind Domains

Let A be a Dedekind domain and $K = \operatorname{frac} A$. If $I, J \subseteq K$ are additive subgroups, we define

$$\begin{aligned} I \cdot J &= \{\text{additive subgroup generated by } \alpha \cdot \beta, \alpha \in I, \beta \in J\} \\ I + J &= \{\alpha + \beta : \alpha \in I, \beta \in J\}. \end{aligned}$$

Remark 10.6. If I, J are A-submodules, then so are $I \cdot J$ and $I + J$. If $I, J \subseteq A$ are ideals, then so are $I \cdot J$ and $I + J$.

Definition 10.7. A **fractional ideal** $I \subseteq K$ is an A-submodule such that for some nonzero $d \in A$, $d \cdot I \subseteq A$. That is to say, if $d' \in I$ is nonzero, $d' = ad^{-1}$ for some $a \in A$. Note that this is *not* the same thing as saying the preimage of I under the localization at d map is an ideal.

Lemma 10.8. *If I, J are fractional ideals, then so are $I \cdot J$ and $I + J$.*

Proof. Choose $d, d' \in A$ nonzero such that $dI \subseteq A$ and $d'J \subseteq A$. Then $dd'(I \cdot J)$ and $dd'(I + J) \subseteq A$. □

Remark 10.9. If I is an A-submodule, $I \cdot A = I$.

Theorem 10.10. *Let A be a Dedekind domain. Then*

(i) The fractional ideals in $K = \operatorname{frac} A$ form a group under ideal multiplication, with unit A. In particular, for every fractional ideal $I \subseteq K$, there is a fractional ideal $I^{-1} \subseteq K$ such that $I \cdot I^{-1} = A$.

(ii) Every fractional ideal $\mathfrak{b} \subseteq K$ can be written uniquely (up to ordering and multiplication by units) as

$$\mathfrak{b} = \prod_{\mathfrak{p} \text{ prime}} \mathfrak{p}^{n(\mathfrak{p})}, \quad n(\mathfrak{p}) \in \mathbb{Z},$$

where $\mathfrak{p}^{-n}$ means $(\mathfrak{p}^{-1})^n$.

11 February 15, 2017

The goal of this lecture is to exhibit some common problem-solving and computational techniques for factoring ideals into irreducibles. While we will not state nor prove any theorems, this is an important lecture.

11.1 Example: Factoring 6 in Two Ways

Recall that in $\mathbb{Z}[\sqrt{-5}]$, $6 = (1+\sqrt{-5})(1-\sqrt{-5}) = 2 \cdot 3$ are two different factorizations into irreducibles. As an example, let us check that $1+\sqrt{-5}$ is irreducible. Suppose $1+\sqrt{-5} = a \cdot b$, where $a, b \in \mathbb{Z}[\sqrt{-5}]$. Apply the

11.2 Example: How can we factor 21?

12 February 17, 2017

12.1 The Beginnings of Unique Factorization

Proposition 12.1. *Let A be a Dedekind domain, and $0 \neq \mathfrak{m} \subsetneq A$ a nonzero maximal ideal. Then $\mathfrak{m}$ is invertible: there exists a fractional ideal $\mathfrak{m}' \subseteq K = \operatorname{frac} A$ such that $\mathfrak{m} \cdot \mathfrak{m}' = A$.*

Proof. Let $\mathfrak{m}' = \{x \in K : x\mathfrak{m} \subseteq A\}$. This clearly contains A. If $d \neq 0 \in \mathfrak{m}$, then $d \cdot \mathfrak{m}' \subseteq A$, so $\mathfrak{m}'$ is a fractional ideal. Moreover,

$$\mathfrak{m} \subseteq \mathfrak{m} \cdot \mathfrak{m}' \subseteq A,$$

so by maximality of $\mathfrak{m}$, either $\mathfrak{m} \cdot \mathfrak{m}' = A$ and we are done, or $\mathfrak{m} \cdot \mathfrak{m}' = \mathfrak{m}$. Suppose $\mathfrak{m} \cdot \mathfrak{m}' = \mathfrak{m}$. Let $x \in \mathfrak{m}'$. Then

$$\mathfrak{m} \supseteq x \cdot \mathfrak{m} \supseteq x^2 \cdot \mathfrak{m} \supseteq \cdots \supseteq x^i \cdot \mathfrak{m} \supseteq \cdots$$

Thus if $d \neq 0 \in \mathfrak{m}$, $x^n \cdot d \in \mathfrak{m} \subseteq A$ for all n, i.e., $x^n \in d^{-1}A$ for all $n = 1, 2, \ldots$. As $A[x] \subseteq d^{-1}A$, which is Noetherian, $A[x]$ is finitely generated. In particular, x is integral over A. But a Dedekind domain is integrally closed in its field of fractions! So $x \in A$. Thus $\mathfrak{m}' \subseteq A$, and $\mathfrak{m}' = A$. We now state two lemmas to help us conclude the proof; we will prove them after.

Lemma 12.2. *If A is a commutative ring with unity, and $\mathfrak{a}_1, \ldots \mathfrak{a}_n \subseteq A$ are ideals, and $\mathfrak{p} \subseteq A$ is a prime ideal such that*

$$\mathfrak{a}_1 \cdots \mathfrak{a}_n \subseteq \mathfrak{p},$$

then $\mathfrak{a}_i \subseteq \mathfrak{p}$ for some i.

Lemma 12.3. *Let A be a Noetherian domain, and $\mathfrak{a} \subseteq A$ a nonzero ideal. Then $\mathfrak{a}$ contains a product of prime ideals.*

Equipped with these lemmas, we may now finish the proof. We wish to find some $b \in \mathfrak{m}'$ such that $b \notin A$. Let $a \in \mathfrak{m}$ be nonzero. By Lemma 12.3, $A \cdot a$ contains a product of nonzero prime ideals $\mathfrak{p}_1 \cdots \mathfrak{p}_n$. Take n to be as small as possible. In particular, $\mathfrak{m} \supseteq A \cdot a \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_n$, so by Lemma 12.2, $\mathfrak{m} \supseteq \mathfrak{p}_\mathfrak{i}$ for some i, say $i = 1$. Because we're in a Dedekind domain and all prime ideals are maximal, $\mathfrak{m} \supseteq \mathfrak{p}_1 \Rightarrow \mathfrak{m} = \mathfrak{p}_1$. Let $\mathfrak{b} = \mathfrak{p}_2 \cdots \mathfrak{p}_n$ (in the case that there was only one factor to begin with, $\mathfrak{b} = A$). Then $A \cdot a \not\supseteq \mathfrak{b}$, by minimality of n.

Thus there exists some $b \in \mathfrak{b}$ such that $b \notin A \cdot A$. But $\mathfrak{m} \cdot b \subseteq \mathfrak{m} \cdot \mathfrak{b} = \mathfrak{p}_1 \cdot \mathfrak{b} \subseteq A \cdot a$. This implies $\mathfrak{m} \cdot (b \cdot a^{-1}) \subseteq A$, so $ba^{-1} \in \mathfrak{m}'$; contradiction. Therefore $\mathfrak{m}' \neq A$, and we are done. □

Now we finish by proving the two lemmas used in the proof of the proposition.

Proof of Lemma 12.2. If $\mathfrak{a}_i \not\subseteq \mathfrak{p}$ for all i, choose $a_i \in \mathfrak{a}_i$ with $a_i \notin \mathfrak{p}$. Then $a_1 \cdots a_n \notin \mathfrak{p}$. But $a_1 \cdots a_n \in \mathfrak{a}_1 \cdots \mathfrak{a}_n \subseteq \mathfrak{p}$; contradiction. □

Proof of Lemma 12.3. Let Φ be the set of ideals in A which do not contain a product of primes. If $\Phi = \varnothing$, then we are done, so suppose that Φ is nonempty. Then Φ contains a maximal element, because A is Noetherian, call it $\mathfrak{b}$. Because $\mathfrak{b} \in \Phi$, $\mathfrak{b}$ is not prime, so there exist $x, y \in A$ not in $\mathfrak{b}$ such that $x \cdot y \in \mathfrak{b}$. Thus $\mathfrak{b} + A \cdot x \supsetneq \mathfrak{b}$ and $\mathfrak{b} + A \cdot y \supsetneq \mathfrak{b}$, but $(\mathfrak{b} + A \cdot x) \cdot (\mathfrak{b} + A \cdot y) \subseteq \mathfrak{b}$. By maximality of $\mathfrak{b}$, neither $\mathfrak{b} + A \cdot x$ nor $\mathfrak{b} + A \cdot y$ are in Φ, so $(\mathfrak{b} + A \cdot x) \cdot (\mathfrak{b} + A \cdot y) \notin \Phi$, and $\mathfrak{b} \notin \Phi$, contradiction. □

13 February 22, 2017

Professor Kisin is away this week. His graduate student Koji Shimizu is lecturing in his place.

13.1 Unique Factorization in Dedekind Domains

The purpose of today is to prove the main theorem that we've stated a few times already:

Theorem 13.1. *Let A be a Dedekind domain with fraction field K.*

1. *Fractional ideals form a group under multiplication with unit A.*
2. *For each fractional ideal $\mathfrak{b} \subseteq K$, we have a unique decomposition of $\mathfrak{b}$ into a product of primes*
$$\mathfrak{b} = \prod_{\substack{\mathfrak{p} \subseteq A \\ \text{prime}}} \mathfrak{p}^{n(\mathfrak{p})},$$
where $n(\mathfrak{p}) \in \mathbb{Z}$ is zero for all but finitely many $\mathfrak{p}$.

Remark 13.2. We proved last time that for $\mathfrak{p} \subseteq A$ maximal, there exists some fractional ideal $\mathfrak{p}'$ such that $\mathfrak{p} \cdot \mathfrak{p}' = A$. We thus define $\mathfrak{p}^{-1} = \mathfrak{p}'$, so it makes sense to have negative exponents in Theorem 13.1.

Remark 13.3. The inverse $\mathfrak{p}'$ is unique. The usual argument to show uniqueness of inverses holds here as well.

Proof of existence. Take a fractional ideal $\mathfrak{b} \subseteq K$. We will reduce to the case where $\mathfrak{b} \subseteq A$ is a proper ideal. By definition, there exists some nonzero $d \in A$ such that $d \cdot \mathfrak{b} \subseteq A$. Thus we can write
$$\mathfrak{b} = (d \cdot \mathfrak{b})(d \cdot A)^{-1},$$
where both $d \cdot \mathfrak{b}$ and $d \cdot A$ are proper ideals. We may thus assume that $\mathfrak{b} \subseteq A$ is an ideal. Define
$$\Phi = \left\{ \mathfrak{a} \subseteq A : \mathfrak{a} \,{}^{\text{is a nonzero ideal that does not}}_{\text{admit a prime decomposition}} \right\}.$$
Because A is Noetherian, if Φ is nonempty, it has a maximal element $\mathfrak{a} \in \Phi$. In particular, we have $\mathfrak{a} \neq A$, because A has a prime decomposition. So there exists some maximal ideal $\mathfrak{p} \subseteq A$ such that
$$\mathfrak{a} \subseteq \mathfrak{p}.$$
Recall that if $\mathfrak{p}'$ is the inverse of $\mathfrak{p}$, then $\mathfrak{p}' \supseteq A$. We have the following:

1. As $\mathfrak{a} \subseteq \mathfrak{p}$, $\mathfrak{a}\mathfrak{p}' \subseteq \mathfrak{p} \cdot \mathfrak{p}' = A$.
2. As $A \subseteq \mathfrak{p}'$, we have $\mathfrak{a} = \mathfrak{a}A \subseteq \mathfrak{a} \cdot \mathfrak{p}'$.

Together, these imply $\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}' \subseteq A$.

Now, we claim that $\mathfrak{a} \subsetneqq \mathfrak{a}\mathfrak{p}'$. To see this, suppose to the contrary that $\mathfrak{a} = \mathfrak{a}\mathfrak{p}'$. Take any $x \in \mathfrak{p}'$. Then

$$\mathfrak{a} \cdot x \subseteq \mathfrak{a}.$$

Repeating this process, we see that for all $n \in \mathbb{N}$, $\mathfrak{a}x^n \subseteq \mathfrak{a} \subseteq A$. Take some nonzero $d \in \mathfrak{a}$. Then $d \cdot x^n \in A$, so $x^n \in d^{-1}A$ for all $n \geq 0$. The fractional ideal $d^{-1}A$ is, in particular, a finite A-module, so this gives that x is integral over A. Since A is integrally closed in K, we must have $x \in A$. Thus $A = \mathfrak{p}'$, which is a contradiction.

As $\mathfrak{a}$ is maximal in Φ, we must have $\mathfrak{a} \cdot \mathfrak{p}' \notin \Phi$. Therefore $\mathfrak{a} \cdot \mathfrak{p}'$ can be factored as

$$\mathfrak{a} \cdot \mathfrak{p}' = \prod \mathfrak{q}^{n(\mathfrak{q})},$$

and

$$\mathfrak{a} = \mathfrak{a} \cdot \mathfrak{p}' \cdot \mathfrak{p} = \mathfrak{p} \cdot \prod \mathfrak{q}^{n(\mathfrak{q})}.$$

This finishes the proof of existence. □

Proof of uniqueness. Suppose that we have

$$\prod \mathfrak{p}^{n(\mathfrak{p})} = \prod \mathfrak{p}^{m(\mathfrak{p})}.$$

Rewrite this as

$$\mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_r^{\alpha_r} = \mathfrak{q}_1^{\beta_1} \cdots \mathfrak{q}_s^{\beta_s}$$

where the $\mathfrak{p}_i$ and $\mathfrak{q}_j$ are distinct prime ideals, and α_i and β_j are positive integers.

The case where $r = s = 0$ is obviously fine. Without loss of generality, assume $r > 0$. We see

$$\mathfrak{p}_1 \supseteq \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_r^{\alpha_r} = \mathfrak{q}_1^{\beta_1} \cdots \mathfrak{q}_s^{\beta_s},$$

so if $s = 0$ then $\mathfrak{p}_1 \supseteq A$, which contradicts $\mathfrak{p}_1$ being a prime ideal of A. So suppose $s > 0$. Recall Lemma 2 from last class: if $\mathfrak{p} \subseteq A$ is a prime ideal and $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subseteq A$ are non-zero ideals, then $\mathfrak{p} \supseteq \mathfrak{a}_1 \cdots \mathfrak{a}_n$ implies $\mathfrak{p} \supseteq \mathfrak{a}_i$ for some i. Therefore, there exists some j such that

$$\mathfrak{p}_1 \supseteq \mathfrak{q}_j,$$

which contradicts the fact that the $\mathfrak{q}_j$ are maximal, and all the primes are distinct. □

Corollary 13.4. *Let $I, J \subseteq K$ be fractional ideals of a Dedekind domain A. Write*

$$I = \prod \mathfrak{p}^{n(\mathfrak{p})}, \qquad J = \prod \mathfrak{p}^{m(\mathfrak{p})}.$$

Then $I \subseteq J$ if and only if $n(\mathfrak{p}) \geq m(\mathfrak{p})$ for all $\mathfrak{p}$.

Proof. In one direction, suppose $n(\mathfrak{p}) \geq m(\mathfrak{p})$ for all $\mathfrak{p}$. Then $n(\mathfrak{p}) - m(\mathfrak{p})$ is non-negative for all $\mathfrak{p}$, so

$$\begin{aligned} I = \prod \mathfrak{p}^{n(\mathfrak{p})} &= \prod \mathfrak{p}^{m(\mathfrak{p})} \cdot \left(\prod \mathfrak{p}^{n(\mathfrak{p})-m(\mathfrak{p})}\right) \\ &\subseteq \prod \mathfrak{p}^{m(\mathfrak{p})} = J. \end{aligned}$$

□

14 February 24, 2017

Professor Kisin is still away, so Koji is lecturing again.

14.1 Wrapping up from Last Time

Remember that last time we proved the main theorem of Dedekind domains, Theorem 13.1.

Lemma 14.1. *Let $p \in \mathbb{Z}$ be a rational prime, and K be a number field. Suppose $\mathcal{O}_K = \mathbb{Z}[\alpha] = \mathbb{Z}[x]/(f(x))$. Let $\overline{f}(x) \in (\mathbb{Z}/p)[x]$ be the reduction mod p of $f(x)$, and write*

$$\overline{f}(x) = \overline{f}_1^{e_1} \cdots \overline{f}_s^{e_s}$$

where the $\overline{f}_i$ are distinct and irreducible. Then

$$(p) = \prod \mathfrak{p}_i^{e_i} \quad \text{in } \mathcal{O}_K,$$

where $\mathfrak{p}_i = (p, f_i(\alpha))$ for $f_i \in \mathbb{Z}[x]$ a lift of $\overline{f}_i$.

Exercise 14.2. If $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$, then show using this argument that $(p) = (\zeta_p - 1)^{p-1}$.

Proof. Let $I := \prod \mathfrak{p}_i^{e_i} \subseteq \mathcal{O}_K$. This is an ideal because e_i are positive. We will prove $I = (p)$. Consider the following diagram:

$$\begin{tikzcd}
I \arrow[r, hook] \arrow[d, equal] & \mathcal{O}_K \arrow[r, two heads] \arrow[d, equal] & \mathcal{O}_K/(p) \arrow[d, equal] \\
\prod (p, f_i(x))^{e_i} \arrow[r, hook] & \mathbb{Z}[x]/(f(x)) \arrow[r, two heads] & (\mathbb{Z}/p)[x]/(\overline{f}(x))
\end{tikzcd}$$

This tells us that I goes to 0 under the map $\mathcal{O}_K \to \mathcal{O}_K/(p)$, which means that $I \subseteq (p)$. So

$$(p) = \prod \mathfrak{p}_i^{e_i'}$$

with $0 \le e_i' \le e_i$ by corollary from last time; suffice it to show that $e_i' = e_i$ for all i.

If $e_i' < e_i$ for some i, then

$$(p) = \prod (p, f_j(x))^{e_j'} \ni f_1^{e_1'} \cdots f_s^{e_s'} = g$$

and consider g. Then $\deg g < \deg f$, so g does not go to zero under the reduction $\mathbb{Z}[x]/(f(x)) \to (\mathbb{Z}/p)[x]/(\overline{f})$. But this is a contradiction, because $g \in (p)$. Thus $e_i = e_i'$ for all i, and thus $(p) = I = \prod \mathfrak{p}_i^{e_i}$. □

14.2 Examples and Pictures of Dedekind Domains

The rest of today is to give some big picture ideas about how Dedekind domains come up.

Notation 14.3. For a ring A, $\operatorname{mSpec} A$ is the set of maximal ideals of A.

Example 14.4. Examples of Dedekind domains:

1. Fields.
2. $\mathcal{O}_K$ for K a number field (also the localization and completion[5] of such).

   Theorem 14.5. *$\mathcal{O}_K$ has a finite class group (recall that $\mathrm{C}\ell_K$ is the group of fractional ideals modulo principal fractional ideals).*

   Proof. Will be given next week. □

3. If k is a field, then $k[x]$ is a Dedekind domain (more strongly, it is a PID).

From this last example, we want to create more examples. Recall that $\mathcal{O}_K = \mathbb{Z}[y]/(f(y))$. Motivated by this, take $f(x,y) \in k[x,y] = (k[x])(y)$, and consider $A = k[x,y]/(f(x,y))$.

Question 14.6. Which A are Dedekind domains?

1. $f = y^2 - x^2$
2. $f = y^2 - x^3$
3. $f = y^2 - (x^3 + x)$.

Number 1 is not a domain, because $y - x$, $y + x \neq 0 \in A$, but $(y-x)(y+x) = 0$ in A. It turns out that both of the others are domains. Consider number 2, and the element $z = \frac{y}{x} \in \operatorname{frac} A \setminus A$. But $z^2 = \frac{y^2}{x^2} = x \in A$, so z satisfies $z^2 - x = 0$. Thus z is integral over A, but not in A. It turns out that number 3 *does* give a Dedekind domain.

From now on, assume $k = \mathbb{C}$, or some algebraically closed field (of any characteristic). Let's record a few facts:

Theorem 14.7. Hilbert's Nullstellensatz. *If k is algebraically closed, then*

$$\operatorname{mSpec}(k[x,y]/(f(x,y))) = \{(x-a, y-b) : f(a,b) = 0\}$$

Theorem 14.8. Consequence of Jacobian criterion. *Suppose $A = k[x,y]/(f(x,y))$ is*

[5] Completion is in the sense of 3-adic integers, for example

an integral domain. Then A is a Dedekind domain if there is no $(a, b) \in k^2$ such that

$$\begin{cases} f(a,b) = 0 \\ (\partial_x f)(a,b) = 0 \\ (\partial_y f)(a,b) = 0 \end{cases}$$

This essentially says that A is a Dedekind domain if f has no singularities.

Example 14.9. In our example 2, the equations $f = y^2 - x^3 = 0$, $\partial_x f = -3x^2 = 0$ and $\partial_y f = 2y = 0$ has a solution $(0, 0) \in k^2$; thus $\mathbb{C}[x, y]/(y^2 - x^3)$ is not a Dedekind domain.

In our example 3, $f = y^2 - (x^3 + x) = 0$, $\partial_x f = -3x^2 + 1 = 0$, and $\partial_y f = 2y = 0$ has no solution in $\mathbb{C}^2$. Thus

$$A = \mathbb{C}[x, y]/(y^2 - (x^3 + x))$$

is a Dedekind domain.

For this ring A, we know that $C\ell_A$ is infinite (cf. Fröhlich-Taylor, *Algebraic Number Theory* (VI.5)).

Brief Idea. We consider $E = \operatorname{mSpec} A \cup \{\infty\}$. This is an **elliptic curve** over $\mathbb{C}$, and we write $E/\mathbb{C}$. The curve E has the structure of an abelian group. We also have the following two exact sequences:

$$\begin{tikzcd}
 & & 0 \arrow[d] & & \\
 & & E \arrow[d] & & \\
0 \arrow[r] & \mathbb{Z} \arrow[r] & C\ell_E \arrow[r] \arrow[d] & C\ell_A \arrow[r] & 0 \\
 & & \mathbb{Z} \arrow[d] & & \\
 & & 0 & &
\end{tikzcd}$$

Since E is an uncountable group, this implies that $C\ell_A$ is uncountable. □

14.3 Scheme Theory

This is a modern way of studying algebraic geometry which combines the classical theory and number theory. Let D be a Dedekind domain that is not a field. Then $\operatorname{mSpec} D$ looks like a smooth curve. Can we draw a similar picture for *any* ring A?

Notation 14.10. $\operatorname{Spec} A$ is the set of prime ideals of A.

Example 14.11. $\operatorname{Spec}(k)$, where k is a field, is $\{(0)\}$. $\operatorname{Spec} \mathbb{Z} = \{(0)\} \cup \{(2), (3), \dots\}$.

Exercise 14.12. A ring homomorphism $f : A \to B$ gives a map $\operatorname{Spec} B \to \operatorname{Spec} A$. This is the reason that we consider Spec and not just mSpec.

Let's end with several pictures! Koji draws pictures of $\operatorname{Spec} \mathbb{Q}[x]$ and $\operatorname{Spec} \mathbb{Z}$.

15 February 27, 2017

15.1 The Geometry of Numbers

The ultimate goal of the next few lectures is to introduce the theory known as *The Geometry of Numbers*, and use it to prove finiteness of the class group of the ring of integers of a number field. To summarize, this is our aim:

Aim: If K is a number field, show that $|\mathrm{C}\ell_K| < \infty$.

The idea is as follows: we look at all embeddings of $K \xhookrightarrow{\sigma_i} \mathbb{C}$. By standard results from field theory, there are $[K : \mathbb{Q}]$ such embeddings. To see this, the primitive element theorem allows us to write

$$K \cong \mathbb{Q}[x]/f(x),$$

where $f(x) \in \mathbb{Q}[x]$ is a monic, irreducible polynomial. The embeddings σ_i correspond precisely to the roots of $f(x)$. We have real embeddings $\sigma_1, \ldots, \sigma_{r_1} : K \hookrightarrow \mathbb{R}$, and complex embeddings $\sigma_{r_1+1}, \ldots, \sigma_{r_1+r_2} : K \hookrightarrow \mathbb{C}$, as well as their complex conjugates $\overline{\sigma_{r_1+1}}, \ldots, \overline{\sigma_{r_1+r_2}} : K \hookrightarrow \mathbb{C}$. Thus we have

$$r_1 + 2r_2 = [K : \mathbb{Q}].$$

We can thus build a map

$$\begin{tikzcd}
K \arrow[r, hook, "\sigma"] \arrow[d] & \prod_{i=1}^{r_1} \mathbb{R} \times \prod_{i=r_1+1}^{r_1+r_2} \mathbb{C} \\
K \otimes_{\mathbb{Q}} \mathbb{R} \arrow[ur, dashed, "\sim"] &
\end{tikzcd}$$

and get that the dashed map is an isomorphism. This is because we have a composition

$$K \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\sim} \mathbb{R}[x]/f(x) \xrightarrow{\sim} \prod_i \mathbb{R}[x]/f_i(x),$$

where $f = f_1(x) \cdots f_s(x)$, and the $f_i(x)$ are distinct and irreducible. We can make this happen because f is separable, i.e., has distinct roots. So

$$\prod_i \mathbb{R}[x]/f_i(x) \cong \prod_{\substack{\sigma_i \\ i=1,\ldots,r_1}} \mathbb{R} \times \prod_{\substack{\sigma_i \\ i=r_1+1,\ldots,r_1+r_2}} \mathbb{C}.$$

as rings. That is to say, the diagram

$$\begin{tikzcd}
K \otimes_{\mathbb{Q}} \mathbb{R} \arrow[r, "\sim"] & \mathbb{R}[x]/f(x) \arrow[r, "\sim"] & \prod_i \mathbb{R}[x]/f_i(x) \arrow[d, phantom, "\rotatebox{90}{$\cong$}"] \\
K \arrow[u] \arrow[rr] & & \prod_{\sigma_i} \mathbb{R} \times \prod_{\sigma_i} \mathbb{C}
\end{tikzcd}$$

commutes. The following diagram may also be useful, where $\mathfrak{a} \subset \mathcal{O}_K$ is an ideal.

$$\begin{tikzcd}
\mathcal{O}_K \subseteq K \arrow[r, hook] \arrow[d, phantom, "\rotatebox{90}{$\subseteq$}"] \arrow[rrd, bend right, "\sigma"'] & K \otimes_{\mathbb{Q}} \mathbb{R} \arrow[r, "\sim"] & \prod_{\sigma_i} \mathbb{R} \times \prod_{\sigma_i} \mathbb{C} \arrow[d, phantom, "\rotatebox{90}{$\cong$}"] \\
\mathfrak{a} & & \mathbb{R}^{[K:\mathbb{Q}]}
\end{tikzcd} \tag{15.1}$$

16 March 1, 2017

16.1 Lattices

17 March 3, 2017

17.1 The Minkowski Theorem

18 March 6, 2017

18.1 Geometry of Numbers Continued

19 March 8, 2017

19.1 Finiteness of the Class Group

20 March 10 2017

20.1 Examples of Class Groups

20.2 Algebraic Closure of the Complex Numbers

21 March 22, 2017

21.1 Number Fields with Bounded Discriminant

22 March 24, 2017

22.1 The Unit Theorem

22.2 Proof for Real Quadratic Fields

23 March 27, 2017

23.1 The Unit Theorem, Continued

24 March 29, 2017

24.1 Applications of the Unit Theorem

24.2 Pell's Equation

25 March 31, 2017

25.1 Factorization of Primes in Extensions

25.2 The Different

26 April 3, 2017

26.1 Factorization Continued

27 April 5, 2017

27.1 Ramification and Degree of an Extension

28 April 7, 2017

28.1 Norm of the Different

28.2 Action of the Galois Group

29 April 10, 2017

29.1 Finite Fields

29.2 Frobenius Elements

30 April 12, 2017

30.1 More on the Galois Action

30.2 Decomposition Group and Inertia Group

31 April 14, 2017

31.1 Example: Frobenius in Cyclotomic Extensions

31.2 Quadratic Reciprocity

32 April 17, 2017

32.1 Quadratic Reciprocity Continued

32.2 Application to Primes of the Form $x^2 + ny^2$

33 April 19, 2017

33.1 Valuations and Discrete Valuation Rings

33.2 Completions of Number Fields

34 April 21, 2017

34.1 More on Completions

34.2 The Decomposition Group and $\mathfrak{p}$-norm

35 April 24, 2017

35.1 Galois Groups of Completions

36 April 26, 2017

36.1 Adeles and Ideles

36.2 The Idele Class Group and Compactness of C_K°

A Homework Problems and Solutions

A.1 Problem Set 1

Problem A.1.1. Let L/K be an extension of number fields, and let $a \in L$. Show that there exists a unique monic polynomial $f \in K[x]$ such that for all $g \in K[x]$, we have $g(a) = 0$ if and only if $g = f \cdot h$ for some $h \in K[x]$. The polynomial f is called the **minimal polynomial** of a over K.

Solution. Consider the set $V_a = \{f \in K[x] : f(a) = 0, f \text{ monic}\}$. We know from lecture that this set is nonempty; let $f_a(x) \in V_a$ be a polynomial of least degree in V_a. If $g(a) = 0$, the division algorithm gives $g = f_a \cdot h + r$, where $h, r \in K[x]$, $\deg h < \deg g$, $\deg r < \deg f_a$. Therefore $f_a(a) \cdot h(a) + r(a) = 0$. Since $f(a) = 0$, this implies $r(a) = 0$. If r is a nonzero polynomial, though, we can divide r by its leading coefficient to get a polynomial $r' \in K[x]$ with degree strictly less than $\deg f_a$ which vanishes on a, contradicting minimality of f_a. Thus $r(x) = 0$, and $g = f_a \cdot h$.

It follows as well that f_a is the *unique* monic polynomial of least degree which vanishes on a: if $f'(a) = 0$ and $\deg f_a = \deg f'$, then $f' = f_a \cdot h$ for some $h \in K[x]$ with $\deg h = \deg f' - \deg f_a = 0$. We see, then, that h must be the identity, in order that f' is still monic. Thus $f' = f_a$.

Problem A.1.2. Let f and g be two monic polynomials with rational coefficients such that $f \cdot g$ has integer coefficients. Prove that f and g have integer coefficients.

Solution. Note that we can find integers $a, b \in \mathbb{Z}$ such that af and $bg \in \mathbb{Z}[x]$, and further that the coefficients of f are coprime, and the coefficients of g are coprime. Set $f' = af$ and $g' = bg$. Let us state and prove a lemma:

Lemma A.1. *If $f, g \in \mathbb{Z}[x]$ have coprime coefficients, then fg has coprime coefficients.*

Proof. Let $p \in \mathbb{Z}$ be a prime; we show that there is some coefficient c_n of fg such that $p \nmid c_n$. We can write

$$c_n = \sum_{i+j=n} a_i b_j,$$

where the a_i are the coefficients of f, and the b_j are the coefficients of g. Let i be the least integer such that $a_i \neq 0$ and a_i is not divisible by p, and the same with j for the b_j. Then $n = i + j$ is such that c_n is not divisible by p, and we are done. □

With this lemma in hand, write $h = fg$, and

$$h = \frac{1}{a} f' \frac{1}{b} g'.$$

Then $abh = f'g'$. Since f' and g' have coprime coefficients, $f'g'$ does by the lemma, from which it follows that $ab = \pm 1$. Thus $h = \pm f'g'$. Because $\mathbb{Z}[x]$ is a UFD, we get $f' = f$ and $g' = g$, and are done.

Problem A.1.3. Review of the Cayley-Hamilton theorem: Let R be a ring, and M a finitely generated free R-module. Let $\varphi : M \to M$ be an R-linear map, and $P_\varphi(x)$ the characteristic polynomial of φ.

(a) If R is an algebraically closed field, show that $P_\varphi(\varphi) = 0$ by writing φ as a matrix in Jordan normal form.

(b) Let $f : R \to R'$ be a map of rings, and let $\varphi' : M \otimes_R R' \to M \otimes_R R'$ be the map induced by φ. Show that if $P_\varphi(\varphi) = 0$ then $P_{\varphi'}(\varphi') = 0$, and that the converse holds if f is injective.

(c) Use the first two parts to show that $P_\varphi(\varphi) = 0$ for any R and φ. (Hint: Write R as a quotient of a polynomial ring over $\mathbb{Z}$, $S = \mathbb{Z}[x_1, x_2, \cdots]$ and then embed S in an algebraically closed field)

Problem A.1.4. By hand (that is, without using any theory from class), find the ring of integers of $\mathbb{Q}(\sqrt{17})$.

A.2 Problem Set 2

Problem A.2.1. List all the integers $-50 < D < 50$ which occur as the discriminant of a quadratic field.

Solution. Let us first look at multiples of 4: $\pm\{4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48\}$. Check which of these, when divided by 4, are $\equiv 3$ (4). From this, we see that $\{12, 28, 44, -4, -20, -36\}$ occur as the discriminant of a quadratic field.

Now, we look at all those integers that are $\equiv 1$ (4), and see that $\{4 \cdot n + 1 : n = -12, \dots, 12\}$ occur as the discriminant of a quadratic extension.

Problem A.2.2. Show that if K is a number field and $\mathcal{O}_K$ its ring of integers, then $\mathcal{O}_K$ is integrally closed in K.

Solution. Suppose $x \in K$ were integral over $\mathcal{O}_K$. By transitivity of integrality, we have x is integral over $\mathbb{Z}$. But $\mathcal{O}_K$ is precisely those elements of K integral over $\mathbb{Z}$, so $x \in \mathcal{O}_K$.

Problem A.2.3. For p, q distinct odd primes, show that the ring of integers $\mathbb{Q}(\zeta_p, \zeta_q)$ is $\mathbb{Z}[\zeta_p, \zeta_q]$. (Hint: Show that the polynomial $\Phi_p(X) = \frac{X^p-1}{X-1}$ is irreducible over $\mathbb{Q}(\zeta_p)$ by adapting the argument for Eisenstein's criterion. To do this, show that the polynomial $\frac{X^q-1}{X-1}$ has distinct roots mod p.)

Solution. Let $K = \mathbb{Q}(\zeta_p)$ and $L = \mathbb{Q}(\zeta_q)$ to simplify notation; note that $d_K = (-1)^{\frac{(p-1)(p-2)}{2}} p^{p-2}$ and $d_L = (-1)^{\frac{(q-1)(q-2)}{2}} q^{q-2}$ are coprime. It thus suffices to show that K and L are linearly disjoint number fields, for then the equality

$$\mathcal{O}_{K \cdot L} = \mathcal{O}_K \cdot \mathcal{O}_L$$

holds.

Let $\Phi_q(x)$ be the cyclotomic polynomial

$$\Phi_q(x) := \frac{x^q - 1}{x - 1} = x^{q-1} + x^{q-2} + \cdots + x + 1.$$

Recall the generalization of Gauss's lemma used in class: if K is a number field and $f \in \mathcal{O}_K[x]$ is monic, then f is irreducible over $K[x]$ if f is irreducible over $\mathcal{O}_K[x]$. In our case, we are considering $\Phi_q(x)$ as a monic polynomial in $\mathcal{O}_K(x) = \mathbb{Z}[\zeta_p]$.

Note that $\mathcal{O}_L \cong \mathbb{Z}[x]/\Phi_q(x)$, so we have

$$\mathcal{O}_L/p\mathcal{O}_L \cong (\mathbb{Z}/p)[x]/\overline{\Phi_q(x)},$$

where $\overline{\Phi_q(x)}$ is the image of $\Phi_q(x)$ in $(\mathbb{Z}/p)[x]$. If $\overline{\Phi_q(x)}$ is separable, then the quotient $\mathcal{O}_L/p\mathcal{O}_L$ is a finite field. By taking the derivative, we see even more that $x^q - 1$ is separable ($x^q - 1$ and qx^{q-1} share no common factors). Indeed, this is all true mod p.

We now argue as with Eisenstein's criterion to show that $\Phi_p(x)$ is irreducible in $\mathbb{Z}[\zeta_q]$. In particular, we can pass to $\mathbb{Z}[\zeta_p]/q\mathbb{Z}[\zeta_q]$ instead of $\mathbb{Z}/q$ because of the above, so the proof works nearly verbatim. Thus $\Phi_p(x)$ is irreducible in $\mathbb{Z}[\zeta_q]$, and we find that $\mathcal{O}_L$ and $\mathcal{O}_K$ are linearly disjoint. This gives the result.

Problem A.2.4. Compute the ring of integers of $\mathbb{Q}(\sqrt{23}, \sqrt{3})$. (Hint: A useful idea is to take the traces down to the quadratic fields contained in $\mathbb{Q}(\sqrt{23}, \sqrt{3})$, and use that the trace of an algebraic integer is an algebraic integer.)

Solution. To simplify notation, let $K = \mathbb{Q}(\sqrt{3}, \sqrt{23})$. It is obvious that $\mathbb{Q}(\sqrt{23})$ and $\mathbb{Q}(\sqrt{3})$ are linearly disjoint. Furthermore, as $\mathrm{Disc}(\mathbb{Q}(\sqrt{23})) = 52$ and $\mathrm{Disc}(\mathbb{Q}(\sqrt{3}) = 12$, we have

$$\mathcal{O}_K \subseteq \frac{1}{4}\mathcal{O}_{\mathbb{Q}(\sqrt{3})} \cdot \mathcal{O}_{\mathbb{Q}(\sqrt{23})}.$$

Thus, any element of $\mathcal{O}_K$ has the form

$$\frac{A + B\sqrt{3} + C\sqrt{23} + D\sqrt{69}}{4}.$$

We consider the trace $\mathrm{Tr}_{K/L}(x)$ for $L = \mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{23})$, and $\mathbb{Q}(\sqrt{69})$. The respective rings of integers are $\mathbb{Z}[\sqrt{3}]$, $\mathbb{Z}[\sqrt{23}]$, and $\mathbb{Z}\left[\frac{1}{2}(1 + \sqrt{69})\right]$. Because of the inclusion $\mathrm{Tr}_{K/L}(\mathcal{O}_K) \subseteq \mathcal{O}_L$, we get the following restrictions:

$$\begin{aligned}
&\frac{A + B\sqrt{3}}{2} \in \mathbb{Z}[\sqrt{3}], \text{ so } A, B \in 2\mathbb{Z} \\
&\frac{A + C\sqrt{23}}{2} \in \mathbb{Z}[\sqrt{23}], \text{ so } A, C \in 2\mathbb{Z} \\
&\frac{A + D\sqrt{69}}{2} \in \mathbb{Z}\left[\frac{1}{2}(1 + \sqrt{69})\right], \text{ from which it follows that } A + D \in 2\mathbb{Z}.
\end{aligned}$$

Note now that $\frac{1}{2}$, $\frac{1}{2}\sqrt{3}$, $\frac{1}{2}\sqrt{23}$, and $\frac{1}{2}\sqrt{69}$ are *not* in $\mathcal{O}_K$: their minimal polynomials are not monic. On the other hand, $\frac{1}{2}(\sqrt{23}-\sqrt{3})$ and $\frac{1}{2}(1+\sqrt{69})$ are; thus we see that

$$\mathcal{O}_K = \left\{\frac{1}{2}(A + B\sqrt{3} + C\sqrt{23} + D\sqrt{69}) \mid A+D, B+C \in 2\mathbb{Z}\right\}.$$

Equivalently, $\mathcal{O}_K$ has a $\mathbb{Z}$-basis $\left\{1, \frac{1+\sqrt{69}}{2}, \sqrt{23}, \frac{\sqrt{23}-\sqrt{3}}{2}\right\}$.

A.3 Problem Set 3

Problem A.3.1. Let $K = \mathbb{Q}(\sqrt{-13})$.

(a) Find the factorization of (7) and (11) into prime ideals in $\mathcal{O}_K$.

(b) Show that there are 3 different factorizations of 77 into irreducible elements in $\mathcal{O}_K$> (Two factorizations $\prod_{i=1}^n a_i = \prod_{i=1}^n b_i$ are the same if $a_i/b_i \in \mathcal{O}_K^\times$ is a unit. In this example, this means that $a_i/b_i = \pm 1$.)

Solution. (a) We consider the compositions

$$\begin{tikzcd}
\mathcal{O}_K/7 \cong \mathbb{Z}[x]/(x^2+13,7) \arrow[r, "\simeq"] & \mathbb{F}_7[x]/(x^2-1) \arrow[r] \arrow[dr] & \mathbb{F}_7[x]/(x-1) \\
& & \mathbb{F}_7[x]/(x+1).
\end{tikzcd}$$

As $\mathbb{F}_7[x]/(x-1) \cong \mathbb{F}_7[x]/(x+1) \cong \mathbb{F}_7$, the preimages in $\mathcal{O}_K$ of the ideals $(x-1)$ and $(x+1)$ are prime. These ideals are $\mathfrak{p}_1 = (7, \sqrt{-13}-1)$ and $\mathfrak{p}_2 = (7, \sqrt{-13}+1)$. I claim that $(7) = \mathfrak{p}_1 \cdot \mathfrak{p}_2$. Indeed, $\mathfrak{p}_1 \cdot \mathfrak{p}_2$ is the ideal generated by $\{49, 7-7\sqrt{-13}, 7+7\sqrt{-13}, 14\}$, so it is clearly contained in (7). But also $49 - 3 \cdot 14 = 7$, so $(7) \subseteq \mathfrak{p}_1 \cdot \mathfrak{p}_2$.

Now begin again by considering the compositions

$$\begin{tikzcd}
\mathcal{O}_K/11 \cong \mathbb{Z}[x]/(x^2+13,11) \arrow[r, "\simeq"] & \mathbb{F}_{11}[x]/(x^2-9) \arrow[r] \arrow[dr] & \mathbb{F}_{11}[x]/(x-3) \\
& & \mathbb{F}_{11}[x]/(x+3).
\end{tikzcd}$$

As before, $(x-3)$ and $(x+3)$ are prime in $\mathbb{F}_7[x]/(x^2-9)$, so they pull back to prime ideals in $\mathcal{O}_K$. Specifically, we have the prime ideals $\mathfrak{q}_1 = (11, \sqrt{-13}+3)$ and $\mathfrak{q}_2 = (11, \sqrt{-13}-3)$. We check that $\mathfrak{q}_1\mathfrak{q}_2 = (11)$: the product of the two is the ideal $(121, 33-11\sqrt{-13}, 33+11\sqrt{-13}, 22)$, so it is clearly contained in (11). For the reverse containment, we note $121 - 5 \cdot 22 = 11$.

(b) First, we show that $77 = 7 \cdot 11$ works. Suppose $7 = a \cdot b$ with $a, b \notin \mathcal{O}_K^\times$. Taking the norm, we see $49 = N(a)N(b)$, and the hypothesis that a and b are non-units implies, say, that $N(a) = 7 = x^2 + 13y^2$ for some integer x, y. This certainly cannot hold if $y \neq 0$, and 7 is not a square. So 7 is irreducible. Similarly, suppose $11 = a \cdot b$, where $a, b \notin \mathcal{O}_K^\times$. It follows that $11 = N(a) = x^2 + 13y^2$, which cannot hold for the same reasoning.

Suppose that $77 = a \cdot b$, where a and b are non-units in $\mathcal{O}_K$. Then

$$N(a) \cdot N(b) = 77^2 = 7^2 \cdot 11^2.$$

The non-unit condition on, say, a means that our only choices for $N(a)$ are $7, 11, 7^2, 11^2, 7 \cdot 11, 7 \cdot 11^2, 7^2 \cdot 11$, and $7^2 \cdot 11^2$. The requirement that b not be a unit immediately rules out the last possibility. We can also see that if $N(a) = 7$, we have $x^2 + 13y^2 = 7$ for some x and y, which never holds. Similarly, $N(a)$ cannot be 11. By symmetry, it follows that $N(a) \neq 7 \cdot 11^2$ or $7^2 \cdot 11$.

In the case where $N(a) = 7 \cdot 11$, say, one wants $a_1^2 + 13a_2^2 = 77$. We have two options: $a_2 = \pm 1$, giving $a_1 = \pm 8$, and $a_2 = \pm 2$, giving $a_1 = \pm 5$. Both of these give valid factorizations:

$$(8 + \sqrt{-13})(8 - \sqrt{-13}) = 77,$$
$$(5 + 2\sqrt{-13})(5 - 2\sqrt{-13}) = 77.$$

All that is left to check is that these factors are irreducible. As these elements were all chosen because they have norm 77, factoring them into non-unit irreducibles would require choosing elements of norm 7 and 11 in $\mathcal{O}_K$; this equates to solving $a^2 + 13b^2 = \{7, 11\}$ over the integers, which is impossible.

One may check that there are no more valid factorizations of 77 into elements of norm 49 and 121; there are only a handful of possibilities. Similarly, there are no more possible factorizations into two elements of norm 77.

Problem A.3.2. Let $K = \mathbb{Q}(\sqrt{-23})$.

(a) Show that not all ideals in $\mathcal{O}_K$ are principal.

(b) Show that the class group of $\mathcal{O}_K$ has an element of order 3.

Solution. (a) Consider the ideal $\mathfrak{p} = (11, 1 + \sqrt{-23}) \subseteq \mathcal{O}_K$. Suppose it were principal, i.e., that $\mathfrak{p} = (a + b\sqrt{-23})$. In particular, we have $11 \in (a + b\sqrt{-23})$, so $11 = (a + b\sqrt{-23})c$ for some non-unit $c \in \mathcal{O}_K$. If we take the norm, we see

$$121 = (a^2 + 23b^2) \cdot N(c),$$

and the non-unit condition on c implies that $11 = a^2 + 23b^2$, which is impossible over the integers. Thus $\mathfrak{p}$ is not principal.

(b) We wish to find a fractional ideal $\mathfrak{P}$ that is not principal, but whose cube $\mathfrak{P}^3$ *is* principal (in fact, it turns out *any* non-principal ideals of $\mathcal{O}_K$ have order 3). Take for instance the ideal $\mathfrak{P} = (4, 1 + \sqrt{-23}) \subseteq \mathcal{O}_K$. This is not principal by a similar argument to that used in part (a). We compute:

$$\begin{aligned}\mathfrak{P}^2 &= (16, 4 + 4\sqrt{-23}, 22 - 2\sqrt{-23})\\ &= (16, 22 - 2\sqrt{-23}).\end{aligned}$$

This represents the same ideal class as $(8, 11 - \sqrt{-23}) = (8, 5 + \sqrt{-23})$. Suppose that $\mathfrak{P}^2$ were principal, i.e., there were some $\alpha \in \mathfrak{P}^2$ such that $\mathfrak{P}^2 = (\alpha)$. Then $\alpha | 8, 5 + \sqrt{-23}$, so in particular $N(\alpha) | N(8), N(5 + \sqrt{-23}$. But $N(8) = 64$ and $N(5 + \sqrt{-23}) = 48$, so $N(\alpha)$ must be 2, 4, 8, or 16. We know immediately that $N(\alpha)$ cannot be 2 or 8, because $a^2 + 23b^2 = 2, 8$ has no solution in integers. If $N(\alpha) = 4$, then $\alpha = 2$. But there is no $\beta \in \mathcal{O}_K$ such that $2\beta = 5 + \sqrt{-23}$. Similarly, if $N(\alpha) = 16$, then $\alpha = 4$, and there is no $\beta \in \mathcal{O}_K$ such that $4\beta = 5 + \sqrt{-23}$. It follows that $\mathfrak{P}^2$ is not principal.

We now compute $\mathfrak{P}^3$:

$$\begin{aligned}\mathfrak{P}^3 &= (4, 1 + \sqrt{-23})(8, 5 + \sqrt{-23})\\ &= (32, 8 + 8\sqrt{-23}, 20 + 4\sqrt{-23}, -18 + 6\sqrt{-23})\\ &= (32, 20 + 4\sqrt{-23}, -38 + 2\sqrt{-23})\\ &= (2)\end{aligned}$$

which is principal.

A.4 Problem Set 4

Problem A.4.1. Let $K \subset L$ be number fields. Show that, for every ideal I of $\mathcal{O}_K$,

$$I = (I\mathcal{O}_L) \cap \mathcal{O}_K.$$

(Hint: use the fact that I has an inverse.)

Solution. Let $I' \subseteq K$ be the inverse for I. We show that $((I\mathcal{O}_L) \cap \mathcal{O}_K) \cdot I' = \mathcal{O}_K$; then, by uniqueness of inverses, the wanted result follows. Recall the definition of I': $I' = \{a \in K : aI \subseteq \mathcal{O}_K\}$. In particular, $\mathcal{O}_K \subseteq I'$. We note that $((I\mathcal{O}_L) \cap \mathcal{O}_K) \cdot I'$ is contained in the distributed intersection $(I\mathcal{O}_L \cdot I') \cap I'\mathcal{O}_K$: an element $x \in ((I\mathcal{O}_L) \cap \mathcal{O}_K) \cdot I'$ can be written as a sum

$$x = \sum_i \alpha_i (a_i b_i)$$

where $a_i \in (I\mathcal{O}_L) \cap \mathcal{O}_K$, $b_i \in I'$, and $\alpha_i \in \mathcal{O}_K$. In particular, $a_i \in I\mathcal{O}_L$ and $a_i \in \mathcal{O}_K$, so

$x \in (I\mathcal{O}_L \cdot I') \cap I'\mathcal{O}_K$. Now, $I\mathcal{O}_L \cdot I' = (I \cdot I')\mathcal{O}_L = \mathcal{O}_K \cdot \mathcal{O}_L$ which is contained in $\mathcal{O}_L$, so

$$(I\mathcal{O}_L) \cdot I' \cap I'\mathcal{O}_K \subseteq \mathcal{O}_L \cap I' = \mathcal{O}_K$$

because it consists of all integral elements in K. Thus $((I\mathcal{O}_L) \cap \mathcal{O}_K) \cdot I' \subseteq \mathcal{O}_K$. But

$$(I\mathcal{O}_L) \cdot I' = \mathcal{O}_K \cdot \mathcal{O}_L \supseteq \mathcal{O}_K,$$

and $I'\mathcal{O}_K \supseteq \mathcal{O}_K$, so we have the chain of inclusions

$$\mathcal{O}_K \subseteq ((I\mathcal{O}_L) \cap \mathcal{O}_K) \cdot I' \subseteq \mathcal{O}_K$$

and equality thus holds. From this, we conclude that I' is the inverse of both I and $(I\mathcal{O}_L) \cap \mathcal{O}_K$, so uniqueness of inverses gives

$$I = (I\mathcal{O}_L) \cap \mathcal{O}_K.$$

Problem A.4.2. Let K be a number field. Remember that the ideal class group $\mathrm{C}\ell_K$ is finite (you may assume this if we haven't proven it in class yet).

(a) Let I be an ideal of $\mathcal{O}_K$. Find a finite extension L of K such that $I\mathcal{O}_L$ is a principal ideal.

(b) Find a finite extension L of K such that, for every ideal I of $\mathcal{O}_K$, the ideal $I\mathcal{O}_L$ is principal.

Solution. (a) Factor I into primes as

$$I = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n},$$

where the $\mathfrak{p}_i$ are prime ideals. By finiteness of the class group, we have some $m \in \mathbb{N}^+$ and $b \in \mathcal{O}_K$ such that

$$I^m = (b)$$

is principal. Let $L = K(b^{1/m})$, so that $(b) = (b^{1/m})^m$ in $\mathcal{O}_L$. Then

$$(\mathfrak{p}_1 \cdots \mathfrak{p}_n)^m = (b^{1/m})^m,$$

so the main idea is that if two fractional ideals I and J are such that $I^m = J^m$, then $I = J$. Suppose $(b^{1/m})$ has a factorization as $\mathfrak{q}_1^{s_1} \cdots \mathfrak{q}_k^{s_k}$. Then

$$\mathfrak{p}_1^{m \cdot r_1} \cdots \mathfrak{p}_n^{m \cdot r_n} = \mathfrak{q}_1^{m \cdot s_1} \cdots \mathfrak{q}^{m \cdot s_k},$$

so by uniqueness of factorization, we can re-order, say, the $\mathfrak{q}_i$ so that $\mathfrak{p}_i = \mathfrak{q}_i$ for all i, $n = k$, and $r_i = s_i$. It is clear then that $I\mathcal{O}_L = (b^{1/m})$, and we are done.

(b) Let us first note that the construction in part (a) works perfectly well for *any* ideal J in the same ideal class as I. Suppose $J = (a) \cdot I$, where $a \in \mathcal{O}_K$. Then $J\mathcal{O}_L =$

$(a) \cdot I\mathcal{O}_L = (a) \cdot (b^{1/m})\mathcal{O}_L = (a \cdot b^{1/m})$, which is principal. Enumerate the ideal classes in $\mathrm{C}\ell_K$ as $[I_1], \ldots, [I_n]$, with representatives $I_1, \ldots, I_n$. The above construction gives elements $b_1, \ldots, b_n \in \mathcal{O}_K$ and positive integers $m_1, \ldots, m_n$ such that

$$I_i^{m_i} = (b_i).$$

Let L be the extension of K defined by

$$L = K(b_1^{1/m_1}, \ldots, b_n^{1/m_n}).$$

It is clear by construction that any ideal $\mathfrak{a} \subseteq \mathcal{O}_K$—because it belongs to a unique ideal class that is "made principal" in L—becomes principal in L, i.e., $\mathfrak{a}\mathcal{O}_L$ is principal.

Index