

Table of Contents

Contents

Table of Contents	2
1 Notation	4
2 Diophantine Equations (Lec. 1, Thursday, January 14)	4
2.1 Intro/Logistics	4
2.2 Motivation	5
2.3 Failure of Unique Factorization	7
3 Number Fields (Lec. 2, Tuesday, January 19)	7
3.1 Embeddings	7
3.2 Algebraic Closures	9
3.3 Rings of Integers and Fraction Fields	12
4 Quadratic Fields (Lec. 3, Thursday, January 21)	14
4.1 Quadratic Number Fields	14
4.2 Norm and Trace	15
4.3 The Field Polynomial	16
4.4 Classification of \mathbb{Z}_K	17
5 Failure of Unique Factorization (Lec. 4, Wednesday, January 27)	18
5.1 Revisiting a Counterexample to Unique Factorization	18
5.2 Factorization Theory	19
6 Euclidean Quadratic Fields (Lec. 5, Thursday, January 28)	23
6.1 Setup	23
6.2 Norm-Euclidean Imaginary Quadratic Fields	25
6.3 Proof of Motzkin's Theorem	30
7 Ideal Theory and Quadratic Fields (Lec. 6, Tuesday, February 02)	31
7.1 Prime Factorization in $\text{Id}(\mathbb{Z}_K)$	31
7.2 Ideal Norms	33
8 Fundamental Theorem of Ideal Theory (Lec. 7, Thursday, February 04)	35
8.1 Norms: Multiplicativity and Computations	36
8.2 Unique Factorization for Ideals	37
8.2.1 Proving Unique Factorization	38
8.3 Preview: Ramification	40
9 Prime Ideals of \mathbb{Z}_K (Lec. 8, Tuesday, February 09)	41
9.1 Dedekind-Kummer Mirroring	41
9.2 Units in \mathbb{Z}_K	44

10 Units in \mathbb{Z}_K (Lec. 9, Monday, February 15)	46
10.1 Review	46
10.2 An Aside: Diophantine approximation	47
10.3 Class Groups and the Class Number	50
11 Class Groups (Lec. 10, Thursday, February 18)	53
11.1 Computing Class Groups	53
11.2 The Class Group as a Measure of Non-unique Factorization	55
11.3 Elasticity	57
12 Prime Producing Polynomials and Unique Factorization (Lec. 11, Tuesday, February 23)	58
12.1 Chapter 11: Prime Producing Polynomials and Unique Factorization	58
12.2 Proof of Rabinowitz's Theorem	61
12.3 Lattice Points	63
13 Lattice Points (Lec. 12, Monday, March 01)	65
13.1 Minkowski (Version 1)	65
13.2 Minkowski (Version 2)	66
13.2.1 Application: The 4 Square Theorem	71
14 Starting Over with General Number Fields (Lec. 13, Thursday, March 04)	73
14.1 Recasting Old Definitions	73
14.2 Discriminants	75
14.3 Integral Bases	76
14.4 Discriminant of Number Fields	78
15 Discriminants and Norms (Lec. 14, Saturday, March 13)	79
15.1 Norms of Ideals	79
15.2 Chapter 14: Integral Bases	82
16 Cyclotomic Fields (Lec. 15, Saturday, March 13)	84
16.1 Ideal Theory in General Number Rings (Ch. 15)	87
17 Ideal Theory in Number Fields Continued (Lec. 16, Tuesday, March 30)	89
17.1 Setting up the Theory	89
17.2 Modern Approach	91
17.3 Norms Revisited	92
17.4 Applications of Finiteness of Class Group	94
ToDo's	95
Definitions	96
Theorems	97
Exercises	99
Figures	100

1 | Notation

Todo: definitions.

- $\overline{\mathbb{Q}}$
- $\overline{\mathbb{Z}}$
- K
- $U(K), K^\times$
- $[K : \mathbb{Q}]$
- $K[\alpha]$
- $K(\alpha)$
- $\mathbb{Z}_K := \overline{\mathbb{Z}} \cap K$, the algebraic integers in K .
- $\text{ff}(K)$
- $\text{Ab}, \mathbb{Z}\text{-Mod}$: the category of abelian groups.

2 | Diophantine Equations (Lec. 1, Thursday, January 14)

2.1 Intro/Logistics

See website for notes on books, intro to class.

- Youtube Playlist: <https://www.youtube.com/playlist?list=PLA0xtXq0Uji8fjQysx4k8a6h-h0Z7x5ue>
- Free copies of textbook: https://www.dropbox.com/sh/rv5j222kn74bjhm/AABZ1qcR1rOnpaBsa5CL3P_Ea?dl=0&lst=

Paul's description of the course:

This course is an introduction to arithmetic beyond \mathbb{Z} , specifically arithmetic in the ring of integers in a finite extension of \mathbb{Q} . Among many other things, we'll prove three important theorems about these rings:

- *Unique factorization into ideals.*
- *Finiteness of the group of ideal classes.*
- *Dirichlet's theorem on the structure of the unit group.*

2.2 Motivation

Remark 2.2.1: The main motivation: solving **Diophantine equations**, i.e. polynomial equations over \mathbb{Z} .

Example 2.2.2 (of a Diophantine equation): Consider $y^2 = x^3 + x$.

Claim: $(x, y) = (0, 0)$ is the only solution.

To see this, write $y^2 = x(x^2 + 1)$, which are relatively prime, i.e. no $D \in \mathbb{Z}$ divides both of them. Why? If $d \mid x$ and $d \mid x + 1$, then $d \mid (x^2 + 1) + (-x) = 1$. It's also the case that both $x^2 + 1$ and x^2 are squares (up to a unit), so $x^2, x^2 + 1$ are consecutive squares in \mathbb{Z} . But the gaps between squares are increasing: $1, 2, 4, 9, \dots$. The only possibilities would be $x = 0, y = 1$, but in this case you can conclude $y = 0$.

Example 2.2.3 (Fermat): Consider $y^2 = x^3 - 2$.

Claim: $(3, \pm 5)$ are the only solutions.

Rewrite

$$\begin{aligned} x^3 = y^2 + 2 &= (y + \sqrt{-2})(y - \sqrt{-2}) \\ &\in \mathbb{Z}[\sqrt{-2}] := \{a + b\sqrt{-2} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}. \end{aligned}$$

This is a subring of \mathbb{C} , and thus at least an integral domain. We want to try the same argument: showing the two factors are relatively prime. A little theory will help here:

Definition 2.2.4 (Norm Map)

$$N\alpha := \alpha\bar{\alpha} \quad \text{for } \alpha \in \mathbb{Z}[\sqrt{-2}].$$

Lemma 2.2.5 (?).

Let $\alpha, \beta \in \mathbb{Z}[\sqrt{-2}]$. Then

1. $N(\alpha\beta) = N(\alpha)N(\beta)$
2. $N(\alpha) \in \mathbb{Z}_{\geq 0}$ and $N(\alpha) = 0$ if and only if $\alpha = 0$.
3. $N(\alpha) = 1 \iff \alpha \in R^\times$

Proof (?). 1. Missing, see video (10:13 AM).

2. $N(\alpha) = a^2 + 2b^2 \geq 0$, so this equals zero if and only if $\alpha = \beta = 0$

3. Write $1 = \alpha\bar{\alpha}$ if $N(\alpha) = 1 \in R^\times$. Conversely if $\alpha \in R^\times$ write $\alpha\beta = 1$, then

$$1 = N(1) = N(\alpha\beta) = N(\alpha)N(\beta) \in \mathbb{Z}_{\geq 0},$$

which forces both to be 1. ■

Claim: The two factors $y \pm \sqrt{-2}$ are *coprime* in $\mathbb{Z}[\sqrt{-2}]$, i.e. every common divisor is a unit.

Proof (?).

Suppose $\delta \mid y \pm \sqrt{-2}$, then $y + \sqrt{-2} = \delta\beta$ for some $\beta \in \mathbb{Z}[\sqrt{-2}]$. Take norms to obtain $y^2 + 2 = N\delta N\beta$, and in particular

- $N\delta y^2 + 2$
- $\delta \mid (y + \sqrt{-2}) - (y - \sqrt{-2}) = 2\sqrt{-2}$ and thus $N\delta \mid N(2\sqrt{-2}) = 8$.

In the original equation $y^2 = x^3 - 2$, if y is even then x is even, and $x^3 - 2 \equiv 0 - 2 \pmod{4} \equiv 2$, and so $y^2 \equiv 2 \pmod{4}$. But this can't happen, so y is odd, and we're done: we have $N\delta \mid 8$ which is even or 1, but $N\delta \mid y^2 + 2$ which is odd, so $N\delta = 1$. ■

We can identify the units in this ring:

$$\mathbb{Z}[\sqrt{-2}]^\times = \{a + b\sqrt{-2} \mid a^2 + 2b^2 = 1\}$$

which forces $a^2 \leq 1, b^2 \leq 1$ and thus this set is $\{\pm 1\}$. So we have $x^3 = ab$ which are relatively primes, so a, b should also be cubes. We don't have to worry about units here, since ± 1 are both cubes. So e.g. we can write

$$y + \sqrt{-2} = (a + b\sqrt{-2})^3 = (a^3 - 6ab^2) + (3a^2b - 2b^3)\sqrt{-2}.$$

Comparing coefficients of $\sqrt{-2}$ yields

$$1 = b(3a^2b - 2b^2) \in \mathbb{Z} \implies b \mid 1,$$

and thus $b \in \mathbb{Z}^\times$, i.e. $b \in \{\pm 1\}$. By cases:

- If $b = 1$, then $1 = 3a^2 - 2 \implies a^2 = 1 \implies a = \pm 1$. So

$$y + \sqrt{-2} = (\pm 1 + \sqrt{-2})^3 = \pm 5 + \sqrt{-2},$$

which forces $y = \pm 5$, the solution we already knew.

- If $b = -1$, then $1 = -(3a^2 - 1)$ which forces $1 = 3a^2 \in \mathbb{Z}$, so there are no solutions. 

2.3 Failure of Unique Factorization

Example 2.3.1 (where unique factorization fails): Consider $y^2 = x^3 - 26$. Rewrite this as

$$x^3 = y^2 + 26 = (y + \sqrt{-26})(y - \sqrt{-26}),$$

then the same lemma goes through with 2 replaced by 26 everywhere where the RHS factors are still coprime. Setting $y + \sqrt{-26} = (a + b\sqrt{-26})^3$ and comparing coefficients, you'll find $b = 1, a = \pm 3$. This yields $x = 35, y = \pm 207$. But there are more solutions: $(x, y) = (3, \pm 1)$! The issue is that we used unique factorization when showing that ab is a square implies a or b is a square (say by checking prime factorizations and seeing even exponents). In this ring, we can have ab a cube with *neither* a, b a cube, even up to a unit.

Question 2.3.2

When does a ring admit unique factorization? Do you even *need* it?

Remark 2.3.3: This will lead to a discussion of things like the **class number**, which measure the failure of unique factorization. In general, the above type of proof will work when the class number is 3!

3 | Number Fields (Lec. 2, Tuesday, January 19)

3.1 Embeddings

Remark 3.1.1: Today: Ch.2 of the book, "Cast of Characters". Note that all rings will be commutative and unital in this course.

Last time: looked at factorization in $\mathbb{Z}[\sqrt{2}], \mathbb{Z}[\sqrt{26}]$. Where do rings like this come from?

Definition 3.1.2 (Number Field)

A **number field** is a subfield $K \subseteq \mathbb{C}$ ^a such that $[K : \mathbb{Q}] < \infty$.

^aSome authors don't require $K \subseteq \mathbb{C}$, but any finite extension of \mathbb{Q} will embed into \mathbb{C} so there's no harm in this extra requirement.

Example 3.1.3 (of number fields): Examples of number fields include

- $\mathbb{Q}[\sqrt[3]{2}]$,
- $\mathbb{Q}[\sqrt{2}, \sqrt[5]{7}]$, or

- $\mathbb{Q}(\theta)$ where θ is a root of $x^5 - x - 1$, which one can check is irreducible.

Note that the round vs. square brackets here won't make a difference, since we're adjoining *algebraic* numbers.

Proposition 3.1.4 (Degree equals number of embeddings for finite extensions).

Let K/\mathbb{Q} be a finite extension, say of degree $n := [K : \mathbb{Q}]$. Then there are n distinct embeddings^a of K into \mathbb{C}

^aAn **embedding** is an injective ring morphism.

Proof (of proposition).

We have K/\mathbb{Q} , which is necessarily separable since $\text{ch}(\mathbb{Q}) = 0$. By the primitive element theorem, we can write $K = \mathbb{Q}(\theta)$ where θ is a root of some degree n irreducible polynomial $f(x) \in \mathbb{Q}[x]$. Since \mathbb{C} is algebraically closed, f splits completely over \mathbb{C} as

$$f = \prod_{i=1}^n (x - \theta_i)$$

with each $\theta_i \in \mathbb{C}$ distinct since f was irreducible and we're in characteristic zero. Then for each i there is an embedding $K = \mathbb{Q}[\theta]$ given by

$$\begin{aligned} \iota_i : \mathbb{Q}[\theta] &\hookrightarrow \mathbb{C} \\ g(\theta) &\mapsto g(\theta_i). \end{aligned}$$

There are some easy things to check:

- This is well-defined: elements in K are polynomials in θ but they all differ by a multiple of the minimal polynomial of θ ,
- This is an injective homomorphism and thus an embedding, and
- For distinct i you get distinct embeddings: just look at the image $\iota_i(\theta)$, these are distinct numbers in \mathbb{C} .

■

Definition 3.1.5 (Real and Nonreal embeddings)

Let K/\mathbb{Q} be a finite extension of degree $n = [K : \mathbb{Q}]$. We'll say an embedding $\sigma : K \rightarrow \mathbb{C}$ is **real** if $\sigma(K) \subseteq \mathbb{R}$, otherwise we'll say the embedding is **nonreal**.

Remark 3.1.6: If σ is a nonreal, then $\bar{\sigma}$ is a nonreal embedding, so these embeddings come in pairs. As a consequence, the total number of embeddings is given by $n = r_1 + 2r_2$, where r_1 is the number of real embeddings and r_2 is the number of nonreal embeddings.

Example 3.1.7 (of computing the number of real and nonreal embeddings): Let $K = \mathbb{Q}(\sqrt[3]{2})$. Here $n = 3$ since this is the root of a degree 3 irreducible polynomial. Using the proof we can find the embeddings: factor

$$x^3 - 2 = (x - \sqrt[3]{2})(x - \omega\sqrt[3]{2})(x - \omega^2\sqrt[3]{2}).$$

where $\omega = e^{2\pi i/3}$ is a complex cube root of unity. We can form an embedding by sending $\sqrt[3]{2} \rightarrow \omega^j \sqrt[3]{2}$ for $j = 0, 1, 2$. The case $j = 0$ sends K to a subset of \mathbb{R} and yields a real embedding, but the other two will be nonreal. So $r_1 = 1, r_2 = 1$, and we have $3 = 1 + 2(1)$, which is consistent.

3.2 Algebraic Closures

Remark 3.2.1: We've only been talking about fields, where unique factorization is trivial since there are no primes. There are thus "too many" units in fields when compared to the rings we were considering before, so we'll restrict to subrings of fields. The question is: where is the arithmetic? Given a number field K , we want a ring \mathbb{Z}_K that fits this analogy:

$$\begin{array}{ccc} \mathbb{Q} & \rightsquigarrow & K \\ \downarrow & & \downarrow \\ \mathbb{Z} & \rightsquigarrow & \mathbb{Z}_K = ? \end{array}$$

Definition 3.2.2 (Algebraic Numbers)

Given $\alpha \in \mathbb{C}$ we say α is an **algebraic number** if and only if α is algebraic over \mathbb{Q} , i.e. the root of some polynomial in $\mathbb{Q}[x]$.

Remark 3.2.3: We know that if we define $\overline{\mathbb{Q}} := \{\alpha \in \mathbb{C} \mid \alpha \text{ is algebraic over } \mathbb{Q}\}$, we can alternatively describe this as $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid [\mathbb{Q}(\alpha) : \mathbb{Q}] < \infty\}$. This is convenient because it's easy to see that algebraic numbers are closed under sums and products, just using the ways degrees behave in towers.

Corollary 3.2.4 (Every number field is a subfield of $\overline{\mathbb{Q}}$).

$\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ is a subfield and every number field is a subfield of $\overline{\mathbb{Q}}$.

Remark 3.2.5: These are still fields, so let's define some interesting subrings.

Definition 3.2.6 ($\overline{\mathbb{Z}}$)

Define $\overline{\mathbb{Z}} := \{\alpha \in \mathbb{C} \mid \alpha \text{ is the root of a monic polynomial } f \in \mathbb{Z}[x]\}$.

Theorem 3.2.7 ($\overline{\mathbb{Z}}$ is a ring).

$\overline{\mathbb{Z}}$ is a ring, and in fact a domain since it's a subring of \mathbb{C} .

Remark 3.2.8: We'll use an intermediate criterion to prove this:

Proposition 3.2.9 (Integrality Criterion).

Let $\alpha \in \mathbb{C}$ and suppose there is a finitely generated \mathbb{Z} -submodule of \mathbb{C} with $\alpha M \subseteq M \neq 0$. Then $\alpha \in \bar{\mathbb{Z}}$, i.e. α is the root of a monic polynomial with integer coefficients.

Proof (of integrality criterion).

Chasing definitions, take M and choose a finite list of generators $\beta_1, \beta_2, \dots, \beta_m$ for M . Then $\alpha M \subseteq M \implies \alpha \beta_i \in M$ for all M , and each $\alpha \beta_i$ is a \mathbb{Z} -linear combination of the β_i . I.e. we have

$$\alpha \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & \cdots \\ a_{21} & a_{22} & \\ \vdots & & \ddots \end{bmatrix} \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix} := A \vec{\beta},$$

where $A \in \text{Mat}(n \times m, \mathbb{Z})$. We can rearrange this to say that

$$(\alpha I - A) \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix} = \mathbf{0}.$$

Not all of the β_i can be zero since $M \neq 0$, and thus $\alpha I - A$ is singular and has determinant zero, so $\det(xI - A)|_{x=\alpha} = 0$. We have

$$x \text{ id} - A = \begin{bmatrix} x - a_{1,1} & & & \\ & x - a_{2,2} & & \\ & & \ddots & \\ & & & x - a_{m,m} \end{bmatrix},$$

where the off-diagonal components are constants in \mathbb{Z} coming from A . Taking the determinant yields a monic polynomial: the term of leading degree comes from multiplying the diagonal components, and expanding over the remaining minors only yields terms of smaller degree. So $\det(xI - A) \in \mathbb{Z}[x]$ is monic. ■

Proof (of theorem).

We want to show that $\bar{\mathbb{Z}}$ is a ring, and it's enough to show that

- $1 \in \bar{\mathbb{Z}}$, which is true since $x - 1$ is monic.
- It's closed under addition (+) and multiplication (\cdot).

Note that the first property generalizes to $\mathbb{Z} \subseteq \bar{\mathbb{Z}}$, since $x - n$ is monic for any $n \in \mathbb{Z}$. For the second, let $\alpha, \beta \in \bar{\mathbb{Z}}$. Define $M := \mathbb{Z}[\alpha, \beta]$, then it's clear that $(\alpha + \beta)M \subseteq M$ and $(\alpha\beta)M \subseteq M$ since $\mathbb{Z}[\alpha, \beta]$ are polynomials in α, β and multiplying by these expression still yields such polynomials. It only remains to check the following:

Claim: M is finitely-generated.

Proof (?).

Let α be a root of $f \in \mathbb{Z}[x]$ and β a root of g , both monic with $\deg f = n, \deg g = m$. We want to produce a finite generating set for $M := \mathbb{Z}[\alpha, \beta]$, and the claim is that the following works: $\{\alpha^i \beta^j\}_{\substack{0 \leq i < n \\ 0 \leq j < m}}$, i.e. every element of M is some \mathbb{Z} -linear combination of these.

Note that this is clearly true if we were to include n, m in the indices by collecting terms of any polynomial in α, β , so the restrictions are nontrivial. It's enough to show that for any $0 \leq I, J \in \mathbb{Z}$, the term $\alpha^I \beta^J$ is a \mathbb{Z} -linear combination of the restricted elements above. Divide by f and g to obtain

$$\begin{aligned} x^I &= f(x)q(x) + r(x) \\ x^J &= g(x)\tilde{q}(x) + \tilde{r}(x) \end{aligned}$$

where $r(x) = 0$ or $\deg r < n$ and similarly for \tilde{r} , where (importantly) all of these polynomials are in $\mathbb{Z}[x]$.

We're not over a field: $\mathbb{Z}[x]$ doesn't necessarily have a division algorithm, so why is this okay? The division algorithm only requires inverting the leading coefficient, so in general $R[x]$ admits the usual division algorithm whenever the leading coefficient is in R^\times . Now plug α into the first equation to obtain $\alpha^I = r(\alpha)$ where $\deg r < n$, which rewrite α^I as a sum of lower-degree terms. Similarly writing $\beta^J = r(\beta)$, we can express

$$\alpha^I \beta^J = r(\alpha)r(\beta),$$

which is what we wanted. ■

Remark 3.2.10: We've just filled in another part of the previous picture:

$$\begin{array}{ccc} \mathbb{Q} & K & \overline{\mathbb{Q}} \\ \downarrow & \downarrow & \downarrow \\ \mathbb{Z} & \mathbb{Z}_K & \overline{\mathbb{Z}} \end{array}$$

3.3 Rings of Integers and Fraction Fields

Definition 3.3.1 (Ring of Integers)

Define $\mathbb{Z}_K = \bar{\mathbb{Z}} \cap K$, the **ring of integers** of K . Note that this makes sense since the intersection of rings is again a ring.

Remark 3.3.2: Why not just work in $\bar{\mathbb{Z}}$? It doesn't have the factorization properties we want, e.g. there are no irreducible elements. Consider $\sqrt{2}$, we can factor it into two non-units as $\sqrt{2} = \sqrt{\sqrt{2}} \cdot \sqrt{\sqrt{2}}$, noting that $\sqrt{2}$ is not a unit, and it's easy to check that if a is not a unit then \sqrt{a} is not a unit. So this would yield arbitrarily long factorizations, and a non-Noetherian ring. The following is a reality check, and certainly a property we would want:

Proposition 3.3.3 (*The ring of integers of \mathbb{Q} is \mathbb{Z}*).

$$\mathbb{Z}_{\mathbb{Q}} = \mathbb{Z}.$$

Proof (of proposition).

\subseteq : Easy, since $\mathbb{Z} \subseteq \bar{\mathbb{Z}}$ and $\mathbb{Z} \subseteq \mathbb{Q}$, and is thus in their intersection $\mathbb{Z}_{\mathbb{Q}}$.

\supseteq : Let $\alpha \in \mathbb{Z}_{\mathbb{Q}} = \mathbb{Q} \cap \bar{\mathbb{Z}}$, so α is a root of $x^n - a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$. We know $\alpha = a/b$ with $a, b \in \mathbb{Z}$, and we can use the rational root test which tells us that $a \mid a_0$ and $b \mid 1$, so $b = \pm 1$ and $\alpha = a/\pm 1 = \pm a \in \mathbb{Z}$ and thus $\alpha \in \mathbb{Z}$. ■

Remark 3.3.4: We'll want to study \mathbb{Z}_K for various number fields K , but we'll need more ground-work.

Proposition 3.3.5 (*Easy criterion to check if an integer is algebraic*).

Let $\alpha \in \bar{\mathbb{Q}}$, then

$$\alpha \in \bar{\mathbb{Z}} \iff \min_{\alpha} \in \mathbb{Z}[x],$$

where $\min_{\alpha}(x)$ is the unique monic irreducible polynomial in $\mathbb{Q}[x]$ which vanishes at α .

Proof (?).

\Leftarrow : Trivial, if the minimal polynomial already has integer coefficients, just note that it's already monic and thus $\alpha \in \bar{\mathbb{Z}}$ by definition.

\Rightarrow : Why should the minimal polynomial have *integer* coefficients? Choose a monic $f(x) \in \mathbb{Z}[x]$ with $f(\alpha) = 0$, using the fact that $\alpha \in \bar{\mathbb{Z}}$, and factor $f(x) = \prod_{i=1}^n (x - \alpha_i) \in \mathbb{C}[x]$. Note that each $\alpha_i \in \bar{\mathbb{Z}}$ since they are all roots of f (a monic polynomial in $\mathbb{Z}[x]$). Use the fact that $\min_{\alpha}(x)$ divides every polynomial which vanishes on α over \mathbb{Q} , and thus divides f (noting

that this still divides over \mathbb{C}). Moreover, every root of $\min_{\alpha}(x)$ is a root of f , and so every such root is some α_i .

Now factor $\min_{\alpha}(x)$ over \mathbb{C} to obtain $\min_{\alpha}(x) = \prod_{i=1}^m (x - \beta_i)$ with all of the $\beta_i \in \overline{\mathbb{Z}}$. What coefficients appear after multiplying things out? Just sums and products of the β_i , so all of the coefficients are in $\overline{\mathbb{Z}}$. Thus $\min_{\alpha}(x) \in \overline{\mathbb{Z}}[x]$. But the coefficients are also in \mathbb{Q} by definition, so the coefficients are in $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$ and thus $\min_{\alpha}(x) \in \mathbb{Z}[x]$. ■

Example 3.3.6 (*Showing an integer is not algebraic using minimal polynomials*): $\sqrt{5}/3 \notin \overline{\mathbb{Z}}$ since $\min_{\alpha}(x) = x^2 - 5/9 \notin \mathbb{Z}[x]$, so this is not an algebraic integer.

Proposition 3.3.7 ($\text{ff}(\mathbb{Z}_K) = K$).

- a. $\overline{\mathbb{Z}}$ has $\overline{\mathbb{Q}}$ as its fraction field, and
- b. For any number field K , the fraction field of \mathbb{Z}_K is K .
- c. If $\alpha \in \overline{\mathbb{Q}}$ then $d\alpha \in \overline{\mathbb{Z}}$ for some $d \in \mathbb{Z}^{\geq 0}$

Moreover, both (a) and (b) follow from (c).

Remark 3.3.8: Thus the subring is “big” in the sense that if you allow taking quotients, you recover the entire field. That $c \implies a, b$: suppose you want to write $\alpha \in \overline{\mathbb{Q}}$ as $\alpha = p/q$ with $p, q \in \overline{\mathbb{Z}}$. Use c to produce $d\alpha \in \overline{\mathbb{Z}}$, then just take $d\alpha/d$. The same argument works for b .

Exercise 3.3.9 (?)

Prove the proposition!

Proposition 3.3.10 (?).

Suppose $\alpha \in \overline{\mathbb{C}}$ and α is a root of a monic polynomial in $\overline{\mathbb{Z}}[x]$. Then $\alpha \in \overline{\mathbb{Z}}$.

Remark 3.3.11: This says that if a number α is the root of a monic polynomial whose coefficients are *algebraic* integers, then α itself is an algebraic integer coefficients. This corresponds to the fact that integral over integral implies integral in commutative algebra.

Exercise 3.3.12 (Prove the proposition.)

Prove this! One can use the integrality criterion (slightly challenging), or alternatively Galois theory.

4 | Quadratic Fields (Lec. 3, Thursday, January 21)

Remark 4.0.1: Today: roughly corresponds to chapter 3 in the book. Goal: do all of the big theorems in the setting of quadratic number fields, then redo everything for general number fields.

4.1 Quadratic Number Fields

Remark 4.1.1: Simplest case: \mathbb{Q} , a degree 1 number field, so the next simplest case is degree 2.

Definition 4.1.2 (Quadratic Number Fields)

A field K is a **quadratic number field** if and only if K is a number field and $[K : \mathbb{Q}] = 2$.

Remark 4.1.3: Some notation: if $d \in \mathbb{R}^\times$, then \sqrt{d} means the *positive* square root of d if $d \geq 0$, and if $d < 0$ this denotes $i\sqrt{|d|}$.

Proposition 4.1.4 (Quadratic fields are parameterized by squarefree integers).

If K is a quadratic number field, then $K = \mathbb{Q}(\sqrt{d})$ for some squarefree ^a integer $d \in \mathbb{Z}$. Moreover, this d is uniquely determined by K , so all quadratic number fields are parameterized by the set of squarefree integers.

^aSquarefree means not divisible by n^2 for any $n > 1 \in \mathbb{Z}$, or equivalently not divisible by the square of any primes.

Proof (of proposition, existence).

Existence: Since $[K : \mathbb{Q}] = 2$, we have $K \supsetneq \mathbb{Q}$ so pick $\alpha \in K \setminus \mathbb{Q}$ then $K = \mathbb{Q}(\alpha)$. Note that we could also furnish this α from the primitive element theorem, although this is overkill here. So α is a root of some degree 2 $p \in \mathbb{Q}[x]$, and by scaling coefficients we can replace this by $p \in \mathbb{Z}[x]$. So write $p(x) = Ax^2 + Bx + C$, in which case we can always write

$$\alpha = \frac{-B \pm \sqrt{B^2 - 4AC}}{2A}$$

where $A \neq 0$, since this would imply that $\alpha \in \mathbb{Q}$. Writing $\Delta := B^2 - 4AC$, we have $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{\Delta})$. This is close to what we want – it's \mathbb{Q} adjoin some integer – but we'd like that integer to be squarefree.

Now let $f \in \mathbb{Z}^{\geq 0}$ be chosen such that $f^2 \mid \Delta$ and f is as large as possible, i.e. the largest square factor of Δ . Writing $\Delta = f^2 - d$ where d is whatever remains. Then d must be squarefree, otherwise if d had a square factor bigger than 1, say $d = r^2 d'$, in which case $f^2 r^2 > f^2$ would be a larger factor of Δ . So d is squarefree, and $\Delta = f\sqrt{d}$ and thus $\mathbb{Q}(\Delta) = \mathbb{Q}(\sqrt{d})$.

Uniqueness: We'll use some extra machinery.

4.2 Norm and Trace

Definition 4.2.1 (Norm and Trace)

Let K be a number field with K/\mathbb{Q} Galois. For each $\alpha \in K$ define

$$N(\alpha) := \prod_{\sigma \in \text{Gal}(K/\mathbb{Q})} \sigma(\alpha) \quad \text{the norm}$$

$$\text{Tr}(\alpha) := \sum_{\sigma \in \text{Gal}(K/\mathbb{Q})} \sigma(\alpha) \quad \text{the trace.}$$

Remark 4.2.2: Why use these kind of sum at all? Applying any element in the Galois group just permutes the elements. Note that $N(\alpha), \text{Tr}(\alpha)$ are $G(K/\mathbb{Q})$ -invariant, and thus rational numbers in \mathbb{Q} . The norm is multiplicative, and the trace is additive and in fact \mathbb{Q} -linear: $\text{Tr}(a\alpha + b\beta) = a \text{Tr}(\alpha) + b \text{Tr}(\beta)$ for all $\alpha, \beta \in K$ and all $a, b \in \mathbb{Q}$.

Remark 4.2.3: What do the norm and trace look like for a quadratic field? We can write $K = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$ and there is a unique (non-identity) element $g \in \text{Gal}(K/\mathbb{Q})$ with $\sigma(a + b\sqrt{d}) = a - b\sqrt{d}$. We'll refer to this automorphism as **conjugation**. We can compute

$$N(a + b\sqrt{d}) = a^2 - db^2$$

$$\text{Tr}(a + b\sqrt{d}) = 2a.$$

Proof (of proposition, uniqueness continued).

Returning to the proof, suppose otherwise that $K = \mathbb{Q}(\sqrt{d_1}) = \mathbb{Q}(\sqrt{d_2})$ with $d_1 \neq d_2$ squarefree integers. Note that they must have the same sign, otherwise one of these extensions would not be a subfield of \mathbb{R} . We know $\sqrt{d_1} \in \mathbb{Q}(\sqrt{d_2})$ and thus $\sqrt{d_1} = a + b\sqrt{d_2}$ for some $a, b \in \mathbb{Q}$.

Taking the trace of both sides, the LHS is zero and the RHS is $2a$ and we get $a = 0$ and $\sqrt{d_1} = b\sqrt{d_2}$. Write $b = u/v$ with $u, v \in \mathbb{Q}$. Squaring both sides yields $v^2 d_1 = u^2 d_2$. Let p be a prime dividing d_1 ; then since d_1 is squarefree there is only one copy of p occurring in its factorization. Moreover there are an even number of copies of p coming from v^2 , thus forcing d_2 to have an odd power of p . This forces $p \mid d_2$, and since this holds for every prime factor p of d_1 , we get $d_1 \mid d_2$ since d_1 is squarefree. The same argument shows that $d_2 \mid d_1$, so they're the same up to sign: but the signs must match and we get $d_1 = d_2$.

Remark 4.2.4: Note that this results holds for every squarefree number not equal to 1. If $K = \mathbb{Q}(\sqrt{d})$, what is the ring of integers \mathbb{Z}_K ? Some more machinery will help here.

4.3 The Field Polynomial

Definition 4.3.1 (The Field Polynomial of an Element)

Assume K/\mathbb{Q} is a Galois number field and for $\alpha \in K$ define the **field polynomial** of α as

$$\varphi_\alpha(x) := \prod_{\sigma \in \text{Gal}(K/\mathbb{Q})} (x - \sigma(\alpha)).$$

Remark 4.3.2: For the same reasons mentioned for the norm/trace, we get $\varphi_\alpha \in \mathbb{Q}[x]$, and moreover $\varphi_\alpha(\alpha) = 0$. When is $\alpha \in \mathbb{Z}_K$? We have the following criterion:

Proposition 4.3.3 (The field polynomial detects integrality).

$$\alpha \in \mathbb{Z}_K \iff \varphi_\alpha(x) \in \mathbb{Z}[x].$$

Proof (of proposition).

\Leftarrow : This is easy, since if φ_α is a monic polynomial with integer coefficients, meaning that α is an algebraic integer and thus in \mathbb{Z}_K .

\Rightarrow : If $\alpha \in \mathbb{Z}_K$ then it's the root of some monic polynomial in $\mathbb{Z}[x]$, and the same is true for $\sigma(\alpha)$ and thus each $\sigma(\alpha) \in \bar{\mathbb{Z}}$. So $\varphi_\alpha(x) \in \bar{\mathbb{Z}}[x]$. We said φ_α has coefficients in \mathbb{Q} too, and thus in $\bar{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$. So the problem is reduced to finding out when $\varphi_\alpha(x)$ has integer coefficients. If $\deg(K/\mathbb{Q}) = n$, then

$$\varphi_\alpha(x) = \prod (x - \sigma(\alpha)) = x^n - \text{Tr}(\alpha)x^{n-1} + \cdots + (-1)^n N(\alpha).$$

If $n = 2$, these are the only terms, and so if K is a quadratic number field then $\alpha \in K$ is in \mathbb{Z}_K if and only if $\text{Tr}(\alpha), N(\alpha) \in \mathbb{Z}$. ■

Example 4.3.4 (of nonintuitive rings of integers): Let $K = \mathbb{Q}(\sqrt{5})$, then is it true that $\mathbb{Z}_K = \mathbb{Z}[\sqrt{5}]$? Since $1, \sqrt{5} \in \mathbb{Z}_K$, we have \supseteq since $1, \sqrt{5}$ are algebraic. The answer is **no**: take $\alpha := \frac{1 + \sqrt{5}}{2}$, then $N(\alpha) - 4/4 = -1$ and $\text{Tr}(\alpha) = 1$. These are integers, so $\alpha \in \mathbb{Z}_K$, and in fact α is a root of $x^2 - x - 1 \in \mathbb{Z}[x]$.

4.4 Classification of \mathbb{Z}_K

Theorem 4.4.1 (Classification of \mathbb{Z}_K for quadratic fields).

Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic number field. Then

- If $d \equiv 2, 3 \pmod{4}$, then $\mathbb{Z}_K = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$.
- If $d \equiv 1 \pmod{4}$, then $\mathbb{Z}_K = \left\{ \frac{1 + b\sqrt{d}}{2} \mid a, b \in \mathbb{Z}, a \equiv b \pmod{2} \right\}$.

Remark 4.4.2: For $d = 1$, if a, b are even then we just recover the $d = 2, 3$ case, so we're picking up extra elements from when a, b both odd.

Proof (?).

Let $\alpha \in K$ and write $\alpha = A + B\sqrt{d}$ with $A, B \in \mathbb{Q}$.

Exercise (?)

Check that $N(\alpha), \text{Tr}(\alpha) \in \mathbb{Z}$ for both cases.

Assuming now that $N(\alpha), \text{Tr}(\alpha) \in \mathbb{Z}$, then $A^2 - dB^2 \in \mathbb{Z}$. Multiply this by 2 to get $(2A)^2 - d(2B)^2 \in 4\mathbb{Z}$. Recalling that $\text{Tr}(\alpha) = 2A$, we have $(2A)^2 \in \mathbb{Z}$ and thus $d(2B)^2 \in \mathbb{Z}$ as well. The claim now is that $2B \in \mathbb{Z}$: we know $2B \in \mathbb{Q}$. If $2B \notin \mathbb{Z}$, then the denominator has some prime factor. This prime factor appears twice in $(2B)^2$, and $d(2B)^2 \in \mathbb{Z}$ then means that two copies of p appear in d in order to cancel – however, we assumed d was squarefree. We now know that $A, B \in \frac{1}{2}\mathbb{Z}$, so write $A = (1/2)a'$ and $B = (1/2)b'$. Thus

$$\alpha = (1/2)a' + (1/2)b'\sqrt{d} \implies N(\alpha) = ((a')^2 - d(b')^2)/4 \in \mathbb{Z}.$$

So the numerator is a multiple of 4, which yields $(a')^2 \equiv d(b')^2 \pmod{4}$. We proceed by cases.

Case 1: $d \equiv 2, 3 \pmod{4}$. If b' is odd then $(b')^2 \equiv 1 \pmod{4}$, which holds for any odd number. But then $(a')^2 = d(b')^2 \equiv d \pmod{4}$, which is a problem – squares modulo 4 can only be 0 or 1. This is a contradiction, so b' must be even. Then $(b')^2 \pmod{4} = 0$, which forces $a' \equiv 0 \pmod{4}$ and a' must be even. But if a', b' are both even, $(1/2)a', (1/2)b' \in \mathbb{Z}$ and we obtain $\alpha \in \mathbb{Z} + \sqrt{d}\mathbb{Z}$.

Case 2: If $d \equiv 1 \pmod{4}$, then $(a')^2 \equiv (b')^2 \pmod{4}$. We can conclude that a', b' are either both odd or both even, otherwise we'd get $0 \equiv 1 \pmod{4}$, and thus we can write $a' \equiv b' \pmod{2}$. But this was exactly the condition appearing in the theorem. ■

Remark 4.4.4: Let K be a quadratic number field. Then we can reformulate the previous results as:

$$\mathbb{Z}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \equiv 2, 3 \pmod{4} \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & d \equiv 1 \pmod{4}. \end{cases}$$

We've also shown that \mathbb{Z}_K is a free \mathbb{Z} -module of rank 2, with basis either $\{1, \sqrt{d}\}$ or $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$.

Remark 4.4.5: What is true for general number fields? Important theorem: \mathbb{Z}_K is always a free \mathbb{Z} -module, i.e. there always exists an *integral basis*. Surprisingly, it's not always true that $\mathbb{Z}_K = \mathbb{Z}[\ell]$ for ℓ a single element.

5 | Failure of Unique Factorization (Lec. 4, Wednesday, January 27)

5.1 Revisiting a Counterexample to Unique Factorization

Remark 5.1.1: Today roughly corresponds to chapter 4: "Paradise Lost"! Setup: K is a quadratic field, a degree 2 extension of \mathbb{Q} , which can be written as $K = \mathbb{Q}(\sqrt{d})$ with d squarefree. Last time, we completely described \mathbb{Z}_K (the algebraic integers in K):

$$\mathbb{Z}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \equiv 2, 3 \pmod{4} \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & d \equiv 1 \pmod{4}. \end{cases}$$

We saw that the second admitted a different description as $\left\{\frac{a+b\sqrt{d}}{2}\right\}$ where a, b are either both even or both odd. Note that we can do interesting arithmetic in \mathbb{Z}_K , but it's not necessarily well-behaved: \mathbb{Z}_K is not always a UFD.

Example 5.1.2 (A counterexample to unique factorization): Letting $d = -5$, we have $\mathbb{Z}_K = \mathbb{Z}[\sqrt{-5}]$ where 6 factors in two ways:

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

Note that this isn't quite enough to show failure of unique factorization, e.g. we can factor $16 = (4)(4) = (2)(8)$. Here you should check that all 4 factors are irreducible, and that the factors on the right aren't unit multiples of the ones on the left. For example, $21 = (-7)(-3) = (7)(3)$, but the factors only differ by the unit $-1 \in \mathbb{Z}^\times$. The key to checking all of those: the **norm map**:

$$N(a + b\sqrt{-5}) = (a + b\sqrt{-5})(a - \sqrt{-5}) = a^2 + 5b^2.$$

where the second factor was the *conjugate*, i.e. the image of the element under the nontrivial element of the Galois group of K/\mathbb{Q} . If $a + b\sqrt{-5} \in \mathbb{Z}_K$, then $N(a + b\sqrt{-5}) \in \mathbb{Z}_{\geq 0}$ and is equal to zero if and only if $a + b\sqrt{-5} = 0$. Moreover, this is a unit if and only if its norm is 1,¹ i.e. $a^2 + 5b^2 = 1$, which forces $b = 0$ and $a = \pm 1$. So $U(\mathbb{Z}[\sqrt{-5}]) = \{\pm 1\}$.

We'll show one of the factors is irreducible, $1 + \sqrt{-5}$. Recall that $x \in R$ a domain is **irreducible** if and only if whenever $x = ab$, one of a, b is a unit. It itself is not a unit, since $N(1 + \sqrt{-5}) = 6 \neq 1$. So suppose $1 + \sqrt{-5} = \alpha\beta$. Then

$$6 = N(\alpha\beta) = N(\alpha)N(\beta),$$

and so up to reordering, we have $N\alpha = 2, N\beta = 3$. Writing $\alpha = a + b\sqrt{-5}$ and taking norms yields $2 = a^2 + 5b^2$, which has no solutions: considering the equation (mod 5) yields $2 \equiv a^2$, but 2 is not a square in $\mathbb{Z}/5\mathbb{Z}$. \nexists

Note that the only other way of factoring 6 is $6 = (1)(6)$, and taking norms shows that one factor is a unit. So if we assume α, β aren't units, both $N\alpha, N\beta > 1$, which leads to the previous situation. By similar arguments, all 4 factors are irreducible.

To see that the LHS factors aren't unit multiples of the RHS factors, we can use the fact that the units are ± 1 , and multiplying the LHS by ± 1 can't yield 2 or 3. So this is a genuine counterexample to unique factorization.

5.2 Factorization Theory

Remark 5.2.1: What went wrong in the previous example? We'll use a big of terminology from an area of algebra called *factorization theory*. Many concepts related to divisibility can be discussed in this language!

Definition 5.2.2 (Monoid)

A **monoid** is a nonempty set with a commutative associative binary operation \cdot with an identity 1. We say a monoid is **cancellative** if and only if whenever $\alpha\beta = \beta\alpha$ or $\beta\alpha = \gamma\alpha$ then $\beta = \gamma$.


Definition 5.2.3 (Terminology for Cancellative Monoids)

Let M be a cancellative monoid. Then

- $\alpha \mid \beta$ if and only if $\beta = \alpha\gamma$ for some γ .
- ϵ is a **unit** if $\epsilon \mid 1$.
- α, β are **associates** if $\alpha = \epsilon\beta$ for some unit ϵ
- $\pi \in M$ is **irreducible** if and only if π is not a unit and whenever $\pi = \alpha\beta$ then either α or β is a unit.

¹ \Leftarrow : If the norm is 1, the conjugate is the inverse. For the reverse direction, the argument was more complicated, and reduced to showing norms of units are ± 1 , and positivity forces it to be 1.

- $\pi \in M$ is **prime** whenever $\pi \mid \alpha\beta$ then $\pi \mid \alpha$ or $\pi \mid \beta$.
- $\delta \in M$ is a greatest common divisor of α, β if and only if δ is a common divisor that is divisible by every other common divisor.
- M is a **unique factorization monoid** if and only if every nonunit element in M factors uniquely (up to order and associates) as a product of irreducibles.

Remark 5.2.4: Given R an integral domain, then $R \setminus \{0\}$ with multiplication is a cancellative monoid. Moreover, $R \setminus \{0\}$ is a unique factorization monoid if and only if R is a UFD. 

Question 5.2.5

How do you show something is a UFD?

Answer 5.2.6

Recall how this proof went for \mathbb{Z} :

- Use existence of a division algorithm.
- Prove Euclid's lemma: every irreducible is prime.
- Use factorization into irreducibles and proceed by induction, writing out two factorizations and cancelling things out in a combinatorial way.

So we'd like

1. To know that irreducibles are prime, and
2. Everything to factor into irreducibles.

Definition 5.2.7 (Atomic)


For M a cancellative monoid, M is **atomic** if every nonunit element of M is a product of irreducibles.

Proposition 5.2.8 (Monoids have unique factorization iff atomic and irreducibles are prime).

Let M be a cancellative monoid, then M is a UFM if and only if M is atomic and every irreducible is prime in M .

Proof (of proposition).

Omitted – no new ideas when compared to proof of unique factorization in \mathbb{Z} . 

Remark 5.2.9: Note that in \mathbb{Z} , working in $\mathbb{Z}_{\geq 0}$ is useful because the only positive unit is 1, and so any elements differing by a unit are in fact equal. Can we emulate this for cancellative monoids? The answer is yes, by modding out by the equivalence relation of being equivalent up to a unit. 

Definition 5.2.10 (Reduced Monoid)

Define $M_{\text{red}} := M / \sim$ where $a \sim b \iff a - b \in M^\times$. The operation on M descends to well-defined operation on M_{red} , and irreducibles and primes are the same in M and M_{red} .

Example 5.2.11 (of a more familiar reduced monoid): This is supposed to look like $\mathbb{Z}_{\geq 0}$, where $-7 \in M \mapsto 7 \in M_{\text{red}}$.

Proposition 5.2.12 (A monoid has unique factorizations iff its reduced monoid does).

M is a UFM if and only if M_{red} is a UFM if and only if every element of M_{red} factors uniquely as a product of irreducibles, up to order.

Remark 5.2.13: What did this buy us? We didn't have to worry about associates in the above statement, and the only unit is 1.

Remark 5.2.14: Why isn't $\mathbb{Z}[\sqrt{-5}]$ is UFD? It doesn't have enough elements to make unique factorization work!

Example 5.2.15 (of common refinements): In \mathbb{Z}^+ , write $210 = 21 \cdot 10 = 14 \cdot 15$. These two factorizations differ but admit a common refinement to $(7 \cdot 3)(2 \cdot 5) = (7 \cdot 2)(3 \cdot 5)$, where it becomes clear that these factorizations are equal up to ordering. This is **Euler's Four Number Theorem**, which turns out to be equivalent to unique factorization.

Theorem 5.2.16 (Characterization of unique factorization monoids).

Let M be a cancellative atomic reduced monoid. Then M is a UFM if and only if whenever $\alpha, \beta, \gamma, \delta \in M$ such that $\alpha\beta = \gamma\delta$, there are ρ, σ, τ, ν with

$$\alpha = \rho\sigma$$

$$\beta = \tau\nu$$

$$\gamma = \rho\tau$$

$$\delta = \sigma\nu.$$

Note that plugging these in on the LHS and RHS respectively yield the same factors, just reordered.

Proof (of theorem).

Omitted, exercise in chasing definitions. The interesting part is that you can go backward! ■

Remark 5.2.17: Let $M_{\text{red}} := (\mathbb{Z}[\sqrt{5}] \setminus \{0\})_{\text{red}}$, motivated by the fact that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD if $\mathbb{Z}[\sqrt{-5}] \setminus \{0\}$ is not a UFM, or equivalently its reduction is not a UFM. Then M is not a UFM. Noting that M is reduced under an equivalence relation, write $\langle \alpha \rangle$ for the class of α in M for any $\alpha \in \mathbb{Z}[\sqrt{-5}]$.

Our original counterexample for unique factorization now reads

$$\langle 1 + \sqrt{-5} \rangle \langle 1 - \sqrt{5} \rangle = \langle 2 \rangle \langle 3 \rangle.$$

This is still a counterexample since these pairs admit no common refinement.

Why are there “not enough elements” in $\mathbb{Z}[\sqrt{-5}]$? Recall that for integral domains (as rings), two elements differ by a unit precisely when they generate the same ideal. So we can think of elements of M_{red} as nonzero principal ideals of M , which we’ll write as $\text{Prin}(\mathbb{Z}[\sqrt{-5}])$. To make this set of ideals into a monoid, one define $\langle \alpha \rangle \langle \beta \rangle = \langle \alpha\beta \rangle$, where it’s easy to check that this is well-defined. So the failure of unique factorization is a failure of factorization in this set of ideals. We can embed this in a larger collection of ideals by just deleting the word “principal”, which will restore unique factorization.

Definition 5.2.18 (Multiplication of Ideals)

Let R be a commutative ring (always with 1). If $I, J \trianglelefteq R$ are ideals, we define

$$IJ := \left\langle \left\{ \alpha_i \beta_i \mid \alpha_i \in I, \beta_i \in J \right\} \right\rangle = \left\langle \sum \alpha_i \beta_i \mid \alpha_i \in I, \beta_i \in J \right\rangle.$$

If R is a domain, define the monoid $\text{Id}(R)$ the collection of nonzero ideals of R with the above multiplication.

Remark 5.2.19: Note that the naive definition $IJ := \{ij \mid i \in I, j \in J\}$ is not necessarily an ideal, since it may not be closed under addition. Taking the smallest ideal containing all products fixes this.

Proposition 5.2.20 (If R is a domain, then $\text{Id}(R)$ is a monoid).

Let R be a commutative ring. Then

- Multiplication \cdot for ideals is commutative,
- Multiplication \cdot for ideals is associative,
- The identity is $\langle 1 \rangle = R$,
- Multiplication distributes over addition of ideals, i.e. $I(J + K) = IJ + IK$,
- $IJ \subseteq I \cap J$,
- If $I = \langle \alpha_1, \dots, \alpha_j \rangle$ and $J = \langle \beta_1, \dots, \beta_k \rangle$ then $IJ = \langle \alpha_1 \beta_1, \dots, \alpha_j \beta_k \rangle$ is generated by all of the jk pairwise products,
- If R is a domain and I, J are nonzero then IJ is nonzero,

As a consequence, $\text{Id}(R)$ is a monoid when R is a domain.

Remark 5.2.21: So instead of working in $\text{Prin}(\mathbb{Z}[\sqrt{-5}])$, we’ll work in $\text{Id}(\mathbb{Z}[\sqrt{-5}])$. The claim is that we can refine our bad factorizations. Define

- $I := \langle 1 + \sqrt{-5}, 2 \rangle$
- $I' := \langle 1 - \sqrt{-5}, 2 \rangle$
- $J := \langle 1 + \sqrt{-5}, 3 \rangle$

- $J' := \langle 1 - \sqrt{-5}, 3 \rangle$

Then

- $IJ = \langle 1 + \sqrt{-5} \rangle$
- $I'J' = \langle 1 - \sqrt{-5} \rangle$
- $JJ' = \langle 3 \rangle$
- $II' = \langle 2 \rangle$

We can then write

$$\langle 1 + \sqrt{-5} \rangle \langle 1 - \sqrt{-5} \rangle = \langle 2 \rangle \langle 3 \rangle \implies (IJ)(I'J') = (II')(JJ'),$$

where the same terms are occurring in a different order. For an example of how to work these out, let's compute IJ . We get

$$\begin{aligned} IJ &= \langle (1 + \sqrt{-5})^2, 3(1 + \sqrt{-5}), 2(1 + \sqrt{-5}), 6 \rangle \\ &= \langle 1 + \sqrt{-5} \rangle \langle 1 + \sqrt{-5}, 3, 2, 1 - \sqrt{-5} \rangle \\ &= \langle 1 + \sqrt{-5} \rangle \langle 1 \rangle \\ &= \langle 1 + \sqrt{-5} \rangle, \end{aligned}$$

using the fact that $3 - 2 = 1$ is in the ideal on the second line.

We'll see later that this process allows you to recover unique factorization in \mathbb{Z}_K for any number field K .

6 | Euclidean Quadratic Fields (Lec. 5, Thursday, January 28)

6.1 Setup

Remark 6.1.1: Today: roughly corresponds to Chapter 5. In a first algebra course, one shows that if R is a Euclidean domain, then the arithmetic of R is very interesting:

- R is a PID, and as a consequence
- R is a UFD

Definition 6.1.2 (Euclidean Domain)

A domain R is **Euclidean** if and only if there is a function $\varphi: R \setminus \{0\} \rightarrow \mathbb{Z}^{\geq 0}$ such that for all $a, b \in R$ with $b \neq 0$ there are $q, r \in R$ with $a = bq + r$ with $r = 0$ or $\varphi(r) < \varphi(b)$. φ is referred to as a **Euclidean function**.

Example 6.1.3 (Examples of Euclidean functions):

- For $R = \mathbb{Z}$, one can take $\varphi(\cdot) := |\cdot|$.
- $R = \mathbb{F}[t]$ for \mathbb{F} a field with $\varphi(\cdot) = \deg(\cdot)$.

Remark 6.1.4: Given a number field K , does \mathbb{Z}_K have nice factorization, i.e. is it a UFD? Not always, as we saw last time. If it were Euclidean, then yes!

Question 6.1.5

Which quadratic fields K have a Euclidean ring of integers \mathbb{Z}_K ?

Definition 6.1.6 (Euclidean and Norm-Euclidean Number Fields)

If K is a quadratic field, then

- K is **Euclidean** if and only if \mathbb{Z}_K is a Euclidean domain,
- K is **norm-Euclidean** if and only if \mathbb{Z}_K is Euclidean with respect to $\varphi(\cdot) := |N(\cdot)|$.

Proposition 6.1.7 (Characterization of norm-Euclidean quadratic fields).

Let K be a quadratic field. Then K is norm-Euclidean if and only if for all $\beta \in K$ there is a $\gamma \in \mathbb{Z}_K$ such that $|N(\beta - \gamma)| < 1$. In other words, K is norm-Euclidean if and only if every element can be approximated by an element in \mathbb{Z}_K .

Proof (of proposition).

\Leftarrow : Let $a, b \in \mathbb{Z}_K$ with $b \neq 0$. Define $\beta := a/b \in K$, then by assumption choose γ such that $\left| N\left(\frac{a}{b} - \gamma\right) \right| < 1$. Multiplying both sides by $N(b)$ and using the fact that $N(\cdot), |\cdot|$ are multiplicative, we have

$$|N(a - b\gamma)| < |N(b)|.$$

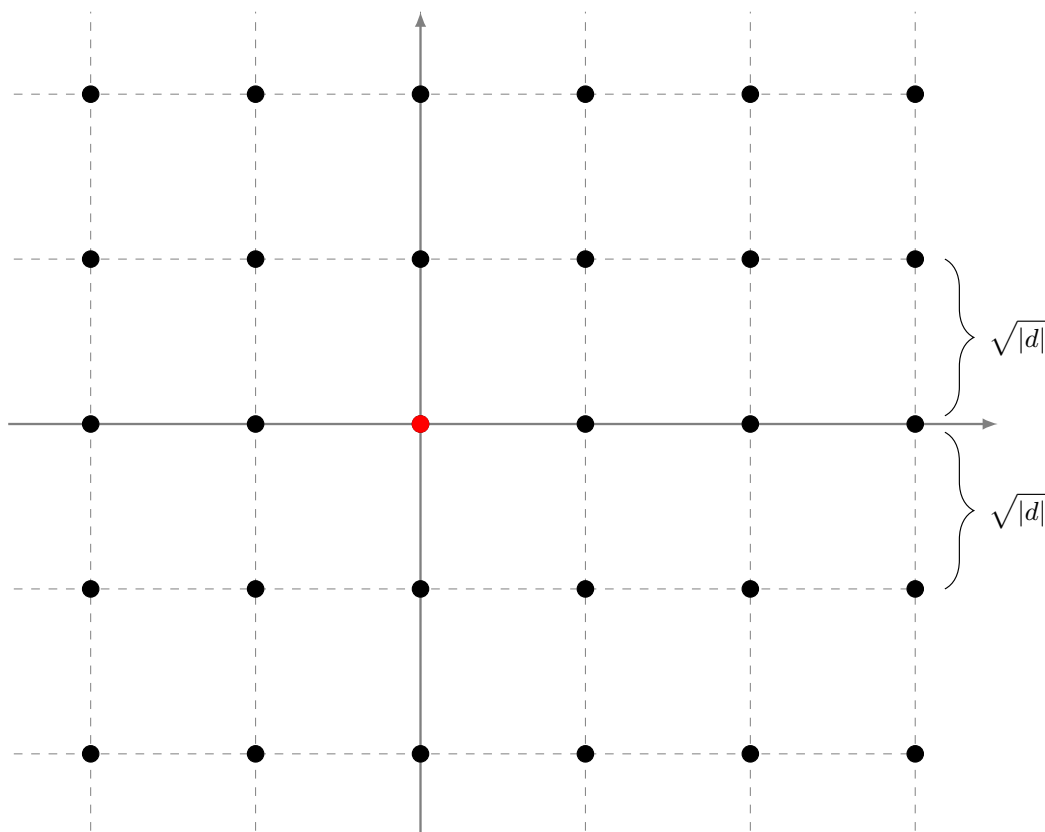
Then $a = bq + r := b\gamma + (a - b\gamma)$. ■

6.2 Norm-Euclidean Imaginary Quadratic Fields

Remark 6.2.1: Suppose $K = \mathbb{Q}(\sqrt{d})$ with $d < 0$ squarefree, so we can write

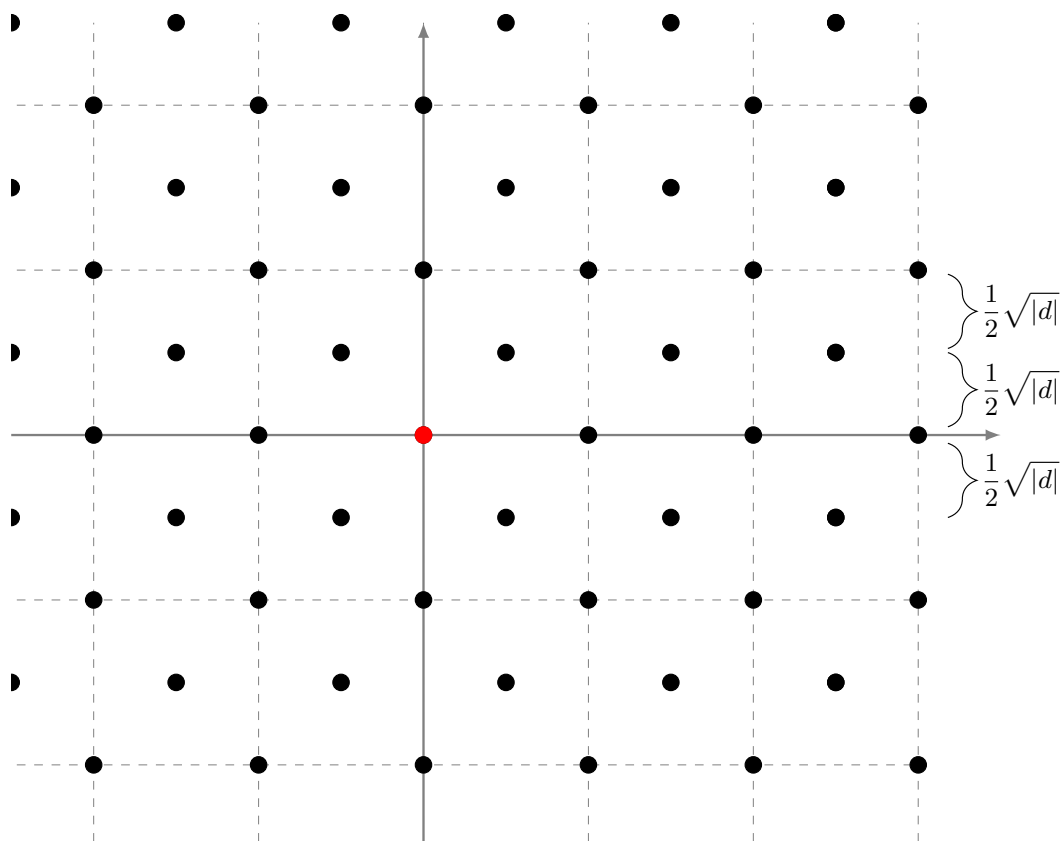
$$K = \{a + b\sqrt{d} \mid a, b, \in \mathbb{Q}\} = \{a + bi\sqrt{|d|} \mid a, b, \in \mathbb{Q}\} \subseteq \mathbb{C}.$$

Geometrically, this is a dense subset of \mathbb{C} , so it's not easy to draw. But we can draw \mathbb{Z}_K – what does it look like? We know that $d \equiv 2, 3 \pmod{4}$ then $\mathbb{Z}_K = \{a + b\sqrt{d} \mid a, b, \in \mathbb{Z}\}$:



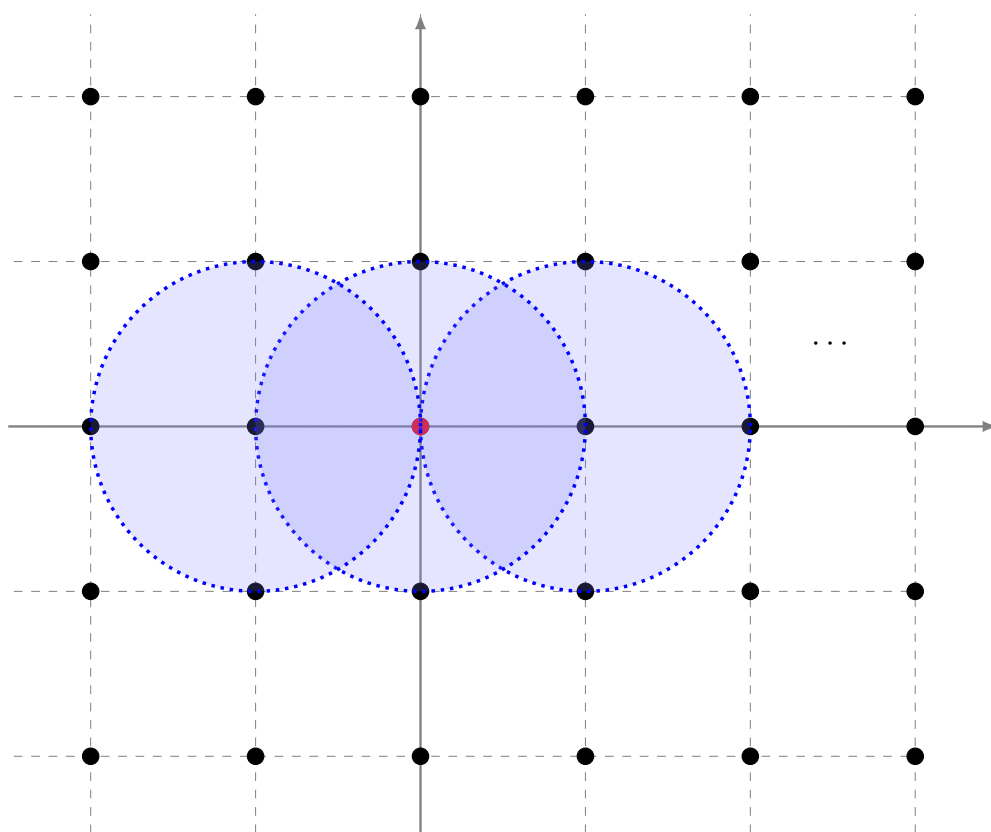
When $d \equiv 1 \pmod{4}$, we have $\mathbb{Z}_K = \left\{ \frac{1}{2}(a + b\sqrt{d}) \mid a, b, \in \mathbb{Z}, a \equiv b \pmod{2} \right\}$. On the real axis, if $b = 0$ then a is an even integer and $\{(1/2)a\}$ is all integers. To get the remaining elements, we

don't just shift up and down: setting $b = 1$ yields elements that look like $(1/2)a + \sqrt{d}$ where a is odd, so we get the following:

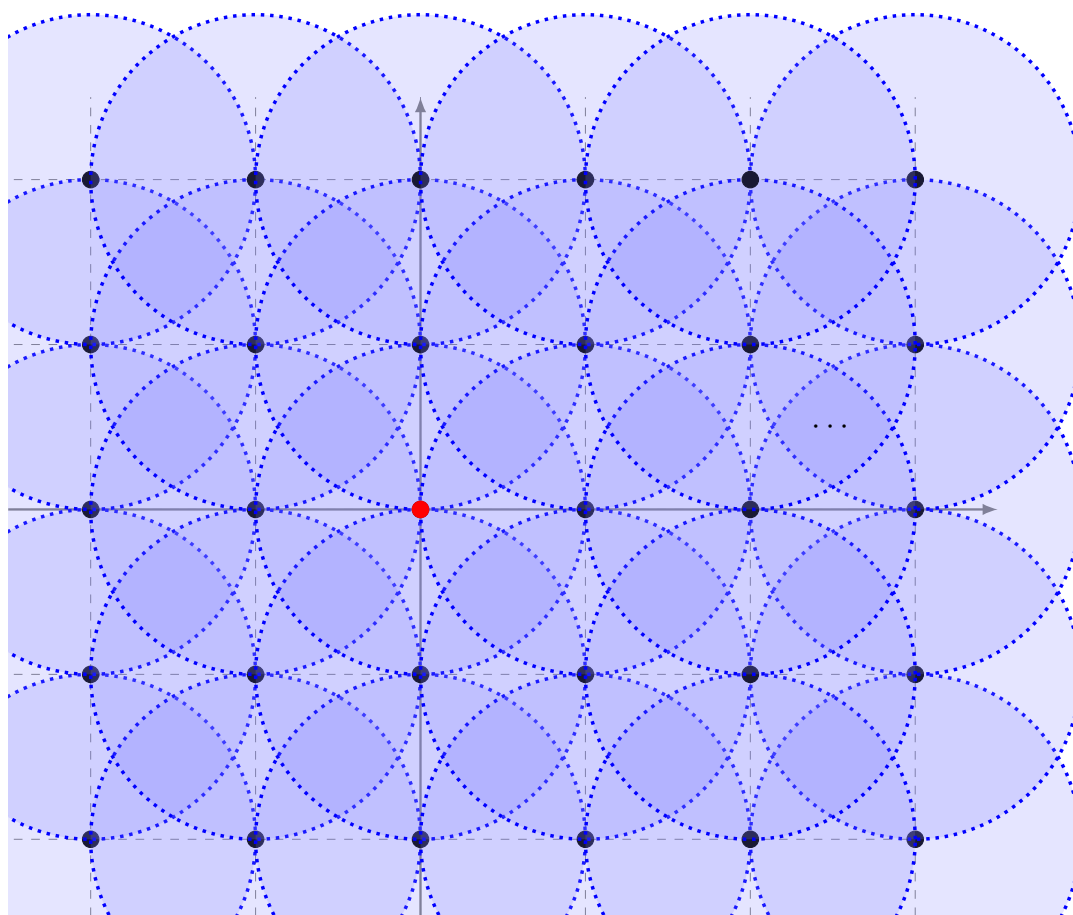


Now we can think of the criterion for an imaginary quadratic field to be norm-Euclidean: what does it mean to be within norm 1 of an element of \mathbb{Z}_K ? If $z \in K$, we can write $N(z) = z\bar{z} = |z|^2$, and thus reformulate our criterion: K is norm-Euclidean if and only if for all $\beta \in K$ there exists a $\gamma \in \mathbb{Z}_K$ such that $|\beta - \gamma| < 1$. Note this this is the familiar geometric distance in \mathbb{C} .

Example 6.2.2(?): $\mathbb{Q}(i)$ is norm-Euclidean: the ring of integers is $\mathbb{Z}(i)$, which is the integer lattice in \mathbb{C} . Note one can cover \mathbb{C} by open circles of radius 1:



Continuing this way, every point with rational coordinates can be covered by some open disc of radius 1:



Remark 6.2.3: Note that this doesn't work for arbitrary d , since the distance between the horizontal lines grows with d . It's not hard to work out the exact list where everything *is* covered:

Theorem 6.2.4 (When quadratic fields are norm-Euclidean).

K is norm-Euclidean if and only if $d \in \{-1, -2, -3, -7, -11\}$.

Corollary 6.2.5 (When rings of integers are PIDs/UFDs).

For these d , \mathbb{Z}_K is a PID and thus a UFD.

Remark 6.2.6: So we've classified all norm-Euclidean imaginary quadratic fields. What about removing the word "norm"? We restricted to $|N(\cdot)|$ because there was a particularly nice geometric

interpretation, whereas being Euclidean involves a mysterious φ . Remarkably, it can be done, and it's the same list!

Theorem 6.2.7 (Motzkin).

For K an imaginary quadratic field, K is Euclidean if and only if $d \in \{-1, -2, -3, -7, -11\}$.

Remark 6.2.8: If \mathbb{Z}_K were never a PID in these cases, we could immediately conclude it wasn't Euclidean either. But there are values of d not on this list for which \mathbb{Z}_K is a PID, e.g. $d = -19$. Since $-19 \equiv 1 \pmod{4}$, one can write $\mathbb{Z}_K = \mathbb{Z} \left[\frac{1 + \sqrt{-19}}{2} \right]$, and by Motzkin's theorem this is a PID which is not a Euclidean domain.

Remark 6.2.9: We'll prove this theorem! First we need a few lemmas.

Lemma 6.2.10 (Most imaginary quadratic fields have only two units).

Let K be an imaginary quadratic field, then $U(\mathbb{Z}_K) = \{\pm 1\}$ except if $d = -1, -3$.

Proof (of lemma (Important!)).

We know that the units u satisfy $|N(u)| = 1$, and for imaginary quadratic fields norms are non-negative, so we know $N(u) = 1$. What are the solutions this equation? Suppose $d = 2, 3 \pmod{4}$, then we can write $\alpha = a + b\sqrt{d}$ with $a, b \in \mathbb{Z}$ and $1 = N\alpha = a^2 - db^2 = a^2 + |d|b^2$. If $|d| = 1$ then this will have four solutions: $(a, b) = (\pm 1, 0), (0, \pm 1)$.

Otherwise if $|d| > 1$ then $b = 0$ and $a^2 = 1 \implies a = \pm 1$ and thus $\alpha = \pm 1$. So in this case, the only units are ± 1 , unless $|d| = 1$. But the only negative squarefree integer of absolute value 1 is -1 .

Suppose $d \equiv 1 \pmod{4}$. In this case, we need

$$1 = \frac{a^2 + |d|b^2}{4} \implies a^2 + |d|b^2 = 4.$$

Note that $d < 0$ is $1 \pmod{4}$, so it's possible that $d = -3$ – but this was one of the exceptions in the theorem, so assume otherwise. Thus $|d| \geq 7$, which forces $b = 0 \implies a^2 = 4 \implies a = \pm 2$. Then $\alpha = \pm 1$. ■

Remark 6.2.11: For the excluded cases, the units can be explicitly computed. When $d = -1$, $U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$, yielding 4 units. When $d = -3$,

$$U\left(\mathbb{Z}\left[\frac{1 + \sqrt{-3}}{2}\right]\right) = \left\{ \pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2} \right\},$$

yielding 6 units. Note that in the first case, these are exactly the 4th roots of unity, and in the second case these are the sixth roots. This is a general phenomenon that will appear again!

Lemma 6.2.12 (Norm of generator of principal ideal equals size of quotient).

Let K be any quadratic field and $\alpha \in \mathbb{Z}_K$. Then $\#\mathbb{Z}_K / \langle \alpha \rangle = |N(\alpha)|$.

6.3 Proof of Motzkin's Theorem

Proof (of Motzkin's Theorem).

We want to show that being Euclidean implies $d = -1, -2, -3, -7, -11$. Suppose \mathbb{Z}_K is Euclidean with respect to φ . Choose $\beta \in \mathbb{Z}_K$ nonzero and not a unit with $\varphi(\beta)$ minimal among all such β .

Claim:

$$\#\mathbb{Z}_K / \langle \beta \rangle \leq 3.$$

Proof (of claim).


For any $\alpha \in \mathbb{Z}_K$ and consider it in the quotient. Since \mathbb{Z}_K is Euclidean, we can write $\alpha = \beta + \gamma + \rho$ where either $\rho = 0$ or $\varphi(\rho) < \varphi(\beta)$. How can the second possibility occur? β was chosen to have a minimal φ value, so the only smaller elements are units. So $\rho = 0$ or ρ is a unit. Reducing $(\text{mod } \beta)$, we obtain $\alpha = \rho \pmod{\beta}$, and hence $\#\mathbb{Z}_K / \langle \beta \rangle \leq 1 + \#U(\mathbb{Z}_K)$ where the 1 comes from the zero element and everything else in the quotient has a representative that is a unit. This is bounded above by 3 when $d \neq -1, -3$, which is one of the exclusions in the theorem. ■

Now we have $N(\beta) \leq 3$ and this can be solved – if d is large, these solutions are widely distributed. If $d \equiv 2, 3 \pmod{4}$ then $\beta = a + b\sqrt{d}$ with $a, b \in \mathbb{Z}$ and $a^2 + |d|b^2 \leq 3$. We can assume $|d| > 3$, since $d = -1, -2$ are excluded. Then $b = 0$ is forced, and $a = 0, \pm 1$. But why can't $\beta = 0, \pm 1$? It was chosen to be minimal among *nonzero nonunits*. ✗

If $d \equiv 1 \pmod{4}$, then $\beta = \frac{a + b\sqrt{d}}{2}$ where $a, b \in \mathbb{Z}$, $a \equiv b \pmod{2}$. Then

$$\frac{a^2 + |d|b^2}{4} \leq 3 \implies a^2 + |d|b^2 \leq 12.$$

Now considering that $-d \equiv 1 \pmod{4} \implies -d \in \{-3, -7, -11, \dots\}$, the first three of which are on our list of exclusions. So we can assume $|d| \geq 15$, which forces $b = 0$, a must be even, and $a^2 \leq 12$. So $a = 0, \pm 2 \implies \beta = 0, \pm 1$. ✗ ■

Remark 6.3.1: What's the story for real quadratic fields? We understand norm-Euclidean ones, although the proofs aren't nearly as simple. Things worked out nicely here because we had circles in the plane; in the real case these end up being complicated hyperbolas. One can prove that if $d > 73$ then $K := \mathbb{Q}(\sqrt{d})$ is not norm-Euclidean. What are the Euclidean real quadratic fields? The situation is much different, and there are two open conjectures. 

Conjecture 6.3.2.

For real quadratic fields K , \mathbb{Z}_K is a PID for infinitely many $d > 0$. We don't even know about to prove there are just infinitely many *number* fields satisfying this condition! We believe this is true since it happens a positive proportion of the time experimentally.

Conjecture 6.3.3.

If \mathbb{Z}_K is a PID, then \mathbb{Z}_K is Euclidean with respect to some norm function. This is a consequence of a certain generalization of the RH. This is not true for imaginary quadratic fields. Why is it different here? The unit group plays a large role, and is infinite here. The real conjecture is that for K any number field, if \mathbb{Z}_K is a PID with infinitely many units then \mathbb{Z}_K is Euclidean.

Remark 6.3.4: There has been some progress, a result along the lines of there being at most two exceptions, but we don't know if those exceptions exist.

7 | Ideal Theory and Quadratic Fields (Lec. 6, Tuesday, February 02)

7.1 Prime Factorization in $\text{Id}(\mathbb{Z}_K)$

Remark 7.1.1: Today: roughly chapter 6. Recall that if R is a domain, we defined $\text{Id}(R)$ as the set of nonzero ideals of R , which is a monoid. We want to get to the following theorem:

Theorem 7.1.2 (Fundamental Theorem of Ideal Theory (for Quadratic Fields)).

Let K be a quadratic field, then $\text{Id}(\mathbb{Z}_K)$ is a UFM.

Remark 7.1.3: This means that everything factors into irreducibles, and when you have unique factorization, irreducible is the same as prime. Note that “prime” here means in this monoidal sense – does this match up with the existing notion of a prime ideal? I.e. that \mathfrak{p} is prime if and only if R/\mathfrak{p} is a domain, or $ab \in \mathfrak{p} \implies a, b \in \mathfrak{p}$?

Proposition 7.1.4 (Prime in monoids equals prime in rings for $\text{Id}(\mathbb{Z}_K)$).

“Prime” in the usual ring-theoretic sense is equivalent to “prime” in the monoidal sense for $\text{Id}(\mathbb{Z}_K)$.

Remark 7.1.5: Recall though that $\text{Id}(\mathbb{Z}_K)$ is a reduced monoid, so the only unit is the identity, so uniqueness is just up to ordering and doesn't involve additional units. We can restart the unique factorization theorem:

Proposition 7.1.6 ($\text{Id}(\mathbb{Z}_K)$ has prime factorization).

Every nonzero ideal of \mathbb{Z}_K factors uniquely as a product of prime ideals in \mathbb{Z}_K .

Remark 7.1.7: Can we explicitly understand what ideals of \mathbb{Z}_K look like for quadratic fields?

Definition 7.1.8 (Standard Bases of Ideals)

Let $K = \mathbb{Q}(\sqrt{d})$, so $\mathbb{Z}_K = \mathbb{Z}[\sqrt{d}]$ if $d \equiv 2, 3 \pmod{4}$ or $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ if $d \equiv 1 \pmod{4}$. Define $\tau = \sqrt{d}$ or $(1 + \sqrt{d})/2$ accordingly and write $\mathbb{Z}_K = \mathbb{Z}[\tau]$.

Remark 7.1.9: Note that $\{1, \tau\}$ is a \mathbb{Z} -basis of \mathbb{Z}_K . An ideal of \mathbb{Z}_K is a submodule as a \mathbb{Z} -module, which is free, so any ideal is free of rank at most 2. Can we write down such a basis?

Lemma 7.1.10 (*Existence of τ*).

Let I be a nonzero ideal of \mathbb{Z}_K , then I contains a nonzero integer and an element of the form $a + b\tau$ where $b \neq 0$.

Proof (of lemma).

How to produce a nonzero rational integer: let $\alpha \in I$ be nonzero and take the norm. Then $N\alpha$ is a nonzero integer, and since $\bar{\alpha} \in \mathbb{Z}_K$ we have $N\alpha = \alpha\bar{\alpha} \in I$. Now since $\tau \in \mathbb{Z}_K$ and I absorbs multiplication we can set $b := N\alpha(\tau) \in I$. ■

Remark 7.1.11: We wanted a nice description of bases for ideals – here it is!

Proposition 7.1.12 (*Existence of a standard basis for an ideal*).

Let $I \leq \mathbb{Z}_K$ be a nonzero ideal. Choose $n \in \mathbb{Z}^+$ such that $I \cap \mathbb{Z} = n\mathbb{Z}$.^a Choosing $B \in \mathbb{Z}^+$ such that $\{b \in \mathbb{Z} \mid a + b\tau \in I \text{ for some } a \in \mathbb{Z}\} = B\mathbb{Z}$.^b Since B is in the LHS, pick $A \in \mathbb{Z}$ with $A + B\tau \in I$. Then $\{n, A + B\tau\}$ is a \mathbb{Z} -basis for I .

Any such basis is referred to as a **standard basis** for I

^aWhy does this n exist? Every ideal in \mathbb{Z} is of the form $n\mathbb{Z}$, and it's easy to check $I \cap \mathbb{Z}$ is an ideal in \mathbb{Z} since it's an ideal of \mathbb{Z}_K intersected with \mathbb{Z} . How do we know it's not the zero ideal? This is exactly given by the last lemma.

^bThe LHS is the set of coefficients of τ , which is an ideal of \mathbb{Z} , and we can take it to be positive since the LHS is not the zero ideal by the lemma.

Remark 7.1.13: Note that this is only determined up to $A \pmod{n}$.

Proof (of proposition).

Take any element in I , which can be represented as $a + b\tau$, we want to show that this can be expressed in terms of the proposed basis. Note that $B \mid b$ by its definition, since B generated the ideal of τ coefficients. So write $b = Bs$, then

$$(a + b\tau) - (A + B\tau)s \in \mathbb{Z} \cap I = \langle n \rangle.$$

So write this difference as nr for some $r \in \mathbb{Z}$, then rearranging yields

$$a + b\tau = nr + (A + B\tau)s,$$

which is a \mathbb{Z} -linear combination of the standard basis elements. Uniqueness is easy and follows from the fact that every element in \mathbb{Z}_K has a unique representation in terms of $1, \tau$. ■

7.2 Ideal Norms

Remark 7.2.1: In the previous section, we used the fact that for $a \in \mathbb{Z}_K$, the number of elements in $\mathbb{Z}_K / \langle n \rangle$ is $|Na|$. That will be a consequence of the theory we develop here.

Definition 7.2.2 (Norm of an ideal)

If $I \trianglelefteq \mathbb{Z}_K$ is a nonzero ideal, define the **norm of I** as $N(I) = |\mathbb{Z}_K / I|$.

Remark 7.2.3: It's not completely obvious, but this quotient is always finite. We can use the fact that $I \leq \mathbb{Z}_K$ is a \mathbb{Z} -submodule of rank exactly 2. It's then a general fact from algebra that A/B is finite when $\text{rank}(A) = \text{rank}(B)$, and there are ways of figuring out the number of elements (see normal forms).

Proposition 7.2.4 (*Norms can be computed in terms of a basis with respect to τ*).

Suppose that $I \trianglelefteq \mathbb{Z}_K$ is a nonzero ideal and let $n, A + B\tau$ be a standard basis for I . Then $N(I) = nB \in \mathbb{Z}^+$.

Proof (of proposition).

Check that $\{a + b\tau \mid 0 \leq a \leq n, 0 \leq b \leq B\}$ is a complete and irredundant set of representatives for \mathbb{Z}_K / I . ■

Remark 7.2.5: So given a standard basis, it's easy to compute norms! What does this have to do with the previous notion of norms for elements?

Theorem 7.2.6 (*The ideal that the norm generates*).

Let $I \trianglelefteq \mathbb{Z}_K$ be nonzero and define $\bar{I} = \{\bar{\alpha} \mid \alpha \in I\} \trianglelefteq \mathbb{Z}_K$. Then $I\bar{I} = \langle N(I) \rangle$.

Lemma 7.2.7 (*The τ coefficient divides the remaining coefficient*).

Let n be as above and let $A + B\tau$ be a standard basis for I . Then $B \mid n$ and $B \mid A$.

Proof (of lemma).

Recall that B was a generator for τ components of elements of I , so we just need to find an

element of I with τ component n , and $n\tau \in I$ works. Now compute $(A + B\tau)\tau \in I$. This is equal to

$$A\tau + B\tau^2.$$

Note that this could in principle be done in cases: if $\tau = \sqrt{d}$, the quantity Bd would be an integer and A would be the τ coordinate. Then since B divides every τ coefficient, we'd be done. But let's try this in a more unified way: we know τ is a root of a monic degree 2 polynomial, namely $(x - \tau)(x - \bar{\tau}) = x^2 - \text{Tr}(\tau)x + N(\tau)$, and thus we can write

$$\tau^2 = \text{Tr}(\tau)\tau - N(\tau).$$

Substituting yields

$$\begin{aligned} (A + B\tau)\tau &= A\tau + B\tau^2 \\ &= A\tau + B(\text{Tr}(\tau)\tau - N(\tau)) \\ &= -BN(\tau) + (A + B\text{Tr}(\tau))\tau. \end{aligned}$$

The coefficient of τ must be a multiple of B , which forces $B \mid A$. ■

Proof (of theorem).

Let $n, A + B\tau$ be a standard basis for I . Then $I = \langle n, A + B\tau \rangle$, which is a generating set as a \mathbb{Z}_K -module since they generate I over \mathbb{Z} and subset containment both ways can be readily checked. We can then write $\bar{I} = \langle n, A + B\bar{\tau} \rangle$, since conjugating ordinary integers doesn't change them. Using the lemma, we can write

$$\begin{aligned} I &= \langle Bn', BA' + B\tau \rangle \\ \bar{I} &= \langle Bn', BA' + B\bar{\tau} \rangle. \end{aligned}$$

We can factor out a B to get

$$\begin{aligned} I &= \langle B \rangle \langle n', A' + \tau \rangle \\ \bar{I} &= \langle B \rangle \langle n', A' + \bar{\tau} \rangle. \end{aligned}$$

Now multiplying the two yields

$$I\bar{I} = \langle B^2 \rangle \langle (n')^2, n'(A' + \bar{\tau}), n'(A' + \tau), N(A' + \tau) \rangle.$$

It's tempting to factor out n' , but it isn't obviously in the last factor. But it is! Note that $N(A' + \tau) \in \langle A' + \tau, n' \rangle$ and thus $BN(A' + \tau) \in \langle B \rangle \langle A' + \tau, n' \rangle = I$. But the first expression is an ordinary integer, i.e. in $I \cap \mathbb{Z} = \langle n \rangle$ and thus a multiple of n . So $Bn' = n \mid BN(A' + \tau)$, and thus $n' \mid N(A' + \tau)$. So we can rewrite

$$\begin{aligned} I\bar{I} &= \langle B^2 \rangle \langle n' \rangle \left\langle n', A' + \bar{\tau}, A' + \tau, \frac{N(A' + \tau)}{n'} \right\rangle \\ &= \langle B^2 n' \rangle \left\langle n', A' + \bar{\tau}, A' + \tau, \frac{N(A' + \tau)}{n'} \right\rangle. \end{aligned}$$

We can now note that $B^2 n' = B^2(n/B) = nB = N(I)$. We've thus shown that

$$I\bar{I} = \langle N(I) \rangle \left\langle n', A' + \bar{\tau}, A' + \tau, \frac{N(A' + \tau)}{n'} \right\rangle.$$

We'd really like the second term to just be $\langle 1 \rangle$. Note that this factor contains some integers: $n', N(A' + \tau)/n'$, and $(A' + \bar{\tau}) + (A' + \tau) = \text{Tr}(A' + \tau)$. So let

$$J := \langle n, N(A' + \tau)/n', \text{Tr}(A' + \tau) \rangle \subseteq \mathbb{Z},$$

then it's enough to show $J = \langle 1 \rangle \subseteq \mathbb{Z}$. Why? If so, 1 is a \mathbb{Z} -linear combination of these elements, but every \mathbb{Z} -linear combination is also a \mathbb{Z}_K -linear combination. Every such combination will be in the original ideal appearing in $I\bar{I}$, which we want to show is the unit ideal. We can write $J = d\mathbb{Z}$ where $d \in \mathbb{Z}^+$ and suppose toward a contradiction that $d > 1$.

Consider $\alpha := (A' + \tau)/d \in K$. Taking the trace is \mathbb{Q} -linear, so $\text{Tr}(\alpha) = (1/d) \text{Tr}(A' + \tau) \in \mathbb{Z}$. This follows because the trace $\text{Tr}(A' + \tau)$ is in J , thus a multiple of d . We can also compute $N\alpha = N(A' + \tau)/d^2$ using that $d\bar{d} = d^2$ since d is rational.

The claim is that $N\alpha$ is also an integer: since $N(A' + \tau)/n', \text{Tr}(A' + \tau)$ are in J , d divides both. So we know that $d^2 \mid (n')(N(A' + \tau)/n') = N(A' + \tau)$, which forces $N\alpha \in \mathbb{Z}$. So we know $N\alpha, \text{Tr} \alpha \in \mathbb{Z}$, which forces $\alpha \in \mathbb{Z}_K$ since α is a root of $x^2 - \text{Tr}(\alpha)x + N\alpha$. But α can't be in \mathbb{Z}_K , since these consist only of \mathbb{Z} -linear combinations of $1, \tau$ – however here the coefficient of τ is $1/d \notin \mathbb{Z}$, and thus $\alpha = A'/d + (1/d)\tau \notin \mathbb{Z}_K$. ■

Remark 7.2.8: This is a long proof! It's nice in that it's direct, but less nice in that it required some clever steps. When we do the case for general number fields, we'll be able to use a more conceptual approach that avoids some of these computations. Many other facts fall out of these theorem – in fact, there are nice results as long as $I\bar{I}$ is a principal ideal. ✍

8 | Fundamental Theorem of Ideal Theory (Lec. 7, Thursday, February 04)

8.1 Norms: Multiplicativity and Computations

Remark 8.1.1: Today: roughly chapter 6. Goal: establish unique factorization of ideals for quadratic fields. Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field and we let

$$\tau = \begin{cases} \sqrt{d} & d \equiv 2, 3 \pmod{4} \\ \frac{1 + \sqrt{d}}{2} & d \equiv 1 \pmod{4}. \end{cases}$$

In this case we saw that $\mathbb{Z}_K = \mathbb{Z} + \mathbb{Z}\tau = \mathbb{Z}[\tau]$. We defined the norm of a nonzero ideal $I \subseteq \mathbb{Z}_K$ by $N(I) = |\mathbb{Z}_K/I|$. The main theorem was that $I\bar{I} = \langle N(I) \rangle$, so the two definitions of norms are closely related. Some corollaries of this theorem:

Corollary 8.1.2 (The norm is multiplicative).

Let $I, J \subseteq \mathbb{Z}_K$ be nonzero, then $N(IJ) = N(I)N(J)$.

Proof (of corollary).

Note that $IJ\bar{I}\bar{J} = \langle N(IJ) \rangle$ on one hand, and on the other hand we can write this as

$$IJ\bar{I}\bar{J} = I\bar{I}J\bar{J} = \langle N(I) \rangle \langle N(J) \rangle = \langle N(I)N(J) \rangle.$$

So we know that $\langle N(IJ) \rangle = \langle N(I)N(J) \rangle$ in \mathbb{Z}_K , how can we conclude that the generators are the same? In a domain, they are the same up to a unit, so

$$\frac{N(IJ)}{N(I)N(J)} \in U(\mathbb{Z}_K),$$

and thus this quotient is in $\mathbb{Z}_K \cap \mathbb{Q} = \mathbb{Z}$. The same argument shows that its reciprocal is also in \mathbb{Z} , so the ratio must be a unit in \mathbb{Z} and we have $N(IJ) = \pm N(I)N(J)$. But the norm counts something, so both sides must be positive. ■

Remark 8.1.3: Note that if we knew I, J were comaximal, we could appeal to the Chinese Remainder Theorem, but we don't need any assumptions on the ideals for this proof.

Corollary 8.1.4 (Computing norms of principal ideals).

Let $\alpha \in \mathbb{Z}_K \setminus \{0\}$, then

$$N(\langle \alpha \rangle) = |N(\alpha)| = |\alpha\bar{\alpha}|.$$

Proof (of corollary).

We have

$$\begin{aligned} \langle N(\langle \alpha \rangle) \rangle \langle \alpha \rangle \langle \bar{\alpha} \rangle &= \langle \alpha \rangle \langle \bar{\alpha} \rangle \\ &= \langle \alpha\bar{\alpha} \rangle \\ &= \langle N\alpha \rangle. \end{aligned}$$

By the same argument as the previous corollary, this can only be true if the generators are the same up to sign, so $N(\langle \alpha \rangle) = \pm N\alpha$.

8.2 Unique Factorization for Ideals

Lemma 8.2.1 (Principal Multiple Lemma).

Let $I \subseteq \mathbb{Z}_K \setminus \{0\}$, then there is another ideal $\tilde{I} \subseteq \mathbb{Z}_K \setminus \{0\}$ such that $I\tilde{I}$ is principal.

Proof (of Principal Multiple Lemma).

Take $\tilde{I} := \bar{I}$, since we proved that this is principal and generated by the norm. ■

Remark 8.2.2: Why write this down when it's weaker than the previous theorem? In the next proofs, we'll only really use that I times something is principal.

Lemma 8.2.3 (Cancellation in the Monoid of Ideals).

Suppose that $IJ = IJ'$ is an equation of nonzero ideals in \mathbb{Z}_K with I principal. Then $J = J'$, so principal ideals can be cancelled from both sides.

Definition 8.2.4 (Dilation of Ideals)

If $I \subseteq \mathbb{Z}_K$, for any $\alpha \in K$ define

$$\alpha I := \{ \alpha \beta \mid \beta \in I \},$$

i.e. scale or dilate the ideal I by the factor α . We'll refer to this as the **dilation of I by α** .

Remark 8.2.5: Is this still an ideal in \mathbb{Z}_K ? It still contains zero, is still closed under addition, and still absorbs multiplication by elements in O_K – however, it may not be a subset of \mathbb{Z}_K , since we can dilate by any element in K . For example, for $I := 2\mathbb{Z}$ take $\alpha := 1/5$. These are referred to as **fractional ideal**, i.e. a \mathbb{Z}_K -submodule of K . It is an ideal in \mathbb{Z}_K when it is contained in \mathbb{Z}_K .

Proof (of cancellation in the monoid of ideals).

Write $I = \langle \alpha \rangle$. Then $\langle \alpha \rangle J = \langle \alpha \rangle J'$, however the RHS is equal to the dilated ideal $\alpha J'$ and the LHS is αJ . So dilate both sides by $1/\alpha$ to get $J = J'$. ■

Remark 8.2.6: This was the easy case, when I was principal. What if I is not principal?

Proposition 8.2.7 (The monoid $\text{Id}(\mathbb{Z}_K)$ is Cancellative).

If $IJ = IJ'$ then $J = J'$, with no assumptions on I .

Proof (?).

Choose \tilde{I} using the previous lemma and multiply it to both sides to obtain

$$(I\tilde{I})J = (I\tilde{I})J'.$$

Then since $I\tilde{I}$ is principal, it can be cancelled using the previous lemma. ■

8.2.1 Proving Unique Factorization

Theorem 8.2.8 (To divide is to contain).

Let I, J be nonzero ideals of \mathbb{Z}_K , then

$$I \mid J \iff I \supseteq J.$$

Proof (of theorem).

\implies : This is true in any ring! If $I \mid J$, then $J = IM$ where $M \trianglelefteq \mathbb{Z}_K$, and by definition $IM \subseteq I$ and so $J \subseteq I$.

\impliedby : Suppose $I \supseteq J$, we then want to find $B \trianglelefteq \mathbb{Z}_K$ with $J = IB$. We'll proceed by pretending we had such a B and seeing what it must be! If B satisfies this equation, pick \tilde{I} where $I\tilde{I} = \langle \alpha \rangle$, then

$$\tilde{I}J = \tilde{I}IB = \langle \alpha \rangle B = \alpha B.$$

From here we can solve for B by dilating by $1/\alpha$, so $B = \alpha^{-1}(\tilde{I}J)$. If we make this definition, does it work?

First, do we have $B \subseteq \mathbb{Z}_K$? This amounts to check that $\tilde{I}J \subseteq \langle \alpha \rangle$. This is true, using the assumption $J \subseteq I$, since $\tilde{I}J \subseteq \tilde{I}I = \langle \alpha \rangle$. So B is not a fractional ideal, and is an honest ideal of \mathbb{Z}_K . We can also check that

$$\begin{aligned} IB &= I(\alpha^{-1}\tilde{I}J) \\ &= \alpha^{-1}(I\tilde{I}J) \\ &= \alpha^{-1}(\langle \alpha \rangle J) \\ &= \alpha^{-1}(\alpha J) \\ &= J, \end{aligned}$$

using that dilation commutes with ideal multiplication. ■

Remark 8.2.9: We now want to prove that $\text{Id}(\mathbb{Z}_K)$ is a UFM. If it's cancellative, we just need to check factorization into irreducibles and that irreducibles are prime, i.e. the analog of Euclid's

lemma.

Remark 8.2.10: We'll use the fact that $\text{Id}(\mathbb{Z}_K)$ is a *reduced* monoid, i.e. the only unit is the identity $\langle 1 \rangle$, the entire ring. This follows from the fact that the product of ideals is contained in both factors, so each factor would contain 1 and thus be the entire ring. We'll proceed in two steps:

Proposition 8.2.11 (Unique Factorization).

1. Every element of $\text{Id}(\mathbb{Z}_K)$ factors into irreducibles in $\text{Id}(\mathbb{Z}_K)$, and
2. (Euclid's Lemma) Irreducibles in $\text{Id}(\mathbb{Z}_K)$ are prime.

Remark 8.2.12: We'll use the fact that it's reduced to avoid having to say "non-unit element" in (1), since we have only one unit and we'll think of it as the empty product.

How do you prove (1)? The same way you prove it for the integers: suppose you have a smallest counterexample. That can't be prime, since a product of 1 prime is an allowable factorization, so this factors into a product of two smaller things which necessarily can *not* be counterexamples by minimality. So the smaller factors break up into primes – but then so does their product, the original counterexample, contradiction. The tricky part here is choosing what "smaller" should mean.

Proof (of 1).

If not, choose I of smallest norm where I has no such factorization. Then $I \neq \langle 1 \rangle$ since by convention this does factor as the product of zero irreducibles, and I is not irreducible since irreducibles count as their own factorization. So we can factor $I = AB$ with $A, B \neq \langle 1 \rangle$. Taking norms yields

$$N(I) = N(AB) = N(A)N(B).$$

We'd like the norms of A, B to be smaller, since then we could apply the inductive hypothesis. The only obstruction to this would be if $N(A) = 1$ and $N(B) = N(I)$. But having norm 1 means that $A = \langle 1 \rangle$, since this means the quotient has one element, forcing it to be the zero ring. So everything in the ring is zero mod the ideal, i.e. in the ideal. So $1 < N(A), N(B) < N(I)$. Since I was the smallest counterexample, both A and B can be factored into irreducibles, but then concatenating the two factorizations yields a factorization for AB . \nexists

■

Proof (of 2: Euclid's Lemma).

Suppose P is irreducible in $\text{Id}(\mathbb{Z}_K)$ and suppose $P \mid IJ$, we want to show P divides one of these two. Suppose $P \nmid I$, then P does not contain I and $P + I \supsetneq P$. This means that $P + I$ is a *proper divisor* of P , i.e. it divides P but is not equal to P . But P was irreducible, so $P + I$ is a unit, which forces $P + I = \langle 1 \rangle$. Multiplying by J yields $PJ + IJ = J$. We said that

$P \mid IJ$ by assumption, so $IJ = PA$ for some nonzero ideal A . So

$$\begin{aligned} J &= PJ + IJ \\ &= PJ + PA \\ &= P(J + A), \end{aligned}$$

which shows that $P \mid J$. ■

Remark 8.2.13: Now running the exact same proof as for \mathbb{Z} yields unique factorization. ✍

Exercise 8.2.14 (?)

Let P be a nonzero ideal of $\text{Id}(\mathbb{Z}_K)$, then P is monoidally prime in $\text{Id}(\mathbb{Z}_K)$ if and only if P is prime in the usual sense of prime ideals.

Hint: use “to divide is to contain”.

8.3 Preview: Ramification

Remark 8.3.1: This chapter is about understanding prime ideals in quadratic number rings, i.e. \mathbb{Z}_K for quadratic fields. What are the building blocks of the nonzero prime ideals? ✍

Definition 8.3.2 (Prime ideal above a prime number)

Let P be a nonzero prime ideal, then P **lies above** the rational prime p if and only if $P \supseteq \langle p \rangle$. Equivalently, $p \in P$, or $P \mid \langle p \rangle$.

Theorem 8.3.3 (*Lying above unique primes*).

Every nonzero prime ideal of \mathbb{Z}_K lies above a unique rational prime p .

Proof (of theorem).

Consider $P \cap \mathbb{Z} \trianglelefteq \mathbb{Z}$. Tracing through the definitions, if P is a prime ideal in \mathbb{Z}_K , then this intersection is also prime in \mathbb{Z} . Moreover $P \cap \mathbb{Z} \neq \{0\}$, since we can take any nonzero element $\alpha \in P$, then $0 \neq \alpha\bar{\alpha} \in \mathbb{Z}$ and since P absorbs multiplication, this is still in P . The nonzero prime ideals of \mathbb{Z} are of the form $n\mathbb{Z}$ with n prime, so $P \cap \mathbb{Z} = p\mathbb{Z}$ for some prime p . But then $p \in P$ and P lies above p . Why is this unique? If P lies above q , we would have $q \in P \cap \mathbb{Z} = p\mathbb{Z}$ and thus $p \mid q$. But since these are both primes, $p = q$. ■

Remark 8.3.4: If we want to figure out all of the prime ideals P of \mathbb{Z}_K , we should see how $\langle p \rangle$ factors, since each P shows up as a factor of some $\langle p \rangle$. Thus the major question will be: given p , how does $\langle p \rangle$ factor into prime ideals in \mathbb{Z}_K ? ✍

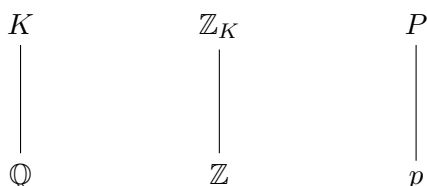
9 | Prime Ideals of \mathbb{Z}_K (Lec. 8, Tuesday, February 09)

9.1 Dedekind-Kummer Mirroring

Remark 9.1.1: Today: chapter 7. Let K be a quadratic number field. Recall that if $P \leq \mathbb{Z}_K$ is a prime then P lies above $p \in \mathbb{Z}$ if $P \supseteq \langle p \rangle$. Equivalently,

- P contains p , or
- $P \mid \langle p \rangle$

Last time we saw that every P lies above a unique p . The following diagram illustrates the situation:



[Link to Diagram](#)

If we want to determine all of the primes P , we should consider factoring all of the ideals $\langle p \rangle$ into prime ideals of \mathbb{Z}_K . We have unique factorization for prime ideals, so we can write $\langle p \rangle = P_1 \cdots P_g$. Taking norms yields

$$N(\langle p \rangle) = \prod N(P_i),$$

where we can identify the LHS as p^2 , since the norm for principal ideals is the square of the generating element. Alternatively, we can check the size of $\mathbb{Z}_K / \langle p \rangle$. Note that \mathbb{Z}_K is a free \mathbb{Z} -module on 2 generators, and we take both coordinates mod p to get $(\mathbb{Z}/p\mathbb{Z})^2$. Since none of the terms on the RHS are the unit ideal, none have norm 1, and we make the following definition based on the possible cases:

Definition 9.1.2 (Inert, Split, and Ramified Primes)

- $g = 1$ and $P_1 = \langle p \rangle$ and $\langle p \rangle$ is prime. In this case we say p is **inert**.
- If $g = 2$ and $P_1 \neq P_2$, then we say p is **split**.
- If $g = 2$ and $P_1 = P_2$ then we say p is **ramified**.

Let $K = \mathbb{Q}(\sqrt{d})$ and τ as usual. We can compute its minimal polynomial:

$$\min_{\tau}(x) = \begin{cases} x^2 - d & d \equiv 2, 3 \pmod{4} \\ x^2 - x + \left(\frac{1-d}{4}\right) & d \equiv 1 \pmod{4}. \end{cases}$$

Theorem 9.1.3 (Dedekind-Kummer, Prime Factorization Mirroring Theorem).

Let $p \in \mathbb{Z}$ be prime. Then the factorization of $\langle p \rangle$ into prime ideals in \mathbb{Z}_K mirrors the factorization of $\min_{\tau}(x)$ into irreducibles mod p , i.e. in $\mathbb{F}_p[x]$. If $\min_{\tau}(x)$ is irreducible, then p is inert. Otherwise,

$$\min_{\tau}(x) \equiv (x - a)(x - b) \pmod{p}$$

for some $a, b \in \mathbb{Z}$, since this is a monic quadratic. In this case $\langle p \rangle = P_1 P_2$ where

- $P_1 := \langle p, \tau - a \rangle$,
- $P_2 := \langle p, \tau - b \rangle$,

and both ideals have norm p . Finally, $P_1 = P_2 \iff a \equiv b \pmod{p}$.

Example 9.1.4 (of inert, split, and ramified cases): Let $K = \mathbb{Q}(\sqrt{5})$, then $\tau = \sqrt{-5}$ and $\min_{\tau}(x) = x^2 + 5$. We can check how this factors modulo small primes

$$x^2 + 5 = (x + 1)^2 \in \mathbb{F}_2[x],$$

and we're in the ramified case. In this case,

$$\langle 2 \rangle = \langle 2, \sqrt{-5} - 1 \rangle^2.$$

We also have

$$x^2 + 5 \equiv (x - 1)(x + 1) \in \mathbb{F}_3[x],$$

which is the split case, so

$$\langle 3 \rangle = \langle 3, \sqrt{-5} - 1 \rangle \langle 3, \sqrt{-5} + 1 \rangle.$$

Taken mod 5, we have

$$x^2 + 5 \equiv x^2 \in \mathbb{F}_5[x],$$

so

$$\langle 5 \rangle = \langle 5, \sqrt{-5} \rangle^2 = \langle \sqrt{-5} \rangle^2.$$

Similarly,

$$x^2 + 5 \text{ is irreducible } \in \mathbb{F}_{11}[x],$$

so $\langle 11 \rangle$ is inert.

Lemma 9.1.5 (Characterization of \mathbb{Z}_K as a quotient of a polynomial ring).

There is a surjective morphism

$$\begin{aligned}\mathbb{Z}[x] &\rightarrow \mathbb{Z}_K = \mathbb{Z}[\tau] \\ f(\alpha) &\mapsto f(\tau),\end{aligned}$$

so by the first isomorphism theorem,

$$\mathbb{Z}[x] / \langle \min_{\tau}(x) \rangle \cong \mathbb{Z}_K.$$

Proof (of Dedekind-Kummer mirroring).

Note that $\mathbb{Z}_K / \langle p \rangle = \mathbb{Z}[\tau] / \langle p \rangle$, and using the lemma, this is isomorphic to $\mathbb{Z}[x] / \langle \min_{\tau}(x), p \rangle \cong \mathbb{F}_p[x] / \langle \min_{\tau}(x) \pmod{p} \rangle$. In this case, if \min_{τ} is irreducible mod p , then the quotient is a field. Why? The numerator is a polynomial ring over a field and the denominator is generated by an irreducible, and a PID mod an irreducible is always a field. Thus $\langle p \rangle$ must be a maximal ideal by considering the first expression above, and maximals are prime here, so p is inert. Now suppose it's not irreducible, so

$$\min_{\tau}(x) = (x - a)(x - b) \pmod{p}.$$

Define P_1, P_2 as in the theorem. Why are these of norm p ? Consider

$$\begin{aligned}\mathbb{Z}_K / P_1 &\cong \frac{\mathbb{Z}[x] / \langle \min_{\tau}(x) \rangle}{\langle p, x - a \rangle} \\ &\cong \mathbb{Z} / p\mathbb{Z}[x] / \langle \min_{\tau}(x), x - a \rangle \\ &\cong \mathbb{Z} / p\mathbb{Z}[x] / \langle \min_{\tau}(x), x - a \rangle \\ &\cong \mathbb{Z} / p\mathbb{Z}[x] / \langle x - a \rangle && \text{since } x - a \mid \min_{\tau}(x) \\ &\cong \mathbb{Z} / p\mathbb{Z}.\end{aligned}$$

So P_1 is maximal and thus prime, and moreover $N(P_1) = p$ since there are p elements in $\mathbb{Z} / p\mathbb{Z}$. The same argument works for P_2 . Now multiplying them yields

$$P_1 P_2 = \langle p, p(\tau - a), p(\tau - b), (\tau - a)(\tau - b) \rangle.$$

Note that

$$\begin{aligned}\min_{\tau}(x) &\equiv (x - a)(x - b) \pmod{p} \\ \implies \min_{\tau}(x) &= (x - a)(x - b) + pG(x)\end{aligned}$$

for some $G \in \mathbb{Z}[x]$. Plugging in τ , the LHS is zero, while on the RHS yields $\dots + pG(\tau)$. This last term is pr for some $r \in R$, which is zero mod $p \in \mathbb{Z}[\tau] = \mathbb{Z}_K$. So p now divides every term in the generating set above, and since to contain is to divide, we have $P_1 P_2 \subseteq \langle p \rangle$ and $\langle p \rangle \mid P_1 P_2$. Write $P_1 P_2 = \langle p \rangle I$ for some ideal I , taking norms yields

$$N(P_1)N(P_2) = N(\langle p \rangle)N(I).$$

The LHS is p^2 as shown above, and the RHS is $p^2 N(I)$ which forces $N(I) = 1 \iff I = \langle 1 \rangle = \mathbb{Z}_K$ (the entire ring)

We now want to show $P_1 = P_2 \iff a \equiv b \pmod{p}$. The reverse direction is clear, since generators in P_1, P_2 can be adjusted by p without changing the ideal. Conversely, suppose $P_1 = P_2$. Then P_1 contains $\tau - a, \tau - b$, and thus their difference $a - b = (\tau - b) - (\tau - a) \in P_1$. Moreover $p \in P_1$, and so P_1 contains the \mathbb{Z} ideals generated by p and $a - b$ and thus $\gcd(p, a - b)$. If $a \not\equiv b \pmod{p}$, this greatest common divisor must be 1, forcing $1 \in P_1$. This is a contradiction since P_1 is prime and thus can't be the unit ideal, so $a \equiv b \pmod{p}$. ■

Question 9.1.6

Can we be more explicit about how \min_{τ} factors?

Proposition 9.1.7 (Characterization of inert/split/ramified primes).

Let p be an odd prime, then

- p is inert $\iff d$ is not a square \pmod{p} ,
- p splits $\iff d$ is a nonzero square \pmod{p} ,
- p ramifies $\iff d \equiv 0 \pmod{p}$.

Proposition 9.1.8 (Inert/Split/Ramified primes for quadratic fields).

- $d \equiv 5 \pmod{8} \implies 2$ is inert.
- $d \equiv 1 \pmod{8} \implies 2$ is split.
- $d \equiv 2, 3 \pmod{4} \implies 2$ is ramified.

Remark 9.1.9: The proof follows from looking at how $\min_{\tau}(x)$ factors $\pmod{2}$, and there aren't many possibilities.

9.2 Units in \mathbb{Z}_K

Remark 9.2.1: Roughly chapter 8. For the imaginary quadratic case, we can write down the unit group explicitly.

Proposition 9.2.2 (Imaginary quadratic fields have at most 6 units).

If $d < 0$ (i.e. the imaginary quadratic case) then $|U(\mathbb{Z}_J)| \leq 6$.

Remark 9.2.3: “Usually” $U(\mathbb{Z}_K) = \{\pm 1\}$. Here “usually” means there are only two exceptions:

- For $\mathbb{Q}(\sqrt{-1})$ then the units are $\{\pm 1, \pm i\}$.

- For $d = -3$, there were 6 units.

In every other case, there are only two.

Proposition 9.2.4 (Existence of the fundamental unit).

Suppose $d > 0$, then there is a unit $\epsilon_0 > 1 \in \mathbb{Z}_K$ such that $U(\mathbb{Z}_K) = \{\pm \epsilon_0^k \mid k \in \mathbb{Z}\}$. Moreover ϵ_0 is unique, and we'll refer to this as the **fundamental unit**.

Corollary 9.2.5 (The unit group is infinite for real quadratic fields).

When $d > 0$, $U(\mathbb{Z}_K)$ is infinite and in fact isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}$.

Remark 9.2.6: Here the $\mathbb{Z}/2\mathbb{Z}$ corresponds to the \pm and the \mathbb{Z} to the exponent.

Example 9.2.7 (of the fundamental unit):

- For $d = 2$, we have $\epsilon_0 = 1 + \sqrt{2}$. This is a unit because it has inverse $\sqrt{2} - 1$.
- For $d = 43$, it turns out that $\epsilon_0 = 531\sqrt{43}$.

Lemma 9.2.8 (Computation of norm of the fundamental unit).

Let $\epsilon \in \mathbb{Z}_K$, then $\epsilon \in U(\mathbb{Z}_K) \iff N(\epsilon) = \pm 1$.

Remark 9.2.9: Note that norms were positive in the imaginary quadratic case, but can be negative for real quadratics.

Proof (of computation of norm).

\Leftarrow : This means $\epsilon\bar{\epsilon} = \pm 1$, so one of $\pm\bar{\epsilon}$ is the inverse.

\Rightarrow : Write $\epsilon\epsilon^{-1} = 1$ and take norms of both sides.

■

Remark 9.2.10: Our strategy: show that the group of positive units $U(\mathbb{Z}_K)^+$ is infinite cyclic. If we get a generator $\epsilon_0 > 1$, replace it with its reciprocal, and note that we don't want $\epsilon_0 = 1$ since this wouldn't yield an infinite group. If we can generate all of the positive units, all of the negative units are negatives of positive units. How we'll do this: we'll look at the map

$$\log : \mathbb{G}_m(\mathbb{R}^+) \rightarrow \mathbb{G}_a(\mathbb{R}).$$

and consider the image $\log(U(\mathbb{Z}_K)^+)$, which will be an infinite cyclic subgroup of $\mathbb{G}_a(\mathbb{R})$.

Proposition 9.2.11 (The log subgroup is discrete).

The subgroup $\log(U(\mathbb{Z}_K)^+)$ is discrete, i.e. it has finite intersection with $[-X, X] \subseteq \mathbb{R}$ for every $X > 0$.

Proof (of proposition).

It's enough to show finite intersection with $[0, X]$ for all $X > 0$. Why? Any subgroup $H \leq \mathbb{G}_a(\mathbb{R})$ is symmetric about 0, i.e. $a \in H \iff -a \in H$, and so having finite intersection

with the positive interval implies finite intersection with both. So let $\epsilon \in U(\mathbb{Z}_K)^+$ with $\log(\epsilon) \in [0, X]$, we'll show there are only finitely many choices for ϵ , since every $\log(\epsilon)$ correspond to a point in the intersection.

Claim: Write $\epsilon = u + v\sqrt{d}$ with $u, v \in \mathbb{Z}$ or $\frac{1}{2}\mathbb{Z}$, then $u, v \geq 0$.

If we have this, we're done since $\log(u + v\sqrt{d}) \leq X$. Exponentiating yields $u + v\sqrt{d} \leq e^X$, and so we must have $u, v \leq e^X$. But there are only finitely many possibilities, since these are integers or half-integers.

Proof (of claim).

We have $\epsilon \geq 1$ since $u, v \geq 0$. There are now two cases:

1. $N(\epsilon) = 1$. In this case, $\epsilon\bar{\epsilon} = 1$ and so $\epsilon^{-1}\epsilon$. We can write $u = (1/2)(\epsilon + \bar{\epsilon}) = (1/2)(\epsilon + \epsilon^{-1}) > 0$. Similarly,

$$v = (\epsilon - \bar{\epsilon})/2\sqrt{d} = (\epsilon - \epsilon^{-1})/2\sqrt{d} \geq 0.$$

2. $N(\epsilon) = -1$. This case proceed similarly.

■

This completes the proof.

■

Question 9.2.12

What do the discrete subgroups of $\mathbb{G}_a(\mathbb{R})$ look like?

Answer 9.2.13

Some examples are $\{0\}$, \mathbb{Z} , $\lambda\mathbb{Z}$ for $\lambda \in \mathbb{R}$, etc. It turns out that these are the only ones. Knowing that these must be the image of the log map, if we're in the $\alpha\mathbb{Z}$ case we're fine because this is infinite cyclic, but the case $\{0\}$ is an issue: this would mean that the only positive unit is $e^0 = 1$, and the only units are ± 1 . So we just need to show that there are units other than ± 1 .

10 | Units in \mathbb{Z}_K (Lec. 9, Monday, February 15)

10.1 Review

Remark 10.1.1: Today: chapter 8. We'll continue with the statements from last time:



Proposition 10.1.2 (*Subgroups of \mathbb{R} are either discrete or infinite cyclic*).

A discrete subgroup $\Lambda \leq \mathbb{R}$ is either 0 or infinite cyclic, where *discrete* means having finite intersection with every interval $[-x, x]$.

Proof (of proposition).

Suppose $\Lambda \neq 0$, then we can choose a smallest positive element $\alpha \in \Lambda$. Why does this exist? There are only finitely many elements in $[0, \alpha]$, so there is a smallest, and we could replace α with it. The claim is that $\Lambda = \mathbb{Z}\alpha$. The reverse containment is clear because the RHS is necessarily a subgroup. Toward a contradiction, suppose there is some $\beta \in \Lambda \setminus \mathbb{Z}\alpha$ with $n\alpha < \beta < (n+1)\alpha$ for some $n \in \mathbb{Z}$. This can't happen: subtracting n from both sides yields

$$0 < \beta - n\alpha < \alpha,$$

where the middle term is necessarily in Λ , contradicting minimality of α .



Remark 10.1.3: Recall that to show the theorem we wanted, it was enough to show $\log U(\mathbb{Z}_K)^+$ is an infinite cyclic subgroup of $\mathbb{G}_a(\mathbb{R})$. We proved that this was a discrete subgroup. If this were just the zero element, the only possible units would be ± 1 , so it suffices to find a unit $\epsilon \in U(\mathbb{Z}_K)$ with $\epsilon > 0$ and $\epsilon \neq 1$.

10.2 An Aside: Diophantine approximation

Remark 10.2.1: Let $\alpha \in \mathbb{R}$ and let $Q \in \mathbb{Z}^+$. How well can we approximate α with a fraction with denominator bounded by Q ?

Theorem 10.2.2 (*Dirichlet's Approximation Theorem*).

There is a $q \leq Q \in \mathbb{Z}^+$ with

$$\|q\alpha\| \leq \frac{1}{Q+1},$$

where $\|\cdot\|$ denotes the distance to the nearest integer.

Remark 10.2.3: The way to think about this inequality: if the LHS is close to an integer p , then α is close to p/q .

Proof (of Dirichlet's theorem).

Chop the interval into $Q + 1$ pieces, and think of the inequality as a condition on the fractional part of α , denoted $\{qa\} := qa - \lfloor qa \rfloor \in [0, 1)$. Note that if $\{qa\} \in [0, 1/Q + 1)$ or $[Q/Q + 1, Q)$ for some q , then we are done. If not, it must land in one of the $q - 1$ middle intervals

$$[1/Q + 1, 2/Q + 1), [2/Q + 1, 3/Q + 1), \dots, [Q - 1/Q + 1, Q/Q + 1)$$

for all $q \leq Q$. But we have Q choices for q and only $Q - 1$ intervals, so there are two values of q with fractional part in the same interval. So choose these, say $q_1 < q_2 \leq Q$, and consider $q := q_2 - q_1$. Since $\{q_1\alpha\}, \{q_2\alpha\}$ are in the same interval, we have $\{q\alpha\} \in [0, 1/Q + 1)$, putting it close to an integer. ■

Corollary 10.2.4 (Infinitude of elements of bounded norm).

There are infinitely many pairs of positive integers (p, q) such that

$$|p^2 - dq^2| \leq 1 + 2\sqrt{d},$$

where d was the squarefree integer for which $K = \mathbb{Q}(\sqrt{d})$.

Remark 10.2.5: Note that the RHS does not depend on p or q , and only depends on the field. Moreover, this proof is also true with the 1 removed. ✍

Proof (of corollary).

Using Dirichlet's approximation theorem, choose $Q \in \mathbb{Z}^+$ and $1 \leq q \leq Q$ such that

$$\|q\sqrt{d}\| \leq \frac{1}{Q+1},$$

then there is a $p \in \mathbb{Z}$ such that

$$|p - q\sqrt{d}| \leq \frac{1}{Q+1}.$$

We know q is positive by Dirichlet's theorem, and p is positive since $q\sqrt{d} \geq \sqrt{d} \geq 1$, and the distance from p to q is at most $1/2$. We can now check

$$\begin{aligned} |p^2 - dq^2| &= |p - q\sqrt{d}| |p + q\sqrt{d}| \\ &= |p - q\sqrt{d}| |(p - q\sqrt{d}) + 2q\sqrt{d}| \\ &\leq |p - q\sqrt{d}| |p - q\sqrt{d}| + |2q\sqrt{d}| \\ &\leq \frac{1}{Q+1} \left(\frac{1}{Q+1} + 2Q\sqrt{d} \right) \\ &= \left(\frac{1}{Q+1} \right)^2 + \frac{2Q}{Q+1} \sqrt{d} \\ &< 1 + 2\sqrt{d}, \end{aligned}$$

where we've applied the triangle inequality and used the bound twice. How do we know that this results in infinitely many distinct pairs? Things could also go wrong if the same pairs

resulted from all but finitely many choices of Q . However, the bound from Dirichlet's theorem prevents this: any pair (p, q) can arise for at most *finitely* many starting values for Q . Pick a Q , then produce q satisfying the bound. Then $\|q\sqrt{d}\| \neq 0$ since \sqrt{d} is irrational, and thus the LHS is some positive irrational number. For a fixed q , choosing Q' big enough can make the RHS smaller than the LHS, meaning that q can not occur for that value of Q' or anything larger. In other words, we're using

$$\|q\sqrt{d}\| \leq \frac{1}{Q+1} \xrightarrow{Q \rightarrow \infty} 0,$$

and there can't be any infinite sequences of Q_i yielding the same fixed q , since the RHS would go to zero while the LHS does not. ■

Remark 10.2.6: Choosing a pair (p, q) as above, we'll have $p + q\sqrt{d} \in \mathbb{Z}_K$ and

$$\begin{aligned} |N(p + q\sqrt{d})| &= |p^2 - dq^2| \\ &< 1 + 2\sqrt{d}. \end{aligned}$$

So we have many elements in \mathbb{Z}_K whose norm is bounded, which will force the existence of a nontrivial unit. ✍

Lemma 10.2.7 (Finitely many ideals of bounded norm).

For all real $x > 0$ there are finitely many nonzero ideals $I \subseteq \mathbb{Z}_K$ with $N(I) := |\mathbb{Z}_K/I| \leq x$.

Proof (of lemma).

Suppose $N(I) := m \leq x$ with $m \in \mathbb{Z}^+$; it's enough to show that for each m there are at most finitely many I , since there are only finitely many values of $m \leq x$. View \mathbb{Z}_K/I as a group under addition, so by Lagrange every element has order dividing m . We can check $m = 1 + 1 + \dots + 1$, which must be the identity in \mathbb{Z}_K/I . So $m \in I$, and since to contain is to divide, $I \mid \langle m \rangle$. But $\langle m \rangle$ has only finitely many ideal divisors. Why? This is because there is unique prime factorization, and just like $n = \prod p_i^{n_i}$ in the integers, n has $\sum n_i < \infty$ possible divisors. ■

Proof (There exists a nontrivial unit).

We now want to show that there exists a unit $\epsilon > 0$ that is not equal to 1. Consider all ideals $I_{p,q} := \langle p + q\sqrt{d} \rangle$ where (p, q) is a pair of positive integers such that $|p^2 - dq^2| < 1 + 2\sqrt{d}$. Taking norms amounts to taking absolute values of generators, so

$$N(I_{p,q}) < 1 + 2\sqrt{d}$$

for all p, q . By the last lemma, this means there are only finitely many different ideals. On the other hand, there are infinitely many such pairs, so infinitely many pairs give rise to the same ideal. Pick two pairs (p, q) and (p', q') such that $\langle p + q\sqrt{d} \rangle = \langle p' + q'\sqrt{d} \rangle$. If two ideals are equal, the generators differ by a unit, and so

$$(p + q\sqrt{d}) = \epsilon(p' + q'\sqrt{d}), \quad \epsilon \in U(\mathbb{Z}_K).$$

Everything in sight is positive, so solving for ε yields $\varepsilon > 0$. But $\varepsilon \neq 1$, since the pairs would have to have been the same by comparing coefficients in the expression above. ■

Remark 10.2.8: This gives us the fundamental unit. How do we actually find it? See the book – use continued fractions! It's not surprising they'd come up, since they provide a more constructive proof of Dirichlet's approximation theorem.

Example 10.2.9 (of the fundamental unit): Take $d = 2$, what is ε_0 ? We have $U(\mathbb{Z}_K) = \{\pm \varepsilon_0^k \mid k \in \mathbb{Z}\}$, and so if we just look at positive units, the smallest power such that $\varepsilon_0^k > 1$ will just be equal to ε_0 . So we're really looking for the smallest unit greater than 1. We proved that if $\varepsilon_0 = u + v\sqrt{d}$, then $u, v \geq 0$, and if $\varepsilon_0 > 1$ is strict then $u, v > 0$ is strict as well. We also know that $u, v \geq 1$, using that $\mathbb{Z}_K = \mathbb{Z}[\sqrt{2}]$. Luckily enough, $1 + \sqrt{2}$ is a unit, and so $\varepsilon_0 = 1 + \sqrt{2}$.

10.3 Class Groups and the Class Number

Remark 10.3.1: This is now chapter 9. Let K be a quadratic field.

Definition 10.3.2 (Dilation Equivalence)

If I, J are nonzero ideals of \mathbb{Z}_K , we say I, J are **dilation equivalent** if there exists a $\lambda \in K^\times$ such that $I = \lambda J$.

Remark 10.3.3: It's easy to check that this is an equivalence relation, so we'll use $I \approx J$.

Definition 10.3.4 (Class Group)

The **class group** of \mathbb{Z}_K is defined as

$$\text{Cl}(\mathbb{Z}_K) := \text{Id}(\mathbb{Z}_K) / \approx .$$

Remark 10.3.5: A priori this is just a set, but we can descent the monoid structure to define a group multiplication. We define $[I][J] = [IJ]$, and it's easy to check that this is well-defined on equivalence classes. The identity is $[\langle 1 \rangle]$, and for inverses we can use the fact that $[I\bar{I}] = [\langle N(I) \rangle] = N(I)[\langle 1 \rangle]$. In fact, any J for which IJ is principal serves as an inverse for I . So the inverses come from the *Principal Multiple Lemma*, and a similar story will go through for general number fields.

Remark 10.3.6: This is an abelian group, wouldn't it be nice if it were finite? This is one of the big theorems of number theory: $\text{Cl}(\mathbb{Z}_K)$ is finite. We can thus define the following:

Definition 10.3.7 (Class Number)

The **class number** of K is defined as:

$$h_K := |\text{Cl}(\mathbb{Z}_K)|.$$

Lemma 10.3.8 (*Comparison bound between element norm and ideal norm*).

There is a constant C depending on K such that for every $I \in \text{Id}(\mathbb{Z}_K)$ there is a nonzero $\alpha \in I$ such that

$$|N\alpha| \leq CN(I).$$

In fact, one can take

$$C := 1 + \text{Tr}(\tau) + |N(\tau)|.$$

Remark 10.3.9: The norm of I is a natural thing to compare $N\alpha$ to, since $I \mid \langle \alpha \rangle$ and thus $N(I) \mid N(\langle \alpha \rangle)$, so there's no hope of the LHS being smaller than $N(I)$.

Proof (?).

Look at all elements $a + b\tau \in \mathbb{Z}_K$ such that $0 \leq a, b, \sqrt{N(I)}$. How many elements does this yield? Precisely $\left(\left\lfloor \sqrt{N(I)} \right\rfloor + 1\right)^2$. Note that this is strictly larger than $N(I)$, using $\lfloor x \rfloor > x - 1$ for any x . Then going to the quotient by I , there are exactly $N(I)$ elements, two elements reduce to the same element of \mathbb{Z}_K/I . So their difference is in I , so we get something of the form $a' + b'\tau$ where $a', b' \in \mathbb{Z}$ (where they could now be negative), but are bounded by

$$-\sqrt{N(I)} \leq a', b' \leq \sqrt{N(I)}.$$

The claim is now that the given value of C in the theorem works:

$$\begin{aligned} |N(\alpha)| &= |N(a' + b'\tau)| \\ &= |(a' + b'\tau)(a' + b'\bar{\tau})| \\ &= |(a')^2 + a'b' \text{Tr}(\tau) + (b')^2 N\tau| \\ &\leq |a'|^2 + |a'| |b'| \text{Tr}(\tau) + |b'|^2 N(\tau) \\ &\leq CN(I), \end{aligned}$$

where we've used $a', b' \leq \sqrt{N(I)}$ and collected terms in the last step. ■

Proposition 10.3.10 (*Class representatives of small norm*).

Every ideal class contains an ideal I of norm $N(I) \leq C$.

Corollary 10.3.11 (*Class numbers are finite*).

$h_K < \infty$.

Remark 10.3.12: Why is this true? There are only finitely many ideals with this norm bound, and this says every ideal class belongs to this finite set.

Proof (of proposition).

Since we're working with a group, it suffices to work with inverses, since these still run over all elements. It's enough to show that for every $I \in \text{Id}(\mathbb{Z}_K)$, we can write $[I]^{-1} = [J]$ for some J satisfying $N(J) \leq C$. Choose a nonzero $\alpha \in I$ with $|N(\alpha)| \leq CN(I)$. Since $\alpha \in I$ we know that $I \mid \langle \alpha \rangle$, so we can write $\langle \alpha \rangle = IJ$ for some ideal J . We have $[I][J] = [IJ] = [\langle \alpha \rangle] = [\langle 1 \rangle]$, since all principal ideals are dilation-equivalent to $\langle 1 \rangle$. This means that $[J] = [I]^{-1}$, and our hope is that it has small norm. Taking norms in $\langle \alpha \rangle = IJ$ yields

$$\begin{aligned} |N\alpha| &= N(I)N(J) \\ \implies N(J) &= \frac{|N\alpha|}{N(I)} \\ &\leq \frac{CN(I)}{N(I)} \\ &= C. \end{aligned}$$

■

Example 10.3.13(?): What we'll look at next: $\text{Cl}(\mathbb{Z}[\sqrt{-5}])$. We know this does not have unique factorization, and the claim is that the class group is nontrivial. If it were, every ideal would be dilation-equivalent to $\langle 1 \rangle$, making every ideal principal, and every PID is a UFD. Here we'll have $C = 6$.

One could try to write down all ideals of norm bounded by 6, but instead let's consider how they factor into primes. Every ideal of norm at most 6 factors into prime ideals, whose norm is also bounded by 6. So this factors into prime ideals lying above 2, 3, 5, since any ideal lying above a prime p has norm p or p^2 , and we need $p, p^2 < 6$ here. We've worked out all such primes before, coming from the *prime factor mirroring theorem*:

- $\langle 2 \rangle = P_1^2, P_1 := \langle 2, 1 + \sqrt{-5} \rangle$
- $\langle 3 \rangle = P_2 P_3, P_2 := \langle 3, 1 - \sqrt{-5} \rangle, P_3 := \langle 1 + \sqrt{-5} \rangle$
- $\langle 5 \rangle = P_4^2, P_4 := \langle \sqrt{-5} \rangle$

This allows us to conclude that

$$\text{Cl}(\mathbb{Z}[\sqrt{-5}]) = \langle [P_1], [P_2], [P_3], [P_4] \rangle.$$

In fact, since P_4 is principal we can leave it out.



11 | Class Groups (Lec. 10, Thursday, February 18)

11.1 Computing Class Groups

Remark 11.1.1: Last time: we defined an equivalence relation on nonzero ideals of \mathbb{Z}_K , namely $I \approx J \iff I = \alpha J$ for some $\alpha \in K^\times$. We then defined the **class group**

$$\text{Cl}(\mathbb{Z}_K) := \text{Id}(\mathbb{Z}_K) / \approx.$$

We saw that ideal multiplication descends to a well-defined group structure on ideal classes. Since ideal multiplication is commutative, this is an abelian group, and moreover it is finite.

Example 11.1.2 (Computing the Class Group): Let $K = \mathbb{Q}(d)$ where $d := \sqrt{-5}$. We saw that every ideal class is represented by an element with bounded norm. Applying it to this specific value of d , every element is represented by $[I]$ where $N(I) \leq 6$. If we have such an ideal, it will factor into primes, and thus the class will factor into prime classes. Thus the group is actually *generated* by prime ideals of norm at most 6. Any such ideal will lie above a prime $p \leq 6$, so $p = 2, 3, 5$. We saw

$$\begin{aligned} \langle 2 \rangle &= P_1^2 & P_1 &:= \langle 2, 1 + \sqrt{-5} \rangle \\ \langle 3 \rangle &= P_2 P_3 & P_2 &:= \langle 3, 1 + \sqrt{-5} \rangle, P_3 := \langle 3, 1 - \sqrt{-5} \rangle \\ \langle 5 \rangle &= P_4^2 & P_4 &:= \langle \sqrt{-5} \rangle. \end{aligned}$$

We conclude that $\text{Cl}(\mathbb{Z}_K) = \langle P_1, \dots, P_4 \rangle$. What are the relations? Consider P_4 , and note that $\langle \sqrt{-5} \rangle \approx \langle 1 \rangle$ since $P_4 = \sqrt{-5} \langle 1 \rangle$. A similar argument works for any principal ideal, and we can throw out P_4 . Consider P_2 and P_3 . Since $\langle 3 \rangle \approx \langle 1 \rangle$, we have $P_2 = P_3^{-1}$, so we can also throw out P_2 , since we don't need to include the inverse of a generator. Recall that there is a factorization

$$\langle 1 - \sqrt{-5} \rangle = \langle 2, 1 - \sqrt{-5} \rangle \langle 3, 1 - \sqrt{-5} \rangle = P_1 P_3$$

and so these are inverses and we can get rid of P_3 . So $\text{Cl}(\mathbb{Z}_K) = \langle [P_1] \rangle$, which is a cyclic group. The generator has to have order 1 or 2, since $P_1^2 = \langle 2 \rangle$. The claim is that the order is 2: otherwise, it would be trivial, making the class group trivial, which would imply that \mathbb{Z}_K is a PID. Why? This implies that every $I \in \text{Id}(\mathbb{Z}_K)$ is dilation equivalent to the unit ideal, so $I = \alpha \langle 1 \rangle$ for some $\alpha \in K^\times$. But since I is an ideal in \mathbb{Z}_K , this forces $\alpha \in \mathbb{Z}_K$ and $I = \langle \alpha \rangle$. This is a contradiction, since every PID is a UFD, and $\mathbb{Q}(\sqrt{-5})$ has non-unique factorization. So we can write $\text{Cl}(\mathbb{Z}_K) \cong \mathbb{G}_a(\mathbb{Z}/2\mathbb{Z})$.

Remark 11.1.3: What is the class group useful for? We'll tie this into Diophantine equations.

Example 11.1.4 (of using the class group to solve Diophantine problems): Solve the following equation in \mathbb{Z} :

$$y^2 + 5 = x^3.$$

Recall that we originally tried to do this by factoring the left-hand side and appealing to unique factorization in a number field to deduce that various factors were powers. However, we don't have unique factorization. Although we can write $(y + \sqrt{-5})(y - \sqrt{-5}) = x^3$, it's not clear that this is helpful. The fix will be to go to $\text{Id}(\mathbb{Z}_K)$, which does have unique factorization, where we'll also be able to use facts about the class group. We can turn this into an equation in ideals:

$$\langle y + \sqrt{-5} \rangle \langle y - \sqrt{-5} \rangle = \langle x \rangle^3 \in \text{Id}(\mathbb{Z}[\sqrt{-5}]).$$

The original strategy was to show the left-hand factors were coprime in order to deduce they were both cubes. We'll try to show these ideals are coprime in the monoid sense, then since their product is a cube they'll have to be cubes. This uses the fact that this is a reduced unique factorization monoid, so being a cube up to a unit is not something we have to worry about here.

Claim: There is no common prime ideal that divides both factors, using unique factorization.

Proof (?).

Suppose toward a contradiction that P is prime and divides both. Using that ideal norms are multiplicative, $N(P) \mid N(\langle y + \sqrt{-5} \rangle) = y^2 + 5$. We also know P contains both factors, so it contains $(y + \sqrt{-5}) - (y - \sqrt{-5}) = 2\sqrt{-5}$, so $N(P) \mid N(\langle 2\sqrt{-5} \rangle) = 20$. Thus $N(P) \mid \gcd(y^2 + 5, 20)$ in \mathbb{Z} . This is impossible!

- y is necessarily even for the original equation to be true. If y is odd, take the equation (mod 8): an odd squared is 1 (mod 8), so $y^2 + 5 \equiv 6 \pmod{8}$, which is not a cube in $\mathbb{Z}/8$ since any cube is 0 (mod 8).
- 5 can not divide y . If so, 5 would divide the left-hand side and thus the right-hand side, which forces $5 \mid x$ since 5 is prime. Then $5^3 \mid x^3$, meaning $5^3 \mid y^2 + 5$. In this case, $5^2 \mid y^2 + 5$, and if $5 \mid y$ then $5^2 \mid y^2$, so we'd need $5^2 \mid 5$.

These together imply that $\gcd(y^2 + 5, 25) = 1$. This $N(P) \nmid 1$, forcing $P = \langle 1 \rangle$, a contradiction. ■

Thus we can write

$$\begin{aligned} \langle y + \sqrt{-5} \rangle &= I^3 \\ \langle y - \sqrt{-5} \rangle &= J^3. \end{aligned}$$

In the previous argument, we wrote out $(a + b\sqrt{-5})^3$, expanded, and compared coefficients. Here we have an equation in ideals, and we can't do something similar unless I, J are principal. This is in fact the case: we'll restrict our attention to the class group. The left-hand side is the unit ideal, since it is principal. So we can write $[I]^3 = [J]^3 = e$, but we also know $\text{Cl}(\mathbb{Z}_K) \cong \mathbb{G}_a(\mathbb{Z}/2\mathbb{Z})$, so this can only happen if $[I] = [J] = e$ and I, J must be principal. So we can write $I = \langle a + b\sqrt{-5} \rangle$ for some $a, b \in \mathbb{Z}$. Thus

$$\langle y + \sqrt{-5} \rangle = \langle (a + b\sqrt{-5})^2 \rangle \implies y + \sqrt{-5} = \pm 1 (a + b\sqrt{-5})^3,$$

using the fact that they differ by a unit but the only units in $\mathbb{Z}[\sqrt{-5}]$ are ± 1 . The original proof now goes through, comparing coefficients of $\sqrt{-5}$. This will force $b = \pm 1$, then plug things back in to find a , then y , then x . The conclusion is that there are no solutions.

Remark 11.1.5: The critical takeaway: unique factorization failed, but the structure of the class group saved us! We crucially used that it had no elements of order 3. See the book for a general theorem about equations $y^2 + d = x^3$. Ideal theory gives us a way to study Diophantine equations.

11.2 The Class Group as a Measure of Non-unique Factorization

Remark 11.2.1: This is chapter 10. This statement shows up in talks: it's more of a vague sentiment than an actual theorem, but we'll discuss a way to make it precise.

Theorem 11.2.2 (Class number 1 iff UFD).

Recall that the class number is defined as $h_K := \# \text{Cl}(\mathbb{Z}_K)$. Then

$$h_K = 1 \iff \mathbb{Z}_K \text{ is a UFD.}$$

Proof (of theorem).

\implies : Every ideal is equivalent to the unit ideal, so every ideal is principal and PID implies UFD.

\impliedby : Note that this is subtle: this is the claim that \mathbb{Z}_K is a UFD $\implies \mathbb{Z}_K$ is a PID, which isn't true for general rings (e.g. $\mathbb{Z}[x]$). Suppose \mathbb{Z}_K is a UFD, then it's enough to show that every prime ideal is principal. Let P be prime, then P lies above some ordinary prime p , so $P \mid \langle p \rangle$. We can factor $\langle p \rangle = \left\langle \prod_{i=1}^k \pi_i \right\rangle = \prod_{i=1}^k \langle \pi_i \rangle$ for some π_i irreducible. A prime ideal dividing a product, by unique factorization, must divide a factor, so $P \mid \langle \pi_i \rangle$ for some i . In a UFD, irreducibles are prime, so $\langle \pi_i \rangle$ is a prime ideal, so we have a prime ideal dividing a prime ideal. By unique factorization, this forces $P = \langle \pi_i \rangle$, make P principal. ■

Question 11.2.3

Can anything be said if $h_K = 2$, even though we know \mathbb{Z}_K is not a UFD?

Theorem 11.2.4 (Carlitz).

$h_K = 2 \iff$ in \mathbb{Z}_K , any two factorizations of nonzero nonunit α into irreducibles have the same number of terms.

Remark 11.2.5: For example, in $\mathbb{Z}[\sqrt{-5}]$ we have $6 = (2)(3) = (1 + \sqrt{-5})(1 - \sqrt{-5})$, which have the same number of factors. To prove this theorem, we'll first need a lemma:

Lemma 11.2.6 (Class Number 2 implies 2 factors).

Suppose $h_K = 2$, and suppose $\pi \in \mathbb{Z}_K$ is an irreducible that is not prime (which is possible in a non-UFD). Then factoring $\langle \pi \rangle = P_1 P_2$ involves exactly two prime ideals P_1, P_2 in \mathbb{Z}_K .

Proof (of lemma).

Write $\langle \pi \rangle = \prod_{i=1}^g P_i$, we then want to show $g = 2$. We have $g \geq 2$, since otherwise this would be a prime ideal, which would make π a prime element. The claim is that none of the P_i can be principal. Suppose toward a contradiction $P_1 = \langle \rho \rangle$. Note that multiplying ideals yields smaller sets, so the right-hand side is a subset of $\langle \rho \rangle$, as is the left-hand side, and so $\rho \mid \pi$. Since the P_i were principal prime ideals, ρ is prime and thus irreducible (since prime \implies irreducible for any domain), so $\rho = u\pi$ for some unit. Thus they generate the same ideal, and $P_1 = \langle \rho \rangle = \langle \pi \rangle$. But then π generates a prime ideal, make π prime, a contradiction. So none of the P_i are principal. Look at this equation in the class group. The left-hand side is the identity, and the right-hand side are all non-identity elements a group of order 2. So $[P_1][P_2] = e$, making $P_1 P_2 = \langle \omega \rangle$ principal. Then $\langle \pi \rangle \subseteq \langle \omega \rangle$ and so $\omega \mid \pi$. Moreover, ω is not a unit since the product of two prime ideals is not the unit ideal. Since π is irreducible, this makes $\omega = u\pi$ and thus $\langle \omega \rangle = \langle \pi \rangle$. If this were the case, we could cancel in the original equation:

$$\begin{aligned} \langle \pi \rangle &= (P_1 P_2) P_3 \cdots P_g = \langle \pi \rangle P_3 \cdots P_g \\ \implies \langle 1 \rangle &= P_3 \cdots P_g, \end{aligned}$$

but this is a product of prime ideals resulting in the unit ideal. This can only happen if there are no terms in this product, so $g = 2$. ■

Proof (of theorem (\implies)).

Suppose $h_K = 2$. We already know \mathbb{Z}_K is not a UFD by the previous theorem. The nontrivial part is showing factorization into nonzero nonunits of the same number of terms. Instead of working with factorization of elements, we'll work with factorization of their principal ideals into principal ideals generated by irreducibles, which will obviate the need to worry about units. We thus want to show that any principal ideal $P \neq \langle 0 \rangle, \langle 1 \rangle$ has all of its factorizations into principal ideals generated by irreducibles the same length.

Example 11.2.7(?): Much like the previous example, we have

$$\langle 6 \rangle = \langle 1 + \sqrt{-5} \rangle \langle 1 - \sqrt{-5} \rangle = \langle 2 \rangle \langle 3 \rangle.$$

Suppose that P factors as

$$P = \prod_{i=1}^k \langle \pi_i \rangle = \prod_{j=1}^{\ell} \langle \rho_j \rangle \quad \pi_i, \rho_j \text{ irreducible,}$$

we'd then like to show that $k = \ell$.

Observation

If π_1 is prime, we can use that $\langle \pi_1 \rangle \mid \prod \langle \rho_j \rangle$, and would thus have to divide (say) $\langle \rho_1 \rangle$ up to

relabeling. Since everything is irreducible, if $\pi_1 \mid \rho_1$ then $\langle \pi_1 \rangle = \langle \rho_1 \rangle$, meaning we can cancel.

So after cancellation, we can suppose that all the π_i, ρ_j and none are prime. Consider the number of prime ideals that show up after factoring all of the principal ideals on either side. By the lemma, any irreducible that's not prime factors into two primes, so we get $2k$ primes on the left-hand side (not necessarily distinct) and 2ℓ on the right-hand side. But the factorization into primes is unique, so $2k = 2\ell$ and $k = \ell$. ■

Remark 11.2.9: See the book for the other direction!

Theorem 11.2.10 (Landau).

Every ideal class contains infinitely many prime ideals.

Remark 11.2.11: This is an analytic theorem! The proof is similar to how Dirichlet proved the infinitude of primes in arithmetic progressions, which involves L -functions.

Remark 11.2.12: What about $h_K \geq 2$? We'll introduce a way of measuring how bad unique factorization fails in a ring, the notion of *elasticity*.

11.3 Elasticity

Definition 11.3.1 (Elasticity of a Ring)

Let $\alpha \in \mathbb{Z}_K$ where $\alpha \neq 0$ and is not a unit. Define

$$\rho(\alpha) := \frac{L(\alpha)}{S(\alpha)},$$

where $L(\alpha)$ is the number of terms in the longest^a factorization of α and $S(\alpha)$ is the shortest number of terms. This measures how far away from unique the factorization of α is. Now define the **elasticity** of \mathbb{Z}_K as

$$\rho(K) := \sup_{\alpha} \rho(\alpha).$$

^aThere is a way to factor that maximizes the number of irreducibles appearing, and there are not arbitrarily long factorizations.

Remark 11.3.2: Note that $h_K = 1, 2 \iff \rho(K) = 1$, and $h_K > 2 \implies \rho(K) > 1$.

Theorem 11.3.3 (Elasticity in terms of the Davenport constant).

For $h_K \geq 2$,

$$\rho(K) = \frac{1}{2} D(\text{Cl}(\mathbb{Z}_K)),$$

where $D(G)$ is the **Davenport constant** of the finite abelian group G : the smallest number D such that every sequence of D elements of G contains a nonempty subsequence whose product is the identity. This is a function from combinatorial group theory.

Exercise 11.3.4 (bounding the Davenport constant)
Show that $D(G) \leq |G|$.

Fact 11.3.5

$D(G) \rightarrow \infty$ as $|G| \rightarrow \infty$.

Corollary 11.3.6(?).

If $h_K \rightarrow \infty$ for a sequence of number fields, then $\rho(K) \rightarrow \infty$.

Remark 11.3.7: This just follows from the above facts, since $h_K \rightarrow \infty$ means the size of the group $G := \text{Cl}(\mathbb{Z}_K)$ goes to infinity, which is a constant times $\rho(K)$. So as the class group gets larger, factorization gets worse.

12 | Prime Producing Polynomials and Unique Factorization (Lec. 11, Tuesday, February 23)

Remark 12.0.1: Today: chapters 11 and 12.

12.1 Chapter 11: Prime Producing Polynomials and Unique Factorization

Remark 12.1.1: 18th century observation by Euler about the following polynomial:

$$f(x) := x^2 - x + 41.$$

Goldbach proved that it's impossible for any polynomial $g \in \mathbb{Z}[x]$ to have *every* output prime. Euler noted that this f produces quite a few: for $x = 1, \dots, 40$, the output $f(x)$ is prime, but $f(41) = 41^2 - 41 + 41 = 41^2$ is not. Let's define a variant: for q a positive integer, set

$$f_q(x) := x^2 - x + q.$$

Note that $f_q(q) = q^2$, so eventually the output is composite. We'll say f_q is **optimal** if $f_q(x)$ is prime for all integers $0 < x < q$. As an example, $q = 41$ was optimal.

Theorem 12.1.2 (Rabinowitz).

Let $q \geq 2 \in \mathbb{Z}^{>0}$ and let $d = \Delta(f_q) = 1 - 4q$ be the discriminant of f_q . Assume that d is squarefree, then f_q is optimal if and only if $\mathbb{Z} \left[\frac{1 + \sqrt{d}}{2} \right]$ is a UFD. ^a

^aNote that this is equal to \mathbb{Z}_K when $K := \mathbb{Q}(\sqrt{d})$.

Example 12.1.3 (of a ring of integers that is a UFD): For $q = 41, d = -163$ and thus $\mathbb{Z} \left[\frac{1 + \sqrt{-163}}{2} \right]$ is a UFD.

Proof (\Leftarrow).

Big idea: uses that $\min_{\tau}(x) = f_q(x)$ and remembering that how $\min_{\tau}(x) \pmod{p}$ factors is exactly how $\langle p \rangle$ factors into prime ideals.

Assume $\mathbb{Z}[\tau]$ is a UFD, where $\tau := \frac{1 + \sqrt{d}}{2}$. Toward a contradiction, suppose $f_q(x)$ is composite for some $0 < x < q$. We can write

$$f_q(x) = x^2 - x + q = (x - \tau)(x - \bar{\tau}) = \min_{\tau}(x)_{/\mathbb{Q}}.$$

By considering how this function increases, we can conclude $1 < q < f_q(x) < f_q(q) = q^2$. Let p be the least prime factor of $f_q(x)$, which is necessarily bounded by $\sqrt{f_q(x)}$, so $p < q$. Since $p \mid f_q(x)$, we have $x \in \mathbb{Z}$ as a root of $f \pmod{p}$. So \min_{τ} has a root modulo p . Recall that studying how $\langle p \rangle$ factors into ideals of \mathbb{Z}_K involved studying how \min_{τ} factors mod p . Since we've shown it has a root mod p , it breaks into two linear factors. So $\langle p \rangle = P_1 P_2$ as prime ideals of norm p . By assumption, $\mathbb{Z}[\tau]$ is a UFD and the ring of integers of a number field, and by an earlier theorem, is thus also a PID (noting that this is not generally the case). So P_1, P_2 are principal, and we can write

$$P_1 = \langle a + b\tau \rangle \implies p = N(p_1) = N(a + b\tau) = a^2 + ab + qb^2.$$

Completing the square yields

$$\dots = (a + b/2)^2 + (q - 1/4)b^2.$$

Note that $b \neq 0$, since this would yield $p = a^2$ in the first equation and $a, p \in \mathbb{Z}$ with p prime. So both terms in the second equation are non-negative, and the second is positive because $b > 1$, so $p \geq q - 1/4$. Since $p, q \in \mathbb{Z}$ we can strengthen this to $p \geq q$. But p was the *least* prime factor of $f_q(x) < q^2$ which was composite, so this is a contradiction. \nexists

Remark 12.1.4: The forward direction is harder here.

Proof (\Rightarrow).

We'll prove something stronger. Assume $f_q(x)$ is prime whenever

$$1 \leq x \leq \frac{1}{2}\sqrt{\frac{|d|}{3}} + \frac{1}{2},$$

then we'll prove that \mathbb{Z}_K is a PID and hence a UFD. Note that this is stronger because the range is smaller than $0 < x < q$.

Claim: p is inert for all $p \leq \sqrt{\frac{|d|}{3}}$ (so the prime ideal $\langle p \rangle$ remains prime).

Proof (?).

If not, \min_{τ} has a root $(\bmod p)$. Recalling that $\min_{\tau}(x) = f_q(x) = x^2 - x + q$, if this has one root then it has two which sum to $-b = -(-1) = 1$, where one of them satisfies

$$1 \leq x \leq \frac{1}{2}\sqrt{\frac{|d|}{3}} + \frac{1}{2}.$$

Why? If the other root $x = r$ with $1 < r < p$ doesn't satisfy this, then the first root is $p + 1 - r$ and will satisfy this. Then $p \mid f_q(x)$, but this is a problem! This forces

$$p = f_q(x) = x^2 - x + q \geq q > \sqrt{\frac{|d|}{3}} \geq p.$$

This contradicts $f_q(x)$ being prime. \nexists

■

So assuming $f_q(x)$ is prime for $1 \leq x \leq \frac{1}{2}\sqrt{\frac{|d|}{3}} + \frac{1}{2}$, we showed that every “small” prime up to $\sqrt{\frac{|d|}{3}}$ is inert. Suppose P is a prime ideal above p , then since p is inert, $P = \langle p \rangle$ is generated by a prime. But we'll just use a slightly weaker conclusion: P is principal.

Theorem 12.1.5 (*When the class group is generated by small primes*).

Let d be a negative squarefree integer with $d \equiv 1 \pmod{4}$ (such as the d we are looking at). Then $\text{Cl}(\mathbb{Z}_K)$ is generated as a group by $[P]$ where P runs over all prime ideals above primes $p \leq \sqrt{\frac{|d|}{3}}$.

Given this theorem, we are done: in our situation, all such $[P]$ are trivial in the class group since they are principal, which makes $\text{Cl}(\mathbb{Z}_K) = 1$ and every ideal is principal.

■

12.2 Proof of Rabinowitz's Theorem

Remark 12.2.1: It just remains to prove the above theorem. We'll use the following:

Proposition 12.2.2 (Almost Euclidean Domains).

Take the same assumptions on d as above. Then for each $\theta \in K = \mathbb{Q}(\sqrt{d})$, there is a positive integer $t \leq \sqrt{\frac{|d|}{3}}$ and a $\xi \in \mathbb{Z}_K$ with norm $N(t\theta - \xi) < 1$.

Remark 12.2.3: This is slightly technical. In words: for any element in your quadratic field, you can approximate it by an *integer* of your field, possibly after a small t dilation. Note that we saw a similar condition for the Euclidean algorithm, namely that $t = 1$ always sufficed.

Proof (of proposition).

Write $\theta = a + b\tau$ where we don't necessarily know $\theta \in \mathbb{Z}_K$ (although this would make the statement trivial), but $a, b \in \mathbb{Q}$. We want to find an appropriate t where $\xi := A + B\tau$ for $A, B \in \mathbb{Z}$. Multiplying the inequality out using the definition of the norm results in

$$\left((ta - A) + \left(\frac{tb - B}{2} \right) \right)^2 + |d| \left(\frac{tb - B}{2} \right)^2 < 1.$$

We'll start by making the second term small by making tb close to an integer (where b is fixed) and choosing B to be that closest integer. We can choose $t \leq \sqrt{\frac{|d|}{3}}$ with $\|tb\| < 1/\sqrt{\frac{|d|}{3}}$, where the norm is the distance to the nearest integer. Why can we do this? This is Dirichlet's approximation theorem, where we could choose $t \leq N$ such that this norm was bounded by $1/(N+1)$, and we can take $N := \left\lfloor \sqrt{\frac{|d|}{3}} \right\rfloor$. How do we choose A, B ? Choose B such that $\|tb\|$ satisfies the above inequality to obtain

$$B \in \mathbb{Z}, \quad |tb - B| < 1/\sqrt{|d|/3}.$$

Then considering the second term in the original equation, we get

$$|d| \left(\frac{tb - B}{2} \right)^2 < |d| \left(\frac{1}{4} \right) \left(\frac{1}{|d|/3} \right) = \frac{3}{4},$$

so it suffices now to choose A such that the first term is bounded by $1/4$. Why can we do this? We have control over A , so we can simply choose it freely to shift the inner quantity into the interval $[-1/2, 1/2]$, i.e.

$$\left| ta - A + \left(\frac{tb - B}{2} \right) \right| \leq \frac{1}{2},$$

and then squaring yields the desired bound. ■

Proof (of theorem).

We have $d \equiv 1 \pmod{4}$ and we want to show that the class group is generated by small primes $p \leq D := \sqrt{|d|}/3$. Let I be a nonzero ideal of \mathbb{Z}_K , we'll find a nonzero ideal J such that $[I] = [J]$ and J is a product of primes above p (which have the appropriate upper bound). In this case, $[J]$ and thus $[I]$ will factor as the product of those primes, and is thus in the subgroup generated by small primes. Fix $\beta \in I$ nonzero of minimal norm.

Claim: For any $\alpha \in I$ there is a $t \leq D$ with $\langle t\alpha \rangle \in \langle \beta \rangle$.

Remark 12.2.4: How to think about this: when the field is Euclidean with respect to the norm, it is a PID. How do you find generators? By taking a nonzero element β of minimal norm in the ideal. Then any element of I would be in β . Here we have an almost-Euclidean property, where elements of I can be hit with a small dilation to land in this principal ideal.

Proof (of claim).

So apply the last element to the element α/β to pick $t \leq D$ and $\xi \in \mathbb{Z}_K$ with $N(t \left(\frac{\alpha}{\beta}\right)) < 1$.

Multiplying through by $N(\beta)$ yields

$$N(t\alpha - \beta\xi) < N(\beta).$$

Note that the inner term on the left-hand side is in I , since $\alpha, \beta \in I$. This is an element of I of norm less than the norm β , but by minimality this can only happen if $t\alpha - \beta\xi = 0$ and thus $t\alpha = \beta\xi \in \langle \beta \rangle$. ■

Now let $T := \lfloor D \rfloor!$, where we take the factorial. Then for any $\alpha \in I$ we have $T\alpha \in \langle \beta \rangle$. Why? We already know *some* factor of T is a multiple of β , and multiplying by other factors doesn't take it out of the ideal. Since this was true for every $\alpha \in I$ we have $TI \subseteq \langle \beta \rangle = \beta\mathbb{Z}_K$. Define $J := (T/\beta)I$, where noting that $T \in \mathbb{Z}^{>0}$, this is just a dilation of I . Then $J \subseteq \mathbb{Z}_K$, since

$$TI \subseteq \beta\mathbb{Z}_K \xrightarrow{\cdot\beta^{-1}} \beta^{-1}TI \subseteq \beta^{-1}\beta\mathbb{Z}_K = \mathbb{Z}_K.$$

Moreover, $J \trianglelefteq \mathbb{Z}_K$ is an ideal, since it's a dilation of an ideal, $[J] = [I]$ since they're related by dilation, and J contains $(T/\beta)\beta = T$. Since to contain is to divide, we have $J \mid \langle T \rangle$. Recall that T was a product of integers, so however $\langle T \rangle$ factors into prime ideals, every such prime ideal will lie above an actual prime no bigger than D . You can factor $\langle T \rangle$ by first factoring T into prime integers, then break them up into prime ideals, all of which would have norm bounded by D . ■

Remark 12.2.5:

Remark 12.2.6: This proves Rabinowitz's theorem.

This says that being an optimal prime is entirely equivalent to a certain ring being a UFD. Are there optimal examples other than $q = 41$? It turns out that there are *no* optimal f_q for $q > 41$, which is not easy to prove. This didn't happen until the 20th century, by folks interested in the UFD side of this statement:

Theorem 12.2.7 (Baker-Heegner-Stark).

\mathbb{Z}_K is not a UFD if $K := \mathbb{Q}(\sqrt{d})$ with d squarefree with $d < -163$.

Remark 12.2.8: So remarkably, there are *not* infinitely many examples for which the ring of integers is a UFD. Thus the class number only takes on the value 1 for finitely many fields. What about for 2? This also only happens finitely often. In fact, for *any* fixed h , there are only finitely many imaginary quadratic fields with class number h . This follows from the fact that $\text{Cl}(\mathbb{Q}(\sqrt{d})) \approx d^{1/2}$, which increases as d does. It's still hard to determine for a given h which values of d appear, partially because the last statement is *ineffective*² in the sense that there aren't constants to put into the asymptotic statement.

Remark 12.2.9: What about real quadratic fields? An expert on this will be joining us here at UGA starting Fall 2021. The situation is expected to be very different, and a conjecture is the following:

Conjecture 12.2.10.

The real quadratic field $\mathbb{Q}(\sqrt{d})$ is a UFD most of the time.

12.3 Lattice Points

Remark 12.3.1: This corresponds to chapter 12. Everything we've done up until now has been for quadratic fields. After this chapter, we'll start anew and rebuild everything for general number fields.

Definition 12.3.2 (Lattice Point)

A **lattice point** in \mathbb{R}^n is a point in \mathbb{Z}^n .

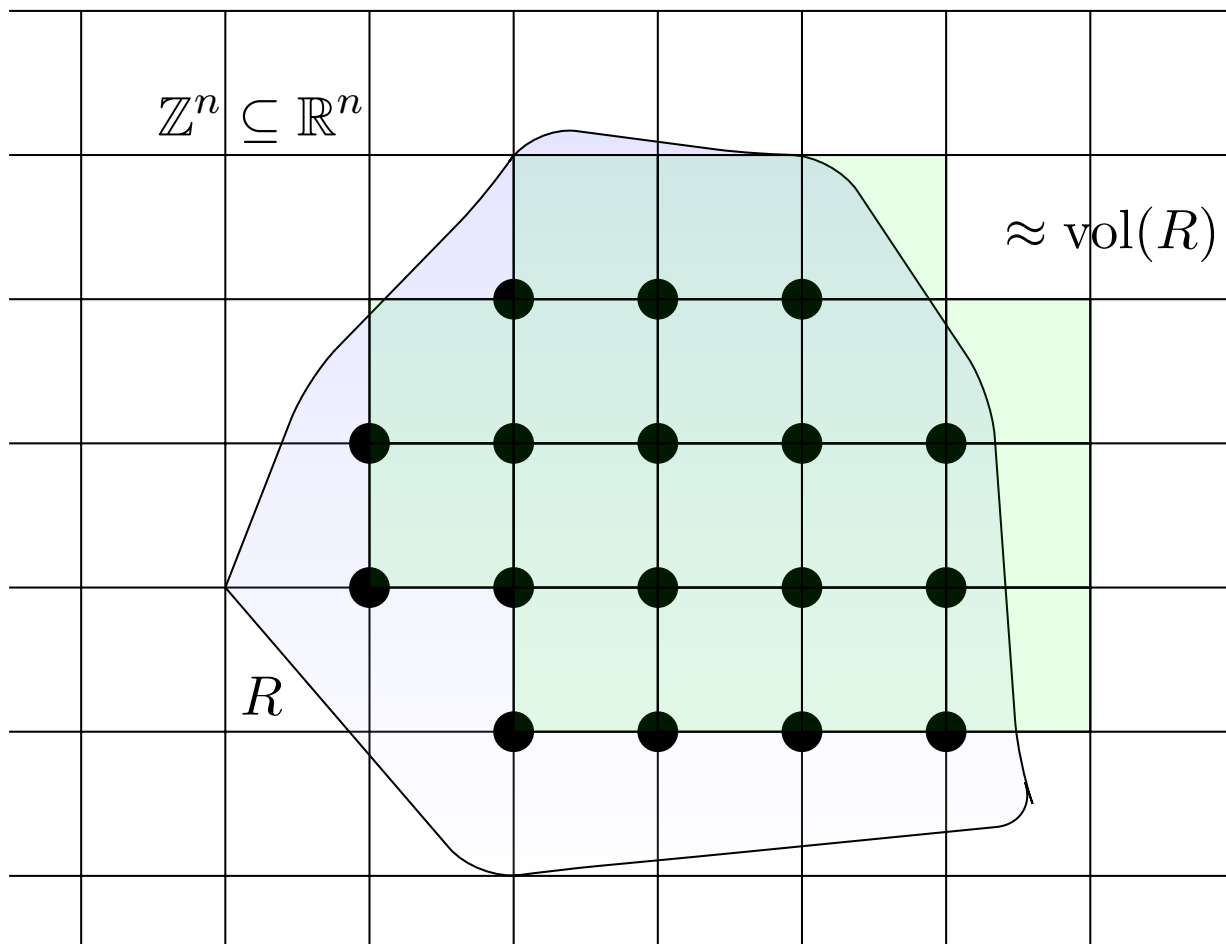
Question 12.3.3

Given a region $R \subseteq \mathbb{R}^n$, how many lattice points does it contain? I.e., how large is the sum

$$\sum_{\mathbf{v} \in \mathbb{Z}^n} \chi_R(\mathbf{v}).$$

Remark 12.3.4: A first guess might be that this is approximately $\text{vol}(R)$. To see why, one can try just choosing to count any squares for which the lower-left point is contained in R and adding up the areas:

²Note that this may not be true as of 2020! See Griffin, M., & Ono, K. (2020). Elliptic curves and lower bounds for class numbers. *Journal of Number Theory*, 214, 1-12.



This isn't exactly right, but would become closer as R grew larger, and the correction term comes from edge effects. For $R \subseteq \mathbb{R}^n$ and $t \in \mathbb{R}$, define the dilation

$$tR := \{t\mathbf{x} \mid \mathbf{x} \in R\}.$$

Theorem 12.3.5 (The number of lattice points in a region is asymptotically the volume).

Let R be a region in \mathbb{R}^n which is *Riemann measurable*.^a Then the number of lattice points satisfies

$$\frac{1}{t^n} \sum_{\mathbf{v} \in \mathbb{Z}^n} \chi_{tR}(\mathbf{v}) \xrightarrow{t \rightarrow \infty} \text{vol}(R).$$

^aThis means that χ_R should be Riemann integrable, i.e. the bounded region is contained in a rectangle, and integrals over such rectangles converges to what we'll call the volume.

Proof (of theorem).

Notice that the left-hand side can be written as

$$\frac{1}{t^n} \sum_{\mathbf{v} \in \mathbb{Z}^n} \chi_{tR}(\mathbf{v}) = \frac{1}{t^n} = \sum_{\mathbf{w} \in t^{-1}\mathbb{Z}^n} \chi_R(\mathbf{w}).$$

This has the effect of making the squares partitioning \mathbb{R}^n finer, the right-hand side is literally the Riemann sum for

$$\int \chi_R(\mathbf{w}) d\mathbf{w} := \text{vol}(R).$$

■

Remark 12.3.6: Note that there is a small technicality since t can take on non-integer values, but the limiting behavior is the same. Next time: we've seen that the number of lattice points is sometimes well-approximated by volume, but it's possible to have regions of unbounded volume with no lattice points, e.g. by taking a large ball and deleting all lattice points. It would be nice to have a theorem which guarantee when a region will have lattice points, and Minkowski's theorem will be one such theorem we'll look at next time.

13 | Lattice Points (Lec. 12, Monday, March 01)

13.1 Minkowski (Version 1)

Remark 13.1.1: Basic heuristic from last time: counting the lattice points in a region R should be approximately $\text{vol}(R)$. We turned this into a theorem for certain regions:

Theorem 13.1.2 (*Lattice points with volume after scaling*).

Let $R \subseteq \mathbb{R}^n$ be a bounded region with a well-defined with respect to the Riemann integral. Letting L_R be the number of lattice points in R , we have

$$\frac{1}{t^n} L_{tR} \xrightarrow{t \rightarrow \infty} \text{vol}(R).$$

Remark 13.1.3: Most of today: Minkowski's theorem, which will guarantee a lattice point under some conditions.

Theorem 13.1.4 (*Minkowski, Version 1*).

Let $R \subseteq \mathbb{R}^n$ be a bounded region that is

1. Convex, so any line segment connecting two points in R is entirely contained within R , and
2. Symmetric about $\mathbf{0}$, so $\mathbf{x} \in R \implies -\mathbf{x} \in R$.

If $\text{vol}(R) > 2^n$, then R contains a nonzero lattice point.

Remark 13.1.5: Any circle/ball or ellipse will be an example. Note that 2^n is sharp, i.e. this theorem does not hold for a smaller constant: take the square $(-1, 1) \times (-1, 1) \subseteq \mathbb{R}^2$, which has volume 4 but only contains the origin as a lattice point.

Proof (of Minkowski Version 1).

Note that any such region already contains $\mathbf{0}$, since containing \mathbf{x} and $-\mathbf{x}$ plus convexity implies containing the line between them, which passes through $\mathbf{0}$. By assumption $\text{vol}(R) > 2^n$, and hence $(1/t^n)L_{tR} > 2^n$ for t large enough. So set $t = m$ for some $m \gg 1 \in \mathbb{Z}^{\geq 0}$, this yields $L_{mR} > (2m)^n$. Consider \mathbb{Z}^n and taking all coordinates $(\bmod 2)m$. This yields $(2m)^n$ equivalence classes of points, so by the pigeonhole principle there exist $\mathbf{v}_1 \neq \mathbf{v}_2 \in mR$ such that $(\mathbf{v}_1 - \mathbf{v}_2)/2m \in \mathbb{Z}^n$, and the claim is that this is the lattice point we want.

Note that this is nonzero, why is it in the region R ? By definition, $(1/m)\mathbf{v}_1 \in R$ and $(-1/m)\mathbf{v}_2 \in R$ using the symmetric assumption. The midpoint between these is precisely the previous point, and this is in R by convexity. ■

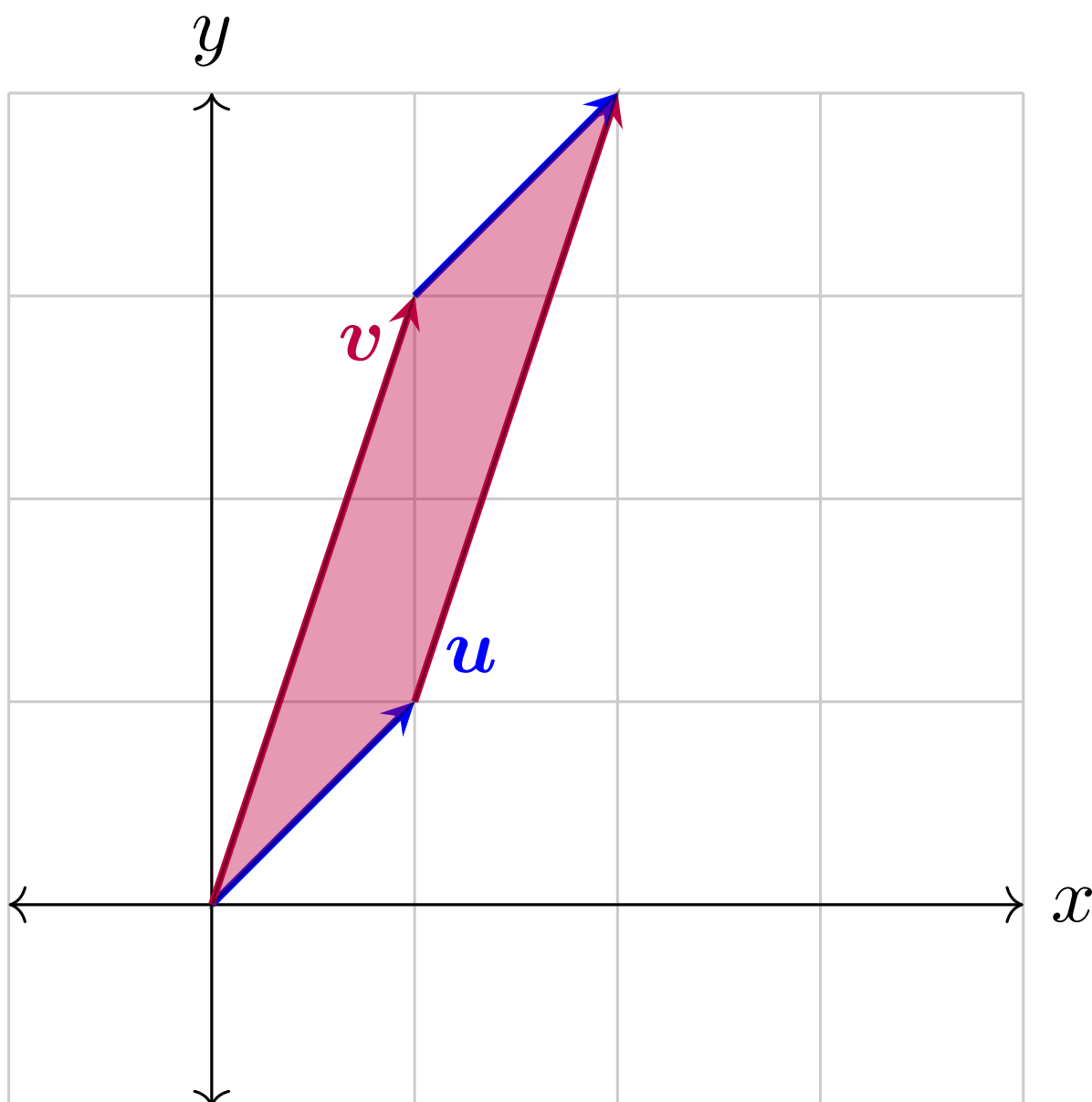
13.2 Minkowski (Version 2)

Definition 13.2.1 (Lattice)

A **lattice** in \mathbb{R}^n is the \mathbb{Z} -span of a collection of \mathbb{R} -linearly independent vectors in \mathbb{R}^n .

Example 13.2.2 ($n = 2$):

- $\Lambda := \mathbb{Z}[1, 0]^t + \mathbb{Z}\{0, 1\}^t$. This tiles the plane by squares.
- $\Lambda := \mathbb{Z}[1, 1]^t + \mathbb{Z}\{1, 3\}^t$. Note that this now tiles the plane by parallelograms:



- $\Lambda := \mathbb{Z}[1, 0]^t$, which recovers $\mathbb{Z} \subseteq \mathbb{R}$. This is not a full lattice, since it lies in a proper subspace of \mathbb{R}^2 .

Note that this will always result in a free abelian group on n generators. Why not define a lattice this way? Here's a non-example:

- $\Lambda := \mathbb{Z}[\sqrt{2}, 0]^t + \mathbb{Z}\{1, 0\}^t$, which are not linearly independent over \mathbb{R} . This yields a dense set of points on the real axis in \mathbb{R}^2 , and is still a free abelian group of rank 2. We'll see later that no lattice can be dense, and in fact they must always be discrete.

Remark 13.2.3: It may not be obvious that a lattice has a uniquely determined number of

generating elements. This turns out to be true: if $\Lambda = \sum_{i=1}^d \mathbb{Z} \mathbf{v}_i$ with $\{\mathbf{v}_i\}_{i=1}^d$ linearly independent over \mathbb{R} , then

$$\Lambda \otimes_{\mathbb{Z}} \mathbb{R} \cong \sum_{i=1}^d \mathbb{R} \mathbf{v}_i \cong \mathbb{R}^d,$$

which is now an \mathbb{R} -vector space of real dimension d . Noting that $\dim_{\mathbb{R}}(\Lambda \otimes_{\mathbb{Z}} \mathbb{R})$ doesn't depend on the choice of basis, any different choice of generating set for Λ must have the same number of generators.

Definition 13.2.4 (Full Lattices)

If $d = n$, we'll call Λ a **full lattice**.

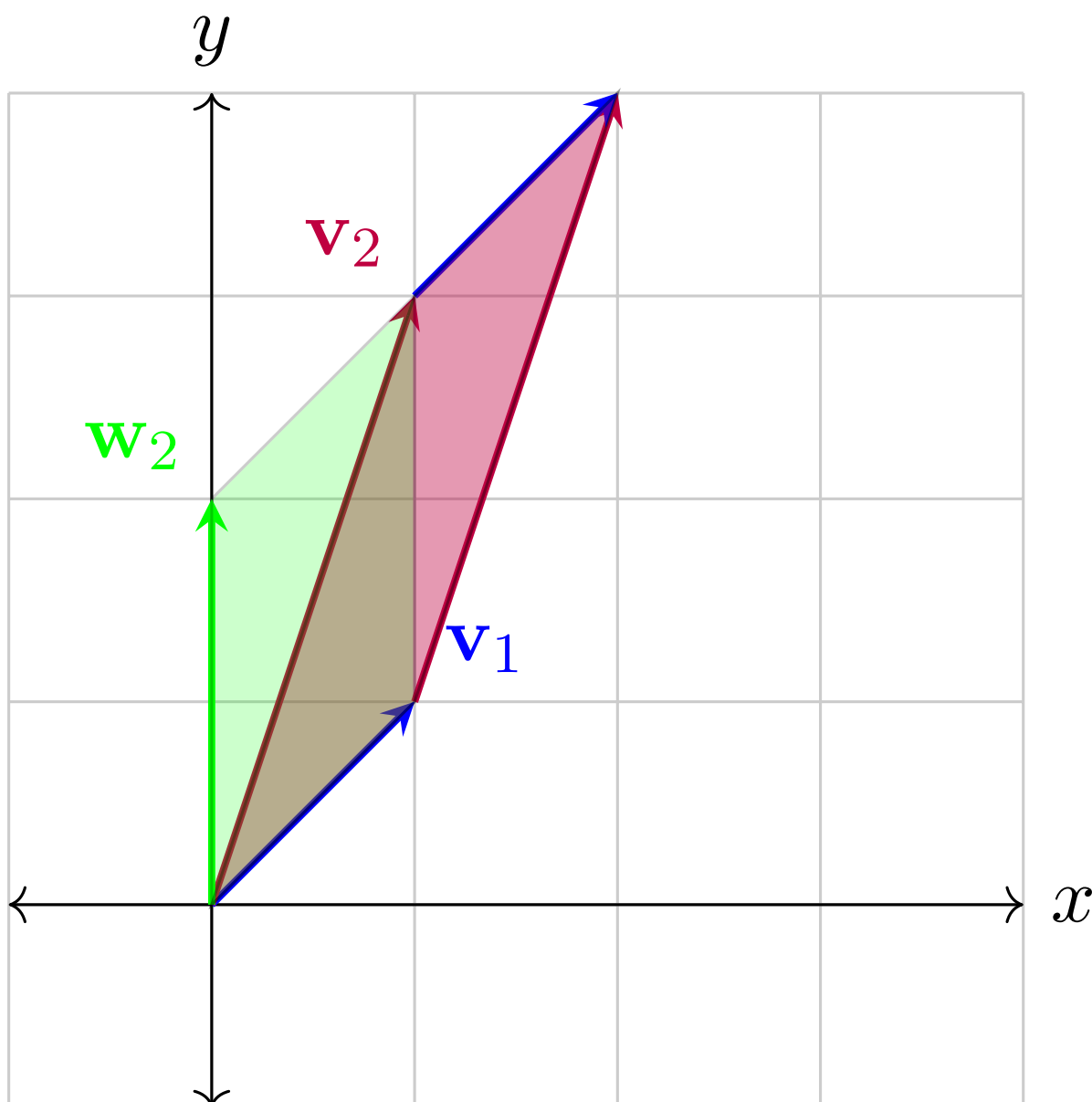
Definition 13.2.5 (Fundamental Parallelepiped)

Note that if Λ is full, then $\Lambda = \sum_{i=1}^n \mathbb{Z} \mathbf{v}_i$ with the \mathbf{v}_i linearly independent over \mathbb{R} . We define the **fundamental parallelepiped** as the set

$$\left\{ \sum_{i=1}^n c_i \mathbf{v}_i \mid 0 \leq c_i \leq 1 \right\}.$$

Note that this depends on the choice of generating set.

Example 13.2.6 (of a fundamental parallelepiped): For $\mathbf{v}_1 = [1, 1]^t$ and $\mathbf{v}_2 = [1, 3]$, we get the parallelogram shown in the earlier figure. Note that Λ is also generated by $\mathbf{v}_1 = \{1, 1\}$, $\mathbf{w}_2 = [0, 2]$, but this generates a different parallelepiped:



Proposition 13.2.7 (*The volume of the fundamental parallelotope is a lattice invariant*).

In general, one gets a parallelotope whose volume is an invariant of the lattice itself.

Proof (of proposition).

How do we compute this? Let $M_v = [\mathbf{v}_1^t, \dots, \mathbf{v}_n^t]$ be the linear transformation obtained by placing all of the generating vectors into the columns of a matrix, and consider scaling the unit cube $C = [0, 1]^n$. Then letting P be the fundamental parallelepiped, we have $P = M_v C$ and so

$$\text{vol}(P) = \text{vol}(M_v C) = |\det(M_v)| \text{vol}(C) = \det(M_v),$$

using that the volume of the standard cube is 1. So it suffices to check that if \mathbf{v}_i and \mathbf{w}_j generate the same lattice Λ , then $\det M_v = \det M_w$. Why is this true? If they generate the same lattice, every \mathbf{v}_i is a \mathbb{Z} -linear combination of the \mathbf{w}_j , and similarly every \mathbf{w}_j can be written as a linear combination of the \mathbf{v}_i . So we get

$$M_v = M_w A \quad M_w = M_v A'$$

for some matrices A, A' . We can thus write

$$M_v = M_v A' A.$$

. Since the \mathbf{v}_i are linearly independent, M_v is invertible, so right-multiplying yields $AA' = I$ and taking determinants yields

$$1 = \det(A') \det(A).$$

Noting that $A, A' \in \text{Mat}(n \times n, \mathbb{Z})$, their determinants must be integers, which forces $\det(A) = \det(A') = \pm 1$. Taking determinants in the original equation yields

$$\det(M_v) = \det(A) \det(M_w) = \pm \det(M_w),$$

and taking absolute values yields the result. ■

Definition 13.2.8 (Covolume of a Lattice)

We'll call the common value $|\det M_v|$ for any choice of generating set $\{\mathbf{v}_i\}$ the **covolume** of Λ :

$$\text{covol}(\Lambda) := |\det M_v|.$$

Theorem 13.2.9 (Minkowski (Version 2)).

Let Λ be a full lattice in \mathbb{R}^n , and let $R \subseteq \mathbb{R}^n$ be a region that is convex and symmetric about zero. Assume that

$$\text{vol}(R) > 2^n \text{covol}(\Lambda).$$

Then R contains a nonzero $\mathbf{v} \in \Lambda$.

Remark 13.2.10: Taking $\Lambda := \mathbb{Z}^n$ recovers the first version. Idea of proof: any full lattice is the image of the standard lattice under some linear transformation. ✍

Proof (of Minkowski Version 2).

Let $\mathbf{v}_1, \dots, \mathbf{v}_n$ be n generators for Λ , then define a linear transformation

$$\begin{aligned} T : \mathbb{R}^n &\rightarrow \mathbb{R}^n \\ \mathbf{v}_i &\mapsto \mathbf{e}_i, \end{aligned}$$

which takes each generator to the corresponding standard basis vector. The $T\Lambda = \mathbb{Z}^n$ is the

standard lattice, and

$$\text{vol}(T(R)) = |\det(T)| \text{vol}(R) = \frac{\text{vol}(R)}{\text{covol}(\Lambda)} > 2^n,$$

noting that $T^{-1} = [\mathbf{v}_1^t, \dots, \mathbf{v}_n^t]$. Now applying the original Minkowski theorem we get a nonzero point

$$\mathbf{x} \in \mathbb{Z}^n \cap T(R) \implies T^{-1}\mathbf{x} \in \Lambda \cap R.$$

■

13.2.1 Application: The 4 Square Theorem

Theorem 13.2.11 (4 Square Theorem (Lagrange)).

Every positive integer is a sum of 4 squares of integers.

Lemma 13.2.12 (Finding sums of squares in \mathbb{Z}/m).

Let $m \in \mathbb{Z}^{>0}$ be squarefree, then there are $A, B \in \mathbb{Z}$ such that

$$A^2 + B^2 + 1 \equiv 0 \pmod{m},$$

i.e. -1 is always the sum of two squares in the ring \mathbb{Z}/m .

Proof (of lemma).

We're trying to solve an equation \pmod{m} , and by the CRT it suffices to solve it for every prime power dividing m , and since m is squarefree, all prime powers occur with exponent 1. So it suffices to consider $m = p$ a prime. We can further assume p is odd, since if $p = 2$ we can take $A = 1, B = 2$. Consider the following two subsets of \mathbb{Z}/p :

$$\begin{aligned} S_1 &:= \{A^2 \pmod{p}\} \\ S_2 &:= \{-1 - B^2 \pmod{p}\}. \end{aligned}$$

Note that $\#S_1 = \frac{p+1}{2}$, since the number of nonzero squares is half the number of elements, so $\frac{p-1}{2}$, and we add in zero. Similarly $\#S_2 = \#S_1$ since it can be obtained from S_1 by sending $x \mapsto -1 - x$. Note that $\frac{p+1}{2} > \frac{p}{2}$, but $|\mathbb{Z}/p| = p$, so these two sets can't be disjoint. So there is some $A^2 = -1 - B^2 \pmod{p}$.

■

Proof (of the 4 Square Theorem).

Suppose m is squarefree. Choose A, B as in the lemma, so $A^2 + B^2 \equiv -1 \pmod{m}$, and define

$\gamma := A + Bi \in \mathbb{Z}[i]$. Let

$$\Lambda := \{(\alpha, \beta) \in \mathbb{Z}[i] \mid \alpha \equiv \beta\gamma \pmod{m}\}.$$

Taking one such ordered pair in Λ , we can apply complex conjugation to obtain

$$\alpha \equiv \beta\gamma \pmod{m} \implies \overline{\alpha}\overline{\beta\gamma} \pmod{\overline{m}} = m,$$

where we can immediately note that $\overline{m} = m$ since $m \in \mathbb{Z}$. Multiplying these two congruences yields

$$\alpha\overline{\alpha} = N(\alpha) \equiv N(\beta)N(\gamma) \pmod{m} \equiv -N(\beta) \pmod{m},$$

and so we have $N(\alpha) + N(\beta) \equiv 0 \pmod{m}$. But these are Gaussian integers, so writing $\alpha = a + bi, \beta = c + di$ we obtain

$$a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod{m}.$$

Being congruent to 0 (mod m) in $\mathbb{Z}[i]$ means that both the real and imaginary parts are divisible by m , but since the left-hand side above is an ordinary integer, it has no imaginary part. So $m \mid a^2 + b^2 + c^2 + d^2$ for every element of Λ . Noting that $\Lambda \subseteq \mathbb{Z}[i]$ we can identify $\Lambda \subseteq \mathbb{Z}^4 \subseteq \mathbb{R}^4$ by pairing $(\alpha, \beta) \mapsto (a, b, c, d)$.

Claim: $\Lambda \subseteq \mathbb{R}^4$ is a full lattice, and after writing a set of generators and computing the determinant, one finds that $\text{covol}(\Lambda) = m^2$.

See the book for a proof of this claim!

Now let

$$R := \{[x, y, z, w] \in \mathbb{R}^4 \mid x^2 + y^2 + z^2 + w^2 < 2m\},$$

which is a convex and centrally symmetric region. A multivariable Calculus exercise shows $\text{vol}(R) = 2\pi^2 m^2$, and $2\pi^2 > 2^4 \text{covol}(\Lambda)$. Applying Minkowski version 2, there exists a nonzero point $\mathbf{x} \in R \cap \Lambda$, and thus its coordinates satisfy

$$0 < x^2 + y^2 + z^2 + w^2 < 2m.$$

The middle term is then an integer that is a multiple of m , forcing it to be equal to m . ■

Remark 13.2.13: We made the assumption that m was squarefree, but we can write any $m \in \mathbb{Z}^{>0}$ as $m = k^2 m'$ where m' is squarefree. Then writing $m' = x^2 + y^2 + z^2 + w^2$, we have

$$m = (kx)^2 + (ky)^2 + (kz)^2 + (kw)^2.$$

There are other applications of Minkowski's theorem that tell you when certain types of numbers are represented by special quadratic forms (such as the above sum of squares). See Pete Clark's papers!

14 | Starting Over with General Number Fields (Lec. 13, Thursday, March 04)

14.1 Recasting Old Definitions

Remark 14.1.1: This corresponds to chapter 13, “Starting Over”. Idea: we’ve phrased everything so far for quadratic fields, now we want to do everything for general number fields. The basic objects and tools: norm and trace. If K/\mathbb{Q} is a number field that’s Galois, we define $N\alpha := \prod_{\sigma \in G} \sigma(\alpha)$ and $\text{Tr } \alpha := \sum_{\sigma \in G} \sigma(\alpha)$. We’ll have to modify this for a general number field since there’s not an immediate candidate for the Galois group.

Setup: let K be a number field with $[K : \mathbb{Q}] = n$, then recall that there exist n different embeddings $\sigma : K \hookrightarrow \mathbb{C}$.

Definition 14.1.2 (Field Polynomial)

If $\alpha \in K$ then define its **field polynomial**

$$\varphi_{\alpha}(x) := \prod_{\sigma: K \hookrightarrow \mathbb{C}} (x - \sigma(\alpha)).$$

Proposition 14.1.3 (*The field polynomial is monic, has rational coefficients, and is a power of the minimal polynomial*).

This is a monic polynomial with \mathbb{C} -coefficients, and in fact $\varphi_{\alpha} \in \mathbb{Q}[x]$ and $\varphi_{\alpha}(x) = \min_{\alpha}(x)^n$ (the minimal polynomial over \mathbb{Q}) for some power n , and the correct choice turns out to be $n := [K : F[\alpha]]$.

Remark 14.1.4: Note that the first claim follows from the second since $\min_{\alpha}(x) \in \mathbb{Q}[x]$.

Lemma 14.1.5 (Number of embeddings of subfields).

Let K be a number field with $[K : \mathbb{Q}] = n$ and $F \leq K$ a subfield with $[F : \mathbb{Q}] = r$. Note that $r \mid n$. Then every embedding $\tau : F \hookrightarrow \mathbb{C}$ extends in n/r ways to an embedding $\sigma : K \hookrightarrow \mathbb{C}$.

Proof (of lemma, sketch).

Standard field theory exercise: by the primitive element theorem, write $K = F(\theta)$ where $\deg(\theta) = [K : F] = n/r$ over F . Since we’re extending an embedding, it suffices to define what it does to θ . If $m(x) = \min_{\theta}(x)$ over F , then $\sigma(\theta)$ must be a root of $(\tau m)(x)$, where the latter polynomial is taking m and applying τ to each of the coefficients. Note that this preserves the degree, so $\deg \tau m = n/r$, and there are n/r choices for $\sigma(\theta)$. Now the proof follows from checking that every single root is a possibility. ■

Proof (of proposition).

By definition, $\varphi_\alpha(x)$ is a product over embeddings $\sigma : K \hookrightarrow \mathbb{C}$, and each such σ restricts to an embedding $F[\alpha] \hookrightarrow \mathbb{C}$, so applying the lemma to $F[\alpha] \leq K$ yields

$$\begin{aligned} \varphi_\alpha(x) &= \prod_{\sigma: K \hookrightarrow \mathbb{C}} (x - \sigma(\alpha)) \\ &= \prod_{\tau: F[\alpha] \hookrightarrow \mathbb{C}} \prod_{\sigma \text{ s.t. } \sigma|_{F[\alpha]} = \tau} (x - \sigma(\alpha)) \\ &= \prod_{\tau: F[\alpha] \hookrightarrow \mathbb{C}} (x - \tau(\alpha))^{n(\tau)} \\ &= \left(\prod_{\tau: F[\alpha] \hookrightarrow \mathbb{C}} (x - \tau(\alpha)) \right)^{[K:F(\alpha)]} \\ &= \min_{\alpha}(x)^{[K:F(\alpha)]}. \end{aligned}$$

where

- We've first just reorganized the product by grouping,
- Then we've used that all of the terms in the inner product must have the same value for $\sigma(\alpha)$ since $\alpha \in F[\alpha]$ and this makes $\sigma(\alpha) = \tau(\alpha)$,
- We note that the exponent should be the number of terms in the inner product, i.e. the number of σ extending τ , i.e. $n(\tau) = [K : F[\alpha]]$ since $r = [F[\alpha] : \mathbb{Q}]$ and $n = [K : \mathbb{Q}]$,
- The last equality follows from remarks in chapter 1.

■

Remark 14.1.6: The field polynomial gives us a way to determine whether an element of a number field is in its ring of integers:

Proposition 14.1.7 (*Field polynomial has integer coefficients iff the element is an integer*).

$$\alpha \in \mathbb{Z}_K \iff \varphi_\alpha(x) \in \mathbb{Z}[x].$$

Proof (of proposition).

\Leftarrow : This direction is easy, since having integer coefficients, being monic, and having α as a root since $x - \sigma(\alpha) = x - \alpha$ for some σ . But this puts $\alpha \in \mathbb{Z}_K$ by definition.

\Rightarrow : We proved that if $\alpha \in \mathbb{Z}_K$ then $\min_{\alpha}(x) \in \mathbb{Z}[x]$, and φ_α is just a power of $\min_{\alpha}(x)$.

■

Definition 14.1.8 (Norm and Trace)

Write

$$\varphi_\alpha(x) = x^n + \sum_{i=1}^n a_i x^i \in \mathbb{Q}[x],$$

we then define the **norm** and **trace**^a respectively as

$$N(\alpha) := (-1)^n a_0 \in \mathbb{Q}$$

$$\mathrm{Tr}(\alpha) := -a_{n-1} \in \mathbb{Q}.$$

Note that if $\alpha \in \mathbb{Z}_K$ then these are both in fact in \mathbb{Z} .

^aThese come from the trace and determinant of the map $y \mapsto y \cdot x$ on L/K , viewed as a K -linear map on L .

Remark 14.1.9: Note that $-(1)^n a_0 = \prod r_i$ is the product of the roots of $\varphi_\alpha(x)$ and $-a_{n-1} = \sum r_i$, so equivalently we can think of these as

$$N(\alpha) = \prod_{\sigma: K \hookrightarrow \mathbb{C}} \sigma(\alpha)$$

$$\mathrm{Tr}(\alpha) = \sum_{\sigma: K \hookrightarrow \mathbb{C}} \sigma(\alpha).$$

It's also the case that $N(\cdot)$ is multiplicative and $\mathrm{Tr}(\cdot)$ is \mathbb{Q} -linear.

14.2 Discriminants

Remark 14.2.1: Let K be a number field and $[K : \mathbb{Q}] = n$. Pick an arbitrary ordering of embeddings $\sigma_1, \dots, \sigma_n : K \hookrightarrow \mathbb{C}$.

Definition 14.2.2 (Tuple Discriminant)

For any n -tuple $(w_1, \dots, w_n) \in K^n$ define the **tuple discriminant** as

$$\Delta(w_1, \dots, w_n) := \det(D_{w_1, \dots, w_n})^2$$

where

$$D_{w_1, \dots, w_n} = \begin{bmatrix} \sigma_1(w_1) & \cdots & \sigma_1(w_n) \\ \sigma_2(w_1) & \cdots & \sigma_2(w_n) \\ \vdots & \cdots & \vdots \\ \sigma_n(w_1) & \cdots & \sigma_n(w_n) \end{bmatrix}.$$

Remark 14.2.3: Why square this? Permuting two columns changes the sign of the determinant, which is just swapping the order of the embeddings. So squaring keeps this invariant under relabeling the σ_i . It turns out that this is a rational number, since we can write

$$\Delta(w_1, \dots, w_n) = \det(D) \det(D) \det(D^t D),$$


where $(D^t D)_{ij} = \mathrm{Tr}(w_i w_j) \implies D^t D \in \mathrm{Mat}(n \times n, \mathbb{Q})$. So taking the determinant yields a rational number, so $\Delta(w_1, \dots, w_n) \in \mathbb{Q}$. Moreover if you start with the $w_i \in \mathbb{Z}_K$, then $D^t D \in \mathrm{Mat}(n \times n, \mathbb{Z})$ and thus $\Delta(w_1, \dots, w_n) \in \mathbb{Z}$.

Why is this called the discriminant?

Theorem 14.2.4 (*The discriminant detects \mathbb{Q} -bases*).

Let $w_1, \dots, w_n \in K$, then

$$\{w_1, \dots, w_n\} \text{ form a } \mathbb{Q}\text{-basis for } K \iff \Delta(w_1, \dots, w_n) \neq 0.$$

Remark 14.2.5: So this *discriminates* between bases and non-bases. 

Proof (of theorem).

\Leftarrow : Suppose $\Delta(w_1, \dots, w_n) \neq 0$. Note that the n elements w_1, \dots, w_n are n elements in an n -dimensional \mathbb{Q} -vector space, so the only way they could fail to be a basis would be if there were a linear dependence. But then considering the matrix D above, a \mathbb{Q} -linear dependence between the w_i , this translates to a corresponding dependence between the columns of D , which would yield the contradiction $\det(D)^2 = 0$.

\Rightarrow : This is the harder part. Toward a contradiction suppose w_1, \dots, w_n are a \mathbb{Q} -basis for K but $\Delta(w_1, \dots, w_n) = \det(D^t D) = 0$. Then the columns of $D^t D$ are linearly dependent, so there are $c_i \in \mathbb{Q}$ not all zero such that

$$\sum_{j=1}^n c_j \operatorname{Tr}(w_i w_j) = 0 \quad \forall i = 1, \dots, n.$$

Introduce an element $\beta := \sum_{j=1}^n c_j w_j \in K^\times$, which is not zero since not all of the c_j are zero and the w_i are a basis. Using linearity of the trace, we can write

$$\operatorname{Tr}(w_i \beta) = 0 \quad \forall i = 1, \dots, n.$$

Again using linearity, we actually have $\operatorname{Tr}(\alpha \beta) = 0$ for all $\alpha \in K$ since every α is in the \mathbb{Q} -span of the w_i , which are a basis. It's then perfectly fine to take $\alpha := \beta^{-1}$, which forces $\operatorname{Tr}(1) = 0$. But we can compute directly that $\operatorname{Tr}(1) = n > 0$ since every embedding σ must send 1 to 1. ■

14.3 Integral Bases

Theorem 14.3.1 (*Integral Basis Theorem*).

For K any number field of degree n , $\mathbb{Z}_K \in \mathbb{Z}\text{-Mod}$ is free of rank n .

Observation 14.3.2

Suppose $(w_1, \dots, w_n), (\theta_1, \dots, \theta_n) \in K$ where $[w_1, \dots, w_n] = [\theta_1, \dots, \theta_n]M$ for some matrix $M \in \operatorname{Mat}(n \times n, \mathbb{Q})$. Then

$$\Delta(w_1, w_2, \dots, w_n) = \Delta(\theta_1, \theta_2, \dots, \theta_n) \det(M)^2.$$

Proof (of observation).

Applying the embeddings σ_i yields an equality $D_{w_1, w_2, \dots, w_n} = D_{\theta_1, \theta_2, \dots, \theta_n} M$. Now taking determinants and squaring yields the result. ■

Proof (of integral basis theorem).

Choose $w_1, w_2, \dots, w_n \in \mathbb{Z}_K$ such that

1. $\Delta(w_1, w_2, \dots, w_n) \neq 0$
2. $|\Delta(w_1, w_2, \dots, w_n)|$ is minimal among those satisfying (1).

Does this make sense? The claim is that if (1) is possible, then (1) and (2) is also possible. This is because $\Delta(w_1, w_2, \dots, w_n) \in \mathbb{Z}$, taking absolute values makes it positive, and then we can minimize among the positive integers occurring using the well-ordering principle. But we can choose tuples satisfying (1): we can always choose a \mathbb{Q} -basis, and to get them down to \mathbb{Z}_K instead of K , they can just be scaled by a rational integer without changing that they form a basis.

Claim: Any tuple w_1, w_2, \dots, w_n satisfying (1) and (2) will be a \mathbb{Z} -basis for \mathbb{Z}_K .

How could this fail? No elements could have multiple representations as a \mathbb{Z} -basis, since they don't admit any in the \mathbb{Q} -basis. So it suffices to show $\text{span}_{\mathbb{Z}} \{w_1, w_2, \dots, w_n\} = \mathbb{Z}_K$. If not, choose $\alpha \in \mathbb{Z}_K$ not in their \mathbb{Z} -span – it must still be in the \mathbb{Q} -span, so we can write $\alpha = \sum c_i w_i$ where the $c_i \in \mathbb{Q}$. We can assume that $c_1 \notin \mathbb{Z}$ by renumbering. Now write

$$\beta := \alpha - [c_1] w_1 \in \mathbb{Z}_K,$$

where $[\cdot]$ denotes taking the integer part. We can write $\beta = [c_1] w_1 + c_2 w_2 + \dots + c_n w_n$. Observe that the tuple

$$[\beta, w_2, \dots, w_n] = [w_1, w_2, \dots, w_n] M, \quad M := \begin{bmatrix} \{c_1\} & 0 & \dots & \vdots \\ c_2 & 1 & \ddots & \vdots \\ c_n & 0 & 0 & 1 \end{bmatrix}.$$

noting that the first column describes how to write β as a linear combination of the w_i . Taking discriminants yields

$$\Delta(\beta, w_2, \dots, w_n) = \Delta(w_1, w_2, \dots, w_n) \det(M)^2 = \Delta(w_1, w_2, \dots, w_n) \{c_1\}^2,$$

where we've computed the determinant using the fact that it is lower triangular. Since $c_1 \notin \mathbb{Z}$, we have $\{c_1\}$ nonzero, real, between 0 and 1. Since the discriminant was nonzero, the right-hand side is nonzero and thus neither is the left-hand side. We would then have

$$0 < |\Delta(\beta, w_2, \dots, w_n)| < |\Delta(w_1, w_2, \dots, w_n)|,$$

which contradicts the minimality of the w_i . ✗ ■

Remark 14.3.3: Note that this is non-constructive, finding a basis is another question!

14.4 Discriminant of Number Fields

Definition 14.4.1 (Discriminant of a Number Field)

Let K be a number field, then the **discriminant** of K is defined as

$$\Delta_K := \Delta(w_1, w_2, \dots, w_n),$$

where $\{w_i\}$ is any \mathbb{Z} -basis for \mathbb{Z}_K .

Remark 14.4.2: Is this actually an invariant of K , since we made a choice of basis? Given two \mathbb{Z} -bases for \mathbb{Z}_K , say $w_1, w_2, \dots, w_n, \theta_1, \theta_2, \dots, \theta_n$, then

$$[w_1, w_2, \dots, w_n] = [\theta_1, \theta_2, \dots, \theta_n]M \quad M \in \mathrm{GL}(n, \mathbb{Z}).$$

Hence

$$\Delta(w_1, w_2, \dots, w_n) = \Delta(\theta_1, \theta_2, \dots, \theta_n) \det(M)^2 = \Delta(\theta_1, \theta_2, \dots, \theta_n).$$

using that invertible matrices have unit determinants, which in \mathbb{Z} are just ± 1 .

Remark 14.4.3: Why do we care? The discriminant measures the complexity of the number field and carries arithmetic information:

Theorem 14.4.4 (*Hermite*).

For every $X > 0$, there are only finitely many number fields such that $|\Delta_K| \leq X$.

Remark 14.4.5: Interesting question: how many are there as a function of X ? This is studied today by fixing a degree n , and we have good answers for $n = 2, 3, 4, 5$, but it's still open to get an asymptotic formula for $n > 5$. Note that our new faculty hire this year is an expert on these kinds of questions!

Theorem 14.4.6 (*Dedekind*).

Taking a prime $p \in \mathbb{Z}$, we have

$$p \text{ ramifies in } \mathbb{Z}_K \iff p \mid \Delta_K,$$

where **ramification** occurs if when $\langle p \rangle \trianglelefteq \mathbb{Z}_K$ factors into prime ideals with a repeated prime factor. In particular, $\Delta(\cdot) < \infty$, and so only finitely many such primes can occur.

15 | Discriminants and Norms (Lec. 14, Saturday, March 13)

Example 15.0.1 (of a discriminant): Suppose $K = \mathbb{Q}(\sqrt{d})$ where d is squarefree. What is its discriminant? We need a \mathbb{Z} -basis of \mathbb{Z}_K , for $d = 2, 3 \pmod{4}$ we can take $(1, \sqrt{d})$. Then we construct a matrix whose columns are the different embeddings of each entry. The embeddings here are the identity and complex conjugation, so we get

$$\Delta_K = \Delta(1, \sqrt{d}) = \det \left(\begin{bmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{bmatrix} \right)^2 = (-2\sqrt{d})^2 = 4d.$$

If $d = 1 \pmod{4}$, then we can take a basis $(1, \frac{1+\sqrt{d}}{2})$, and

$$\Delta_K = \left(\det \begin{bmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{bmatrix} \right)^2 = (-\sqrt{d})^2 = d.$$

So we have

$$\Delta_K = \begin{cases} d & d = 1 \pmod{4} \\ 4d & d = 2, 3 \pmod{4}. \end{cases}$$

Remark 15.0.2: Note that $\Delta_{\mathbb{Q}} = 1$ if you trace through the computation.

15.1 Norms of Ideals

Definition 15.1.1 (Norm of an ideal)

Let $I \subseteq \mathbb{Z}_K$ be a nonzero ideal, then define $N(I) := \#\mathbb{Z}_K/I$.

Remark 15.1.2: Note that this was finite in the quadratic field case since nonzero ideals had a “standard basis”. For general number fields, the ideals can be more complicated, so we’ll need another way to show finiteness.

Lemma 15.1.3 (Elements divide their norms).

Let $\alpha \in \mathbb{Z}_K$, then $\alpha \mid N(\alpha)$ in \mathbb{Z}_K .

Proof (of lemma).

Write down the obvious thing and see that it works!

$$\begin{aligned} N\alpha &:= \prod_{\sigma: K \hookrightarrow \mathbb{C}} \sigma(\alpha) \\ &= \alpha \prod_{\substack{\sigma: K \hookrightarrow \mathbb{C} \\ \sigma \neq \mathbb{1}_K}} \sigma(\alpha) \\ &:= \alpha C, \end{aligned}$$

where we've used that one embedding is the identity and factored it out. So it only remains to show that the *cofactor* C (the product term) is actually in \mathbb{Z}_K . It is $\overline{\mathbb{Z}\mathbb{Z}}$, since α was an algebraic integer, i.e. a root of some monic polynomial with integer coefficients. But then under every embedding, $\sigma(\alpha)$ is a root of the same monic polynomial, so each $\sigma(\alpha) \in \overline{\mathbb{Z}}$, as is their product since it's a ring. On the other hand, we can write $C = N\alpha/\alpha$. Since $N\alpha$ is a nonzero rational integer and $\alpha \in K$, and since K is a field, this quotient is in K . But then $C \in \overline{\mathbb{Z}} \cap K = \mathbb{Z}_K$. ■

Proposition 15.1.4 (*Nonzero ideals have finite norms in rings of integers*).

For $I \trianglelefteq \mathbb{Z}_K$ nonzero,

$$N(I) < \infty.$$

Proof (of proposition).

We start with principal ideals. Let $m \in \mathbb{Z}^+$, then $\mathbb{Z}_K \langle m \rangle := \mathbb{Z}_K / m\mathbb{Z}_K \cong_{\mathbb{Z}\text{-Mod}} \mathbb{Z}^n / m\mathbb{Z}^n \cong (\mathbb{Z}/m\mathbb{Z})^n$ where we've forgotten the ring structure and are just considering it as a \mathbb{Z} -module. But this has size $m^n < \infty$.

Now let $\alpha \in I$ be nonzero and let $m := \pm N\alpha$, choosing whichever sign makes $m > 0$. Since $\alpha \mid N\alpha$, so $N\alpha = \ell\alpha$ is a multiple of α . But $\alpha \in I$ and I is an ideal, so $N\alpha \in I \implies m \in I$. Then (check!) the following map is surjective:

$$\begin{aligned} \mathbb{Z}_K / \langle m \rangle &\twoheadrightarrow \mathbb{Z}_K / I \\ [\alpha]_m &\mapsto [\alpha]_I, \end{aligned}$$

where we've used $m \in I$ for this to be well-defined. So $\#\mathbb{Z}_K / I \leq \mathbb{Z}_K / \langle m \rangle = m^n < \infty$. ■

Theorem 15.1.5 (*The norm is multiplicative*).

For every pair $I, J \trianglelefteq \mathbb{Z}_K$ nonzero,

$$N(IJ) = N(I)N(J).$$

Proof (that the norm is multiplicative).

Deferred! ■

Theorem 15.1.6 (Formula for norm of principal ideals).

For all $\alpha \in \mathbb{Z}_K$ nonzero,

$$N(\langle \alpha \rangle) = |N(\alpha)|,$$

i.e. the norm of a principal ideal is the absolute value of the norm of the element-wise ideal.

Remark 15.1.7: This will follow from the following proposition:

Proposition 15.1.8 (Index = Determinant).

Let $M \in \mathbb{Z}\text{-Mod}$ be free of rank n and let $H \leq M$. Then H is free of rank at most n , so suppose $\text{rank}_{\mathbb{Z}} H = n$. Suppose that $\omega_1, \dots, \omega_n$ is a \mathbb{Z} -basis for M and $\theta_1, \dots, \theta_n$ a \mathbb{Z} -basis for H . We can thus write $[\theta_1, \dots, \theta_n] = [\omega_1, \dots, \omega_n]A$ for some $A \in \text{Mat}(n \times n, \mathbb{Z})$. Then $[M : H] = \#M/H = |\det A|$.

Proof (Sketch).

Idea: convert this problem about an arbitrary $M \in \mathbb{Z}\text{-Mod}$ to a problem about \mathbb{Z}^n . We know $M \cong \mathbb{Z}^n$, and if we send the ω_i to the standard basis vectors, this identifies $H \cong A\mathbb{Z}^n$. So $M/H \cong \mathbb{Z}^n/A\mathbb{Z}^n$, and it's easy to see that $\det A \neq 0$: if not, there would be a linear dependence among the θ_j . Using *Smith normal form*, we can choose $S, T \in \text{GL}_n(\mathbb{Z})$ with

$$SAT = \text{diag}(a_1, \dots, a_n) \quad a_i \in \mathbb{Z}.$$

Since $\det A \neq 0$, we have $\det S, \det T \neq 0$, and so all of the a_i are nonzero. We can write $\mathbb{Z}^n/A\mathbb{Z}^n \cong \mathbb{Z}^n/SAT\mathbb{Z}^n \cong \bigoplus_{i=1}^n \mathbb{Z}/a_i\mathbb{Z}$, which has size $\prod |a_i| = \left| \prod a_i \right| = |\det(SAT)| = |\det(A)|$ since S, T are invertible and thus have determinant ± 1 . ■

Proof (of formula for norm of principal ideals).

Let $\omega_1, \dots, \omega_n$ be a \mathbb{Z} -basis for \mathbb{Z}_K , then $\alpha\omega_1, \dots, \alpha\omega_n$ is a \mathbb{Z} -basis for $\alpha\mathbb{Z}_K = \langle \alpha \rangle$. Now to compute $\#\mathbb{Z}_K/\langle \alpha \rangle$, we use the “index equals determinant” result: write

$$[\alpha\omega_1, \dots, \alpha\omega_n] = [\omega_1, \omega_n]A \implies \#\mathbb{Z}_K/\langle \alpha \rangle = |\det(A)|,$$

we now just need to show that this is equal to $|N\alpha|$. We'll proceed by taking discriminants of tuples, applied to the first equation above. This yields

$$\begin{aligned} \Delta(\alpha\omega_1, \dots, \alpha\omega_n) &= \Delta(\omega_1, \dots, \omega_n) \det(A)^2 \\ \implies \det(A)^2 &= \frac{\Delta(\alpha\omega_1, \dots, \alpha\omega_n)}{\Delta(\omega_1, \dots, \omega_n)} \\ &= \frac{\det(D_{\alpha\omega_1, \dots, \alpha\omega_n})^2}{\det(D_{\omega_1, \dots, \omega_n})^2} = \left(\frac{\det(D_{\alpha\omega_1, \dots, \alpha\omega_n})}{\det(D_{\omega_1, \dots, \omega_n})} \right)^2. \end{aligned}$$

Recall that these matrices were formed by taking the j th tuple element for the j th column and letting the column entries be the images under all embeddings. Just looking at the first rows in each, we'll have

$$[\sigma_1(\alpha\omega_1), \dots, \sigma_1(\alpha\omega_n)] \quad [\sigma_1(\omega_1), \dots, \sigma_1(\omega_n)].$$

In general, the i th row of the first matrix will be $\sigma_i(\alpha)$ times the i th row of the second matrix. But then this ratio of determinants will be $\left(\prod_{i=1}^n \sigma_i(\alpha)\right)^2 := (N\alpha)^2$. So $\det(A)^2 = (N\alpha)^2$, and taking square roots yields the result. ■

15.2 Chapter 14: Integral Bases

Question 15.2.1

Given K a number field, can you find an explicit \mathbb{Z} -basis for \mathbb{Z}_K ?

Remark 15.2.2: This depends on how one is given K , and in general this is hard! This is a question in algorithmic number theory. We'll focus on a specific sub-problem.

Question 15.2.3

Let K be a number field with $[K : \mathbb{Q}] = n$ and suppose $\theta_1, \dots, \theta_n$ in \mathbb{Z}_K are a \mathbb{Q} -basis for K . Is there a simple condition for when they form a \mathbb{Z} -basis for \mathbb{Z}_K ?

Remark 15.2.4: We know there is *some* \mathbb{Z} -basis for \mathbb{Z}_K , so let $\omega_1, \omega_2, \dots, \omega_n$ be one. Then express the θ in terms of the ω :

$$\begin{aligned} [\theta_1, \theta_2, \dots, \theta_n] &= [\omega_1, \omega_2, \dots, \omega_n]A \\ \implies \Delta(\theta_1, \theta_2, \dots, \theta_n) &= \Delta(\omega_1, \omega_2, \dots, \omega_n) \det(A)^2. \end{aligned}$$

We can view $|\det(A)|$ as the index of the subgroup generated by the θ_i in the group generated by the ω_i , so

$$|\det(A)| = [\mathbb{Z}_K : H], \quad H := \text{span}_{\mathbb{Z}} \{\theta_i\}.$$

Thus

$$\Delta(\theta_1, \theta_2, \dots, \theta_n) = \Delta(\omega_1, \omega_2, \dots, \omega_n) [\mathbb{Z}_K : H]^2.$$

We can thus form a simple condition for when $H = \mathbb{Z}_K$:

Corollary 15.2.5 (A sufficient condition).

If $\Delta(\theta_1, \theta_2, \dots, \theta_n)$ is squarefree, then $\theta_1, \theta_2, \dots, \theta_n$ are a \mathbb{Z} -basis of \mathbb{Z}_K .

Remark 15.2.6: Why? If the left-hand side is squarefree, then use that $[\mathbb{Z}_K : H]^2$ divides the left-hand side to conclude it must be 1. Note that this is *not* necessary! We saw that for $d = 2, 3 \pmod{4}$ that $\Delta_K = 4d$, which is not squarefree.

Example 15.2.7 (of finding bases): Let $K = \mathbb{Q}(\theta)$ where θ is a root of

$$f(x) = x^5 - 3x^2 + 1,$$


which is irreducible over \mathbb{Q} . This yields a degree 5 number field. We can look for an n -tuple of elements in \mathbb{Z}_K which is a \mathbb{Q} -basis for \mathbb{Z}_K with a squarefree discriminant. A candidate would be $\{\theta^j \mid 0 \leq j \leq 4\}$, which are all in \mathbb{Z}_K since $\theta \in \mathbb{Z}_K$ which is closed under multiplication.

Claim:

$$\Delta(1, \theta, \theta^2, \theta^3, \theta^4) \text{ is squarefree.}$$

We have

$$\begin{aligned} \Delta(1, \theta, \theta^2, \theta^3, \theta^4) &:= \det([\sigma_i(\theta^{j-1})])^2 \\ &= \det([\sigma_i(\theta)^{j-1}])^2 && \text{since the } \sigma_i \text{ are embeddings} \\ &= \prod_{1 \leq i < j \leq 5} (\sigma_j(\theta) - \sigma_i(\theta))^2 && \text{since this is a Vandermonde matrix} \\ &= \Delta(f), \end{aligned}$$

where this is the *polynomial* discriminant. This can be computed in a computer algebra system, and in this case it equals $-23119 = (-61)(379)$ which is squarefree. So this yields a \mathbb{Z} -basis for \mathbb{Z}_K , i.e. $\mathbb{Z}_K = \mathbb{Z}[\theta]$. Note that $\Delta_K = -23119$ as well, since it's the discriminant of *any* integral basis. 

Example 15.2.8 (of finding bases): Let $K = \mathbb{Q}(\alpha)$ where α is a root of


$$f(x) = x^3 + x^2 - 3x + 8.$$

We can try $1, \alpha, \alpha^2$, and check

$$\Delta(1, \alpha, \alpha^2) = \Delta(f) = (-4)(503),$$

so we can't conclude this is a \mathbb{Z} -basis. Going back to the proof, we *can* conclude that $[\mathbb{Z}_K : H]^2 \mid \Delta(1, \alpha, \alpha^2)$ where $H := \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\alpha^2 = \mathbb{Z}[\alpha]$. This allows us to conclude that $[\mathbb{Z}_K : H] = 1, 2$, so this could still be an index 2 subgroup. If this happens, $\#\mathbb{Z}_K/H = 2$ and every element is annihilated by 2, so $2\mathbb{Z}_K \subseteq H = \mathbb{Z}[\alpha]$. This would mean

$$\mathbb{Z}_K \subseteq \frac{1}{2}\mathbb{Z}[\alpha] = \left\{ \frac{c_0 + c_1\alpha + c_2\alpha^2}{2} \mid c_i \in \mathbb{Z} \right\}.$$

So are there elements of \mathbb{Z}_K of this form that are *not* in $\mathbb{Z}[\alpha]$? If there's nothing of this form in $\mathbb{Z}_K \setminus \mathbb{Z}[\alpha]$ then we can conclude $\mathbb{Z}_K = \mathbb{Z}[\alpha]$. If there *is* something of this form in $\mathbb{Z}_K \setminus \mathbb{Z}[\alpha]$, then $\mathbb{Z}_K \supsetneq \mathbb{Z}[\alpha]$. One can check that $\frac{\alpha + \alpha^2}{2} \in \mathbb{Z}_K \setminus H$. So the original candidate basis was wrong, but we can take $1, \alpha, \frac{\alpha + \alpha^2}{2}$ instead, which is an integral basis. 

Remark 15.2.9: Why is this last part true? These are 3 elements of \mathbb{Z}_K that are still \mathbb{Q} -linearly independent and contains the \mathbb{Z} -span of the previous 3 elements defining H . But the index of H was 2, so this forces it to be everything. So $\mathbb{Z}_K \neq \mathbb{Z}[\alpha]$, and in fact Dedekind showed that $\mathbb{Z}_K \neq \mathbb{Z}[\beta]$ for *any* choice of $\beta \in \mathbb{Z}_K$. So cubic number fields exhibit new behavior when compared to quadratic number fields!

Remark 15.2.10: Next time: integral bases for cyclotomic fields.

16 | Cyclotomic Fields (Lec. 15, Saturday, March 13)

Remark 16.0.1: This is chapter 14 continued.

Definition 16.0.2 (Cyclotomic Fields)

A **cyclotomic field** is a number field $\mathbb{Q}(\zeta_m)$ where $\zeta_m := e^{2\pi i/m}$, a primitive m th root of 1.

Remark 16.0.3: The Kronecker-Webber theorem: any *abelian extension* K/\mathbb{Q} (so $\text{Gal}(K/\mathbb{Q}) \in \text{Ab}$) is contained in a cyclotomic extension, and every cyclotomic field is an abelian extension. Given such a number field $K = \mathbb{Q}(\zeta_m)$, what is \mathbb{Z}_K ?

Theorem 16.0.4 (*The ring of integers of a cyclotomic field is given by adjoining a primitive root of unity*).

For $K = \mathbb{Q}(\zeta_m)$,

$$\mathbb{Z}_K = \mathbb{Z}[\zeta_m].$$

Remark 16.0.5: The degree of any such K/\mathbb{Q} is $\varphi(m)$, and here $\varphi(p) = p - 1$. Also recall Eisenstein's criterion: if p divides all of the coefficients of a polynomial $f(x) := \sum a_i x^i$ but $p^2 \nmid a_0$, then f is irreducible over \mathbb{Q} .

Lemma 16.0.6 (*The minimal polynomials of roots of unity*).

The minimal polynomial of ζ_p over \mathbb{Q} is

$$\Phi_p(x) := x^{p-1} + x^{p-2} + \cdots + x + 1,$$

and so $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$.

Proof (of lemma, a sketch).

Note that ζ_p is a root of Φ_p , since

$$\Phi_p(x) = \frac{x^p - 1}{x - 1},$$

and ζ_p is a root of the numerator of the right-hand side and not of the denominator. This is irreducible by Eisenstein's criterion at p , using $x \mapsto x + 1$.

Proposition 16.0.7 (Eisenstein primes don't divide the extension degree).

Let $\alpha \in \overline{\mathbb{Z}}$ be an algebraic integer such that

$$\min_{\alpha}(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$$

is Eisenstein at the prime p . Let $K := \mathbb{Q}(\alpha)$, a number field of degree n . Then

$$p \nmid [\mathbb{Z}_K : \mathbb{Z}[\alpha]].$$

Proof (of proposition).

We first observe that α^n is a multiple of p in \mathbb{Z}_K . To see this, plug α into the minimal polynomial to get $0 = \alpha^n + \cdots$ and solve for α^n to obtain

$$\alpha^n = -(a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0) \equiv 0 \pmod{p} \text{ in } \mathbb{Z}_K,$$

and this is a multiple of p by the assumption on Eisenstein's criterion. We want to show p doesn't divide $\#\mathbb{Z}_K/\mathbb{Z}[\alpha]$ as \mathbb{Z} -modules, identify the index as the size of this quotient. It suffices to show that $\mathbb{Z}_K/\mathbb{Z}[\alpha]$ has no elements of order p , by applying Cauchy's theorem. If $\beta \in \mathbb{Z}_K$ represents an element of order p in the quotient, then $p\beta \in \mathbb{Z}[\alpha]$ and so $p\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$ for some $b_i \in \mathbb{Z}$. The order of β to be exactly p , so not all of the b_i are multiples of p : otherwise one could divide through by p and conclude $\beta \in \mathbb{Z}[\alpha]$, making it zero in the quotient (and in particular, not of order p as assumed). Suppose toward a contradiction that i is the smallest index such that p does not divide b_i . Then take this last equation mod p :

$$p\beta \equiv 0 \equiv b_i\alpha^i + \cdots + b_{n-1}\alpha^{n-1} \pmod{p}.$$

Now multiply by α^{n-1-i} to obtain

$$0 \equiv b_i\alpha^{n-1} + \cdots \equiv b_i\alpha^{n-1} \pmod{p},$$

where p divides all of the other terms since they all contain a factor of $\alpha^n \equiv 0 \pmod{p}$. So $b_i\alpha^{n-1}/p \in \mathbb{Z}_K$, and by a previous theorem, this forces $N(b_i\alpha^{n-1}/p) \in \mathbb{Z}$. But we can write

$$\begin{aligned} N\left(\frac{b_i\alpha^{n-1}}{p}\right) &= N\left(\frac{b_i}{p}\right) N(\alpha^{n-1}) \\ &= \left(\frac{b_i}{p}\right)^n N(\alpha)^{n-1} \\ &= \left(\frac{b_i}{p}\right)^n \pm a_0 \\ &= \pm \frac{b_i^n a_0^{n-1}}{p^n} \notin \mathbb{Z}. \end{aligned}$$

where we've used that all embeddings fix rational numbers. But this is not an integer, since by Eisenstein p^2 does not divide a_0 . So a_0^{n-1} contributes exactly $n-1$ copies of p , leaving a p in the denominator, and $p \nmid b_i$ since we choose i precisely to arrange for this. \nexists

Remark 16.0.8: Recall some facts about the discriminant: let F be a field and $f(x) \in F[x]$ monic. Then factor $f(x) = \prod_{i=1}^n (x - \alpha_i)$ over some splitting field. We then define

$$\Delta(f) := \prod_{i < j} (\alpha_j - \alpha_i)^2.$$

We won't discuss the theory, but we'll use a few facts.

Fact 16.0.9

For each fixed n and all polynomials f of degree n , $\Delta(f)$ is given by a universal polynomial in the coefficients of f with integer coefficients. For example, for $n = 2$ and $f(x) = x^2 + bx + c$, we have $\Delta(f) = b^2 - 4c \in \mathbb{Z}[b, c]$. If $n = 3$ and $f(x) = x^3 + bx^2 + cx + d$, we have

$$\Delta(f) = 18bcd - 4b^3d + b^2c^2 - 4c^3 - 27d^2 \in \mathbb{Z}[b, c, d].$$

So the discriminant is some polynomial expression in the coefficients, which (more importantly) have *integer* coefficients.

Some consequences:

- $\Delta(f) \in F$, despite the fact that the roots are generally not in F and are instead in some splitting field.
- If $F = \mathbb{Q}$ and $f \in \mathbb{Q}[x]$ and in fact $f \in \mathbb{Z}[x]$, then $\Delta(f) \in \mathbb{Z}$.
- If $F = \mathbb{Q}$ and $f \in \mathbb{Z}[x]$ with q some prime,

$$\Delta(f) \pmod{q} = \Delta(f \pmod{q}),$$

where we first take the discriminant to land in \mathbb{Z} and then reduce to \mathbb{F}_q , or we reduce $f \in \mathbb{Z}[x]$ to $f \pmod{q} \in \mathbb{F}_q[x]$ and take the discriminant using some algebraic close of \mathbb{F}_q .

Proof (That $\mathbb{Z}_K = \mathbb{Z}[\zeta_p]$ for $K = \mathbb{Q}(\zeta_p)$).

To save space, we'll write $\zeta := \zeta_p$. We want to show $1, \zeta, \dots, \zeta^{p-2}$ forms an integral basis, from last time we have

$$\Delta(1, \zeta, \dots, \zeta^{p-2}) = \Delta_K[\mathbb{Z}_K : \mathbb{Z}[\zeta]]^2 \implies [\mathbb{Z}_K : \mathbb{Z}[\zeta]]^2 \mid \Delta(1, \zeta, \dots, \zeta^{p-2}).$$

Claim: The right-hand side is a power of p (up to a sign), and hence so is the left-hand side. We'll proceed by showing that the only prime that could divide the right-hand side is p . Suppose q divides the right-hand side, i.e. $q \mid \Delta(x^{p-1} + \dots + x + 1)$. So this is zero mod q , and thus $\Delta(x^{p-1} + \dots + x + 1 \pmod{q}) \equiv 0$. The discriminant was a product of roots, so it can only be zero if two roots coincide, so there is a multiple root of $x^{p-1} + \dots + x + 1 \pmod{q}$ and thus also of $x^p - 1$. So $x^p - 1$ and its derivative px^{p-1} have a root in common, and (check!) this can only happen if $q = p$.

So $[\mathbb{Z}_K : \mathbb{Z}[\zeta]] = p^\ell$ for some ℓ . Using that fact that $\mathbb{Z}[\zeta] \cong \mathbb{Z}[\zeta - 1]$, we have $[\mathbb{Z}_K : \mathbb{Z}[\zeta]] =$


$[\mathbb{Z}_K : \mathbb{Z}[\zeta - 1]]$. But by the previous lemma, we know that the minimal polynomial of $\zeta_p - 1$ is $\Phi(x + 1)$, which is p -Eisenstein. So by that lemma, $p \nmid [\mathbb{Z}_K : \mathbb{Z}[\zeta - 1]]$, which forces $\ell = 0$ and $\mathbb{Z}_K = \mathbb{Z}[\zeta_p]$. ■

Proof (Sketch of the same proof for $K = \mathbb{Q}(\zeta_m)$).

1. Do roughly the same proof for prime powers $m = p^\ell$
2. Show that if $a, b \in \mathbb{Z}^{\geq 0}$ are coprime then $\Delta_a := \Delta_{\mathbb{Q}(\zeta_a)}, \Delta_b := \Delta_{\mathbb{Q}(\zeta_b)}$ are coprime.

These are defined in terms of integral bases, and we're trying to prove that something *is* an integral basis, so how do you show this if you don't know your basis is integral to begin with? Without knowing the exact values of the discriminants, you can show $\Delta_a \mid a^2$ divides some power of a , and the same for b , and so a, b coprime will make a^2, b^2 coprime as well. This can be shown by computing the discriminant of a *candidate* integral bases rather than an actual one.


3. Use a key lemma: if K_1, K_2 are number fields with coprime discriminants, then considering the composite field, we have $\mathbb{Z}_{K_1 K_2} = \mathbb{Z}_{K_1} \mathbb{Z}_{K_2}$, a composite ring.
4. If a, b are coprime, check that $\mathbb{Q}(\zeta_a) \mathbb{Q}(\zeta_b) = \mathbb{Q}(\zeta_{ab})$ and $\mathbb{Z}[\zeta_a] \mathbb{Z}[\zeta_b] = \mathbb{Z}[\zeta_{ab}]$.
5. Factor $m = \prod_i p_i^{\ell_i}$ and apply steps (3) and (4) inductively. ■

Remark 16.0.10: The hard part is the lemma in (3). Also, questions about discriminants tend to come up during oral exams that include algebraic number theory. 

16.1 Ideal Theory in General Number Rings (Ch. 15)

Remark 16.1.1: Here “number rings” means \mathbb{Z}_K for K a general number field. Let K be a number field with $[K : \mathbb{Q}] = n$. We'd want

1. $\text{Id}(\mathbb{Z}_K)$ to be a UFM as a monoid,
2. $\text{Cl}(\mathbb{Z}_K)$ is a finite group,

Recall that we proved (1) and used it to deduce (2) for quadratic fields, whereas for the general case we'll prove (2) and deduce (1). The approach we'll take here is somewhat idiosyncratic – the standard treatment involves the theory of Dedekind domains, which uses a lot of commutative algebra. This approach is more classic (circa 19th century, very concrete), and we'll skip over less important details (e.g. those that are unlikely to show up on oral exams). 

Definition 16.1.2 (Class Group of a Number Ring)

$$\text{Cl}(\mathbb{Z}_K) := \text{Id}(\mathbb{Z}_K) / \sim,$$

where \sim denotes dilation equivalence.

Remark 16.1.3: Our strategy:

- Prove $\text{Cl}(\mathbb{Z}_K)$ is finite.
- Prove $\text{Cl}(\mathbb{Z}_K)$ is actually a group, i.e. there are inverses, so that for every ideal there is another ideal such that their product is principal (the “Principal Multiple Lemma”).
- The remaining proofs from the quadratic field case go through almost word-for-word.

Proposition 16.1.4 (*Dilations of elements are always close to integers*).

There is a constant $T = T(K)$ that only depends on K such that for every $\theta \in K$, there is a positive integer $t \leq T$ and a $\xi \in \mathbb{Z}_K$ such that

$$|N(t\theta - \xi)| < 1.$$

Remark 16.1.5: I.e. anything in the field can be multiplied by a bounded integer to make it close to something in the ring of integers. This proposition came up for imaginary quadratic fields in the Rabinowitz criterion, crucial for proving that the class group was generated by prime ideals which lie above small primes.

Proof (of proposition).

Omitted! See book, this proof wouldn’t show up on an oral exam. This uses Dirichlet’s approximation criterion again, although in a different way.

■

Theorem 16.1.6 (*The class group is finite*).

$$\# \text{Cl}(\mathbb{Z}_K) < \infty.$$

Proof (that the class group is finite).

Very similar to how it goes for quadratic fields. As before, let $I \in \text{Id}(\mathbb{Z}_K)$ be nonzero and $\beta \in I$ nonzero with $|N\beta|$ minimal.

Claim: Let T be as in the proposition, then $T!I \subseteq \langle \beta \rangle$.

This follows from exactly the same argument as before.

Now define $J := \frac{T!}{\beta}I \subseteq \mathbb{Z}_K$, which is a dilation of I and thus $J \leq \mathbb{Z}_K$ as well. By definition, $I \sim J$, i.e. $[I] = [J] \in \text{Id}(\mathbb{Z}_K)$, and it's now enough to show that there are only finitely many possibilities for J , since then every class is equal to the class of one of finitely many such J . Since $\beta \in I$, we can deduce that $T! \in J$ and thus $\langle T! \rangle \subseteq J$. We'd like to say "to contain is to divide" (as in the case of unique factorization) and conclude $J \mid T!$, which only has finitely many divisors. However, we haven't proved this yet! We can use an algebra fact instead:

$$\left\{ \begin{array}{l} \text{Ideals of } \mathbb{Z}_K \\ \text{containing } \langle T! \rangle \end{array} \right\} \rightleftharpoons \{ \text{Ideals of } \mathbb{Z}_K / \langle T! \rangle \},$$

so it's enough to show that the right-hand side is finite. This is "obvious", since $\#\mathbb{Z}_K / \langle T! \rangle = (T!)^n$. This comes from the fact that $\mathbb{Z}_K \cong_{\text{Ab}} \mathbb{Z}^n$, so as a \mathbb{Z} -module this is isomorphic to $\mathbb{Z}^n / T! \mathbb{Z}^n \cong (\mathbb{Z} / T! \mathbb{Z})^n$, so this is a finite ring and can thus only have finitely many ideals.^a ■

^aIn fact, we've already proved that \mathbb{Z}_K / I for any nonzero ideal I is finite.

Remark 16.1.7: We now want to establish the cancellation law in $\text{Id}(\mathbb{Z}_K)$, then the principal multiple lemma, and then everything else will follow as in the quadratic case.

17 | Ideal Theory in Number Fields Continued (Lec. 16, Tuesday, March 30)

17.1 Setting up the Theory

Remark 17.1.1: We want to develop theorems of ideal theory for \mathbb{Z}_K for K a general number field, i.e. factorization into prime ideals and the finiteness of the class group. The strategy:

- Prove $\text{Cl}(\mathbb{Z}_K)$ is a finite monoid,
- Prove $\text{Cl}(\mathbb{Z}_K)$ has inverses and is thus a group, i.e. every nonzero ideal can be multiplied by another ideal to become principal (principal multiple lemma),
- Run proofs/corollaries as before.

Last time, we proved the first one.

Lemma 17.1.2 (When ideals are left identities under multiplication).

Let $I, J \in \text{Id}(\mathbb{Z}_K)$, then if $IJ = J$ then $I = \langle 1 \rangle$.

Remark 17.1.3: Note that this is a special case of cancellation. To prove this, we'll use that \mathbb{Z}_K is Noetherian, i.e. every ideal is finitely generated as a \mathbb{Z}_K -module. In fact, $\mathbb{Z}_K \cong \mathbb{Z}^n$, so any ideal is free of rank $\leq n$ as a \mathbb{Z} -module, hence finitely generated as a \mathbb{Z} -module, hence finitely-generated as a \mathbb{Z}_K -module since one can use the same generators.

Proof (of lemma).

Let $J = \langle \beta_1, \dots, \beta_n \rangle$, then since $IJ = J$, for every j we can write $\beta_j = \sum_{i=1}^m A_{ij} \beta_i$. This means that there is some matrix $A \in \text{Mat}(m \times m, I)$ with entries $A_{ij} \in I$ such that

$$[\beta_1, \dots, \beta_m] = [\beta_1, \dots, \beta_m]A.$$

Then $A - \mathbb{1}\beta = 0$, making $A - \mathbb{1}$ singular since not all of the β_i were zero since they were generators of a nonzero ideal. Now take the determinant mod I , which yields

$$0 \equiv \det(A - \mathbb{1}) \equiv \det(-\mathbb{1}) \equiv \pm 1 \pmod{I},$$

but this can only occur if $1 \in I$, making $\langle 1 \rangle = I$. ■

Lemma 17.1.4 (Right-cancellation when principal ideals are involved).

Let $I, J \trianglelefteq \mathbb{Z}_K$, then if $IJ = \beta J$ with $\beta \in \mathbb{Z}_K \setminus \{0\}$, we have $I = \langle \beta \rangle$.

Remark 17.1.5: Note that the previous lemma is a special case of this where $\beta = 1$. One can then bootstrap the previous lemma to get this, see the book. ✍

Lemma 17.1.6 (Principal Multiple Lemma).

For all $I \in \text{Id}(\mathbb{Z}_K)$ there is a $J \in \text{Id}(\mathbb{Z}_K)$ such that IJ is principal.

Proof (of principal multiple lemma).

Consider $[I], [I]^2, \dots \in \text{Cl}(\mathbb{Z}_K)$. By the pigeonhole principal, there is some k, ℓ such that $[I^k] = [I]^\ell$, so $I^k = \lambda I^\ell$ for some $\lambda \in K^\times$. Note that any nonzero element of K can be written as k/n for $k \in K$ and $n \in \mathbb{Z}_K$. So we can scale λ to put it in \mathbb{Z}_K , yielding $\lambda = \alpha/m$ where $\alpha \in \mathbb{Z}_K$ and $m \in \mathbb{Z}^\times$. We then have

$$mI^k = \alpha I^\ell = (\alpha I^{\ell-k})I^k.$$

We have enough to cancel the I^k , and so $\langle m \rangle = \alpha I^{\ell-k}$. Dilating both sides by α^{-1} yields $\langle m/\alpha \rangle = I^{\ell-k}$. But this is a power of I that is principal, so we can take $J := I^{\ell-k-1}$. ■

Remark 17.1.7: Note that the logical order in which these theorems are proved is slightly reversed. ✍

Corollary 17.1.8 (Class groups are finite and Id is a cancellative monoid).

- a. $\text{Cl}(\mathbb{Z}_K)$ is a group, and thus a finite abelian group.
- b. $\text{Id}(\mathbb{Z}_K)$ is cancellative. Just show one can cancel principal ideals (by dilation), and then in general you cancel by multiplying both sides principal and cancelling that principal ideal.

To show unique factorization, we before showed factorization into irreducibles first, then uniqueness as a consequence of Euclid's lemma.

Lemma 17.1.9 (*The monoid Id is atomic*).

$\text{Id}(\mathbb{Z}_K)$ is atomic, i.e. every element factors into irreducibles.

Proof (of lemma).

We'll proceed by induction on $N(I)$, using that $N(AB) \leq N(A)$ for any A and so $I \mid J \implies N(I) < N(J)$. Before we used that $N(AB) = N(A)N(B)$, but we haven't proved that here yet. We also don't know that "to divide is to contain" here, but since $I \mid J$ and $I \neq J$, we do obtain $J \subsetneq I$. Hence there is a surjection

$$\mathbb{Z}_K/J \rightarrow \mathbb{Z}_K/I.$$

This has nontrivial kernel since $I \setminus J \neq \emptyset$, so $|\mathbb{Z}_K/J| > |\mathbb{Z}_K/I|$. ■

Lemma 17.1.10 (*Analog of Euclid's Lemma*).

Irreducibles in $\text{Id}(\mathbb{Z}_K)$ are prime.

Proof (of lemma).

Same as before! Literally use the exact same words, we've set it up this way. ■

Theorem 17.1.11 (*The monoid Id is a unique factorization monoid*).

$\text{Id}(\mathbb{Z}_K)$ is a UFM, or equivalently every nonzero ideal factors uniquely as a product of prime ideals.

17.2 Modern Approach

Question 17.2.1

What is the widest class of domains for which the previous theorem holds?

Definition 17.2.2 (Dedekind Domains)

Let R be a domain that is not a field (since ideals in fields are uninteresting). Then R is a **Dedekind domain** if and only if

- a. R is Noetherian,
- b. R is integrally closed, so if $K = \text{ff}(R)$, then if $\alpha \in K$ is a root of a monic polynomial in $R[x]$ we have $\alpha \in R$.^a
- c. Every nonzero prime ideal is maximal.

^aCompare to the classical rational root theorem.

Theorem 17.2.3 (Noether).

TFAE:

1. R is a Dedekind domain,
2. Every nonzero ideal of R factors into prime ideals (not necessarily uniquely).
3. (2) along with uniqueness.

*Proof (of Noether's theorem).*Omitted, this is an exercise in commutative algebra. ■**Proposition 17.2.4 (Rings of integers are Dedekind domains).**For any number field K , \mathbb{Z}_K is a Dedekind domain.*Proof (of proposition).*

We can check the definitions directly:

- a. This is a consequence of the integral basis theorem.
 - b. Suppose $\alpha \in K$ and is a root of a monic polynomial in $\mathbb{Z}_K[x]$, we then want to show $\alpha \in \mathbb{Z}_K$. Then α is a root of a monic polynomial in $\overline{\mathbb{Z}}[x]$, and by a previous proof, any monic polynomial with $\overline{\mathbb{Z}}$ coefficients is itself in $\overline{\mathbb{Z}}$. Since $\alpha \in K$ as well, we have $\alpha \in \overline{\mathbb{Z}}_K \cap K := \mathbb{Z}_K$.
 - c. Let $P \trianglelefteq \mathbb{Z}_K$ be nonzero. Then \mathbb{Z}_K/P is a domain, but any finite integral domain is a field and we know this is finite since $N(P) < \infty$.
-

~
17.3 Norms Revisited
~

Remark 17.3.1: We left one theorem hanging when we discussed norms. We proved that norms of ideals are finite, and $N(P)$ for P principal is equal to $N(a)$ for a any generator. We haven't yet proved the following:

Theorem 17.3.2 (The norm is multiplicative).

$$N(IJ) = N(I)N(J) \qquad \forall I, J \in \text{Id}(\mathbb{Z}_K).$$

Remark 17.3.3: If $I, J \in \text{Id}(\mathbb{Z}_K)$, we have $\gcd(I, J) = I + J$, since this is the smallest ideal such that any $P \mid I, P \mid J$ must satisfy $P \mid \gcd(I, J)$.

Proof (that the norm is multiplicative).

It's enough to show $N(IP) = N(I)N(P)$ for P prime, since every J factors into primes and we can apply this result recursively. Now

$$\begin{aligned} N(IP) &= [\mathbb{Z}_K, IP] \\ &= [\mathbb{Z}_K : I][I : IP] \\ &= N(I)[I : IP], \end{aligned}$$

so it suffices to show $N(P) = [I : IP]$.

Claim: This is true because $\mathbb{Z}_K \cong I/IP$ are isomorphic as \mathbb{Z} -modules.

Choose $\beta \in I \setminus IP$, using that I properly divides IP when it is properly contained. Define a map

$$\begin{aligned} \psi : \mathbb{Z}_K/p &\rightarrow I/IP \\ \alpha \pmod{p} &\mapsto \alpha\beta \pmod{IP}. \end{aligned}$$

This is well-defined since for any two elements which differ by a multiple of P , multiplying by $\beta \in I$ lands in IP .

Exercise (?)

Check that this is a well-defined group morphism.

Injectivity: Suppose that $\alpha \pmod{P} \in \ker \psi$, so $\alpha\beta \in IP$ and $IP \mid \langle \alpha \rangle \langle \beta \rangle$. Note that without the α this would be false, so we're critically using that β is in I but not IP : $IP \nmid \langle \beta \rangle$ since $\beta \notin IP$. So IP divides this product but not β while I does divide β , this forces $P \mid m \langle \alpha \rangle$. Then $\alpha \in P$ and $\alpha \pmod{P} = 0$, so $\ker \psi = 0$.

Surjectivity: We might want to write $\Im(\psi) = \langle \beta \rangle / IP$, but this doesn't quite make sense since IP may not be a subgroup. This can be fixed, $\text{im } \psi = (\langle \beta \rangle + IP)/IP$. But this equals $\gcd(\langle \beta \rangle, IP)/IP$, and this numerator is I since $\beta \in I$ and $\beta \notin IP$. So we have

$$\begin{aligned} \text{im}(\psi) &= \frac{\langle \beta \rangle + IP}{IP} \\ &= \frac{\gcd(\langle \beta \rangle, IP)}{IP} \\ &= I/IP. \end{aligned}$$

■

Remark 17.3.5: For quadratic fields, we could compute ideal norms by multiplying an ideal I by its conjugate \bar{I} to get a principal ideal generated by $N(I)$. Here we don't know what conjugates mean yet for a general number field – one could try applying all of the embeddings into \mathbb{C} and taking a product, but this may not yield an ideal in the same ring again. In particular, if K isn't

Galois, the embedding can land outside of K in \mathbb{C} .

Definition 17.3.6 (Extending Ideals)

For $R \subseteq S$ and $I \trianglelefteq R$, define IS to be the smallest ideal of S containing I (i.e. take all intersections), or equivalently take all finite S -linear combinations of elements from I .

Exercise 17.3.7 (Arithmetic of ideals)

Check that

- $(IJ)S = (IS)(JS)$,
- $(\alpha R)S = \alpha S$.

Theorem 17.3.8 (*Norm is generated by product of conjugates*).

Let $I \in \text{Id}(\mathbb{Z}_K)$ and let L be the Galois closure of K/\mathbb{Q} . For each $\sigma : K \hookrightarrow \mathbb{C}$, the image $\sigma(I)$ is an ideal of $\mathbb{Z}_{\sigma(K)} \subseteq \mathbb{Z}_L$. Then

$$\prod_{\sigma: K \hookrightarrow \mathbb{C}} \sigma(I)\mathbb{Z}_L = N(I)\mathbb{Z}_L.$$

Remark 17.3.9: This shows why the norm is multiplicative, and why $N(\langle \alpha \rangle) = |N(\alpha)|$.

17.4 Applications of Finiteness of Class Group

Question 17.4.1

Where do ideals come from?

Remark 17.4.2: They're meant to generalize multiples of an integer in \mathbb{Z} , but not all ideals in a general number field are principal. However, there is a way in which this is true for \mathbb{Z}_K even when it's not a PID.

Theorem 17.4.3 (*Dedekind's theorem on the actuality of ideals*).

Let K be a number field and $I \trianglelefteq \text{Id}(\mathbb{Z}_K)$. Then there is a $\beta \in \bar{\mathbb{Z}}$ such that $I = \beta\bar{\mathbb{Z}} \cap K$, or equivalently $I = \beta\bar{\mathbb{Z}} \cap \mathbb{Z}_K$.

Remark 17.4.4: Example of a non-principal ideal: in $\mathbb{Z}[\sqrt{-5}]$, the ideal $I := \langle 2, 1 + \sqrt{-5} \rangle$ is not principal, i.e. not all such elements are given by multiples of some element in $\mathbb{Z}[\sqrt{-5}]$. It turns out that instead this is all multiples (in $\bar{\mathbb{Z}}$) of $\sqrt{2}$. So anything that's a multiple of $\sqrt{2}$ and an algebraic integer that's in $\mathbb{Z}[\sqrt{-5}]$ will be in I and vice-versa. So ideals are multiples of a single element, provided you allow that element to be outside of \mathbb{Z}_K and in $\bar{\mathbb{Z}}$ instead.

Lemma 17.4.5 (Ideals become principal after extending).

Let K be a number field and $I \in \text{Id}(\mathbb{Z}_K)$. Then there is a finite extension L/K in which $I\mathbb{Z}_L$ is principal. So any ideal can be made principal after passing to some finite extension.

Proof (of lemma).

Let $m := \# \text{Cl}(\mathbb{Z}_K)$. Then $I^m = \alpha\mathbb{Z}_K$ is principal since m is the order of this group. Let $\beta := \sqrt[m]{\alpha} \in \mathbb{C}$ and let $L := K(\beta)$. Here β is an algebraic integer since it's an m th root of an algebraic integer. The claim is that $I\mathbb{Z}_L$ is principal. We have

$$\begin{aligned} (I\mathbb{Z}_L)^m &= I^m\mathbb{Z}_L \\ &= (\alpha\mathbb{Z}_K)\mathbb{Z}_L \\ &= \alpha\mathbb{Z}_L \\ &= \beta^m\mathbb{Z}_L \\ &= (\beta\mathbb{Z}_L)^m. \end{aligned}$$

But how can two ideals have the same m th power? By unique factorization, they must be the same, so $I\mathbb{Z}_L = \beta\mathbb{Z}_L$.

To be continued.



ToDos

List of Todos

Todo: definitions. 4

Definitions

2.2.4	Definition – Norm Map	5
3.1.2	Definition – Number Field	7
3.1.5	Definition – Real and Nonreal embeddings	8
3.2.2	Definition – Algebraic Numbers	9
3.2.6	Definition – \mathbb{Z}	9
3.3.1	Definition – Ring of Integers	12
4.1.2	Definition – Quadratic Number Fields	14
4.2.1	Definition – Norm and Trace	15
4.3.1	Definition – The Field Polynomial of an Element	16
5.2.2	Definition – Monoid	19
5.2.3	Definition – Terminology for Cancellative Monoids	19
5.2.7	Definition – Atomic	20
5.2.10	Definition – Reduced Monoid	21
5.2.18	Definition – Multiplication of Ideals	22
6.1.2	Definition – Euclidean Domain	24
6.1.6	Definition – Euclidean and Norm-Euclidean Number Fields	24
7.1.8	Definition – Standard Bases of Ideals	32
7.2.2	Definition – Norm of an ideal	33
8.2.4	Definition – Dilation of Ideals	37
8.3.2	Definition – Prime ideal above a prime number	40
9.1.2	Definition – Inert, Split, and Ramified Primes	41
10.3.2	Definition – Dilation Equivalence	50
10.3.4	Definition – Class Group	50
10.3.7	Definition – Class Number	50
11.3.1	Definition – Elasticity of a Ring	57
12.3.2	Definition – Lattice Point	63
13.2.1	Definition – Lattice	66
13.2.4	Definition – Full Lattices	68
13.2.5	Definition – Fundamental Parallelepiped	68
13.2.8	Definition – Covolume of a Lattice	70
14.1.2	Definition – Field Polynomial	73
14.1.8	Definition – Norm and Trace	74
14.2.2	Definition – Tuple Discriminant	75
14.4.1	Definition – Discriminant of a Number Field	78
15.1.1	Definition – Norm of an ideal	79
16.0.2	Definition – Cyclotomic Fields	84
16.1.2	Definition – Class Group of a Number Ring	88
17.2.2	Definition – Dedekind Domains	91
17.3.6	Definition – Extending Ideals	94

Theorems

3.1.4	Proposition – Degree equals number of embeddings for finite extensions	8
3.2.7	Theorem – $\bar{\mathbb{Z}}$ is a ring	9
3.2.9	Proposition – Integrality Criterion	10
3.3.3	Proposition – The ring of integers of \mathbb{Q} is \mathbb{Z}	12
3.3.5	Proposition – Easy criterion to check if an integer is algebraic	12
3.3.7	Proposition – $\text{ff}(\mathbb{Z}_K) = K$	13
3.3.10	Proposition – ?	13
4.1.4	Proposition – Quadratic fields are parameterized by squarefree integers	14
4.3.3	Proposition – The field polynomial detects integrality	16
4.4.1	Theorem – Classification of \mathbb{Z}_K for quadratic fields	17
5.2.8	Proposition – Monoids have unique factorization iff atomic and irreducibles are prime	20
5.2.12	Proposition – A monoid has unique factorizations iff its reduced monoid does	21
5.2.16	Theorem – Characterization of unique factorization monoids	21
5.2.20	Proposition – If R is a domain, then $\text{Id}(R)$ is a monoid	22
6.1.7	Proposition – Characterization of norm-Euclidean quadratic fields	24
6.2.4	Theorem – When quadratic fields are norm-Euclidean	28
6.2.7	Theorem – Motzkin	29
7.1.2	Theorem – Fundamental Theorem of Ideal Theory (for Quadratic Fields)	31
7.1.4	Proposition – Prime in monoids equals prime in rings for $\text{Id}(\mathbb{Z}_K)$	31
7.1.6	Proposition – $\text{Id}(\mathbb{Z}_K)$ has prime factorization	31
7.1.12	Proposition – Existence of a standard basis for an ideal	32
7.2.4	Proposition – Norms can be computed in terms of a basis with respect to τ	33
7.2.6	Theorem – The ideal that the norm generates	33
8.2.7	Proposition – The monoid $\text{Id}(\mathbb{Z}_K)$ is Cancellative	37
8.2.8	Theorem – To divide is to contain	38
8.2.11	Proposition – Unique Factorization	39
8.3.3	Theorem – Lying above unique primes	40
9.1.3	Theorem – Dedekind-Kummer, Prime Factorization Mirroring Theorem	42
9.1.7	Proposition – Characterization of inert/split/ramified primes	44
9.1.8	Proposition – Inert/Split/Ramified primes for quadratic fields	44
9.2.2	Proposition – Imaginary quadratic fields have at most 6 units	44
9.2.4	Proposition – Existence of the fundamental unit	45
9.2.11	Proposition – The log subgroup is discrete	45
10.1.2	Proposition – Subgroups of \mathbb{R} are either discrete or infinite cyclic	47
10.2.2	Theorem – Dirichlet's Approximation Theorem	47
10.3.10	Proposition – Class representatives of small norm	51
11.2.2	Theorem – Class number 1 iff UFD	55
11.2.4	Theorem – Carlitz	55
11.2.10	Theorem – Landau	57
11.3.3	Theorem – Elasticity in terms of the Davenport constant	57

12.1.2	Theorem – Rabinowitz	59
12.1.5	Theorem – When the class group is generated by small primes	60
12.2.2	Proposition – Almost Euclidean Domains	61
12.2.7	Theorem – Baker-Heegner-Stark	63
12.3.5	Theorem – The number of lattice points in a region is asymptotically the volume	64
13.1.2	Theorem – Lattice points with volume after scaling	65
13.1.4	Theorem – Minkowski, Version 1	65
13.2.7	Proposition – The volume of the fundamental parallelotope is a lattice invariant	69
13.2.9	Theorem – Minkowski (Version 2)	70
13.2.11	Theorem – 4 Square Theorem (Lagrange)	71
14.1.3	Proposition – The field polynomial is monic, has rational coefficients, and is a power of the minimal polynomial	73
14.1.7	Proposition – Field polynomial has integer coefficients iff the element is an integer	74
14.2.4	Theorem – The discriminant detects \mathbb{Q} -bases	76
14.3.1	Theorem – Integral Basis Theorem	76
14.4.4	Theorem – Hermite	78
14.4.6	Theorem – Dedekind	78
15.1.4	Proposition – Nonzero ideals have finite norms in rings of integers	80
15.1.5	Theorem – The norm is multiplicative	80
15.1.6	Theorem – Formula for norm of principal ideals	81
15.1.8	Proposition – Index = Determinant	81
16.0.4	Theorem – The ring of integers of a cyclotomic field is given by adjoining a primitive root of unity	84
16.0.7	Proposition – Eisenstein primes don't divide the extension degree	85
16.1.4	Proposition – Dilations of elements are always close to integers	88
16.1.6	Theorem – The class group is finite	88
17.1.11	Theorem – The monoid Id is a unique factorization monoid	91
17.2.3	Theorem – Noether	92
17.2.4	Proposition – Rings of integers are Dedekind domains	92
17.3.2	Theorem – The norm is multiplicative	92
17.3.8	Theorem – Norm is generated by product of conjugates	94
17.4.3	Theorem – Dedekind's theorem on the actuality of ideals	94

Exercises

3.3.9	Exercise – ?	13
3.3.12	Exercise – Prove the proposition.	13
4.4.3	Exercise – ?	17
8.2.14	Exercise – ?	40
11.3.4	Exercise – bounding the Davenport constant	58
17.3.4	Exercise – ?	93
17.3.7	Exercise – Arithmetic of ideals	94

Figures

List of Figures