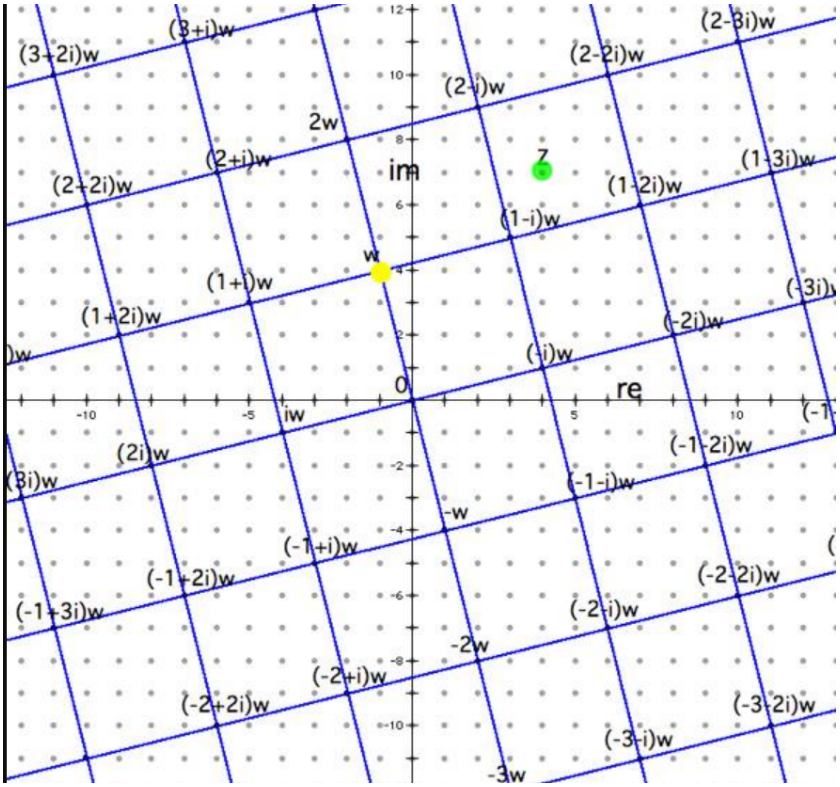


Notes: These are notes live-tex'd from a graduate course in Algebraic Number Theory taught by Paul Pollack at the University of Georgia in Spring 2021. As such, any errors or inaccuracies are almost certainly my own.

Algebraic Number Theory

Lectures by Paul Pollack. University of Georgia, Spring 2021

D. Zack Garza
University of Georgia
dzackgarza@gmail.com

Last updated: 2021-08-22

Table of Contents

Contents

1 Preface

See Youtube Video Playlist.

2 Notation

Todo: definitions.

- $U(\mathbb{Z}/k), (\mathbb{Z}/k)^\times$ denotes the group of
- $\mathbb{Z}/k$: the integers modulo k.
- $\overline{\mathbb{Z}}, \overline{\mathbb{Q}}$: the algebraic closures of $\mathbb{Z}, \mathbb{Q}$ respectively.
- K, L will generally denote fields, and most likely number fields (so extensions of $\mathbb{Q}$) $K/\mathbb{Q}$ will denote that K is a field extension of $\mathbb{Q}$, and $K/L/\mathbb{Q}$ denotes a tower of extensions K/L and $L/\mathbb{Q}$.
- $[K : \mathbb{Q}]$ is the degree of the extension $K/\mathbb{Q}$, i.e. the dimension of K as a $\mathbb{Q}$-vector space.
- $K(\alpha)$ will denote adjoining an element $\alpha \in \overline{K}$ to K to get a field extension $K(\alpha)/K$.
- $\mathbb{Z}_K \coloneqq \overline{\mathbb{Z}} \cap K$, the algebraic integers in K.
- $\mathrm{ff}(K)$ is the fraction field of K.
- $\mathsf{Ab}, \mathbb{Z}\text{-}\mathsf{Mod}$: the category of abelian groups.
- ζ_n will denote a primitive nth root of unity, so e.g. for n prime one can take $\zeta_n \coloneqq e^{\frac{2\pi i}{n}}$.
- $H \leq G$: H is a subgroup of G.

3 Diophantine Equations (Lec. 1, Thursday, January 14)

3.1 Intro/Logistics

See website for notes on books, intro to class.

- Youtube Playlist: https://www.youtube.com/playlist?list=PLA0xtXqOUji8fjQysx4k8a6h-hOZ7x5ue
- 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.*

3.2 Motivation

Remark 3.2.1: The main motivation: solving **Diophantine equations**, i.e. polynomial equations over $\mathbb{Z}$.

Example 3.2.2 ***(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: $1, 2, 4, 9, \cdots$. The only possibilities would be $x = 0, y = 1$, but in this case you can conclude $y = 0$.

Example 3.2.3 ***(Fermat):*** Consider $y^2 = x^3 - 2$.

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

Rewrite

$$\begin{aligned} x^3 = y^2 + 2 &= (y + \sqrt{-2})(y - \sqrt{-2}) \\ &\in \mathbb{Z}[\sqrt{-2}] \coloneqq \left\{ a + b\sqrt{-2} \;\middle|\; a, b, \in \mathbb{Z} \right\} \leq \mathbb{C}. \end{aligned}$$

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 3.2.4 ***(Norm Map)***

$$N\alpha \coloneqq \alpha\bar{\alpha} \qquad \text{for } \alpha \in \mathbb{Z}[\sqrt{-2}].$$

Lemma 3.2.5 *(?).*
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 $x^3 - 2 \equiv 0 - 2 \bmod 4 \equiv 2$, and so $y^2 \equiv 2 \bmod 4$. 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:

$$\mathbb{Z}[\sqrt{-2}]^\times = \left\{ a + b\sqrt{-2} \;\middle|\; a^2 + 2b^2 = 1 \right\}$$

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.

3.3 Failure of Unique Factorization

Example 3.3.1 ***(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 3.3.2
When does a ring admit unique factorization? Do you even *need* it?

Remark 3.3.3: 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!

4 Number Fields (Lec. 2,Tuesday, January 19)

4.1 Embeddings

Remark 4.1.1: 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 4.1.2 (Number Field)
A **number field** is a subfield $K \subseteq \mathbb{C}$ [a] such that $[K : \mathbb{Q}] < \infty$.

[a] Some 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 4.1.3 ***(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 4.1.4 ***(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 $\mathbb{C}$

[a] An **embedding** is an injective ring morphism.

Proof (of proposition).
We have $K/\mathbb{Q}$, which is necessarily separable since $\mathrm{ch}(\mathbb{Q}) = 0$. 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 4.1.5 (Real and Nonreal embeddings)
Let $K/\mathbb{Q}$ be a finite extension of degree $n = [K : \mathbb{Q}]$. We'll say an embedding $\sigma : K \to \mathbb{C}$ is **real** if $\sigma(K) \subseteq \mathbb{R}$, otherwise we'll say the embedding is **nonreal**.

Remark 4.1.6: 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 4.1.7 ***(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 $\sqrt[3]{2} \to \omega^j\sqrt[3]{2}$ 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.

4.2 Algebraic Closures

Remark 4.2.1: 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 4.2.2 (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 4.2.3: We know that if we define $\overline{\mathbb{Q}} \coloneqq \left\{\alpha \in \mathbb{C} \;\middle|\; \alpha \text{ is algebraic over } \mathbb{Q}\right\}$, we can alternatively describe this as $\overline{\mathbb{Q}} = \left\{\alpha \in \mathbb{C} \;\middle|\; [\mathbb{Q}(\alpha) : \mathbb{Q}] < \infty\right\}$. 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 4.2.4 ***(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 4.2.5: These are still fields, so lets define some interesting subrings.

Definition 4.2.6 ($\overline{\mathbb{Z}}$)
Define $\overline{\mathbb{Z}} \coloneqq \left\{\alpha \in \mathbb{C} \;\middle|\; \alpha \text{ is the root of a monic polynomial } f \in \mathbb{Z}[x]\right\}$.

Theorem 4.2.7 *($\overline{\mathbb{Z}}$ is a ring).*
$\overline{\mathbb{Z}}$ is a ring, and in fact a domain since it's a subring of $\mathbb{C}$.

Remark 4.2.8: We'll use an intermediate criterion to prove this:

Proposition 4.2.9 *(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 $\alpha \in \overline{\mathbb{Z}}$, 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 $\beta_1, \beta_2, \cdots, \beta_m$ 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

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

where $A \in \mathrm{Mat}(n \times m, \mathbb{Z})$. 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 $\det(xI - A)\Big|_{x=\alpha} = 0$. We have

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

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

- $1 \in \overline{\mathbb{Z}}$, which is true since $x - 1$ is monic.

- It's closed under addition $(+)$ and multiplication $(\cdot)$.

Note that the first property generalizes to $\mathbb{Z} \subseteq \overline{\mathbb{Z}}$, since $x - n$ is monic for any $n \in \mathbb{Z}$. For the second, let $\alpha, \beta \in \overline{\mathbb{Z}}$. Define $M \coloneqq \mathbb{Z}[\alpha, \beta]$, 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 $M \coloneqq \mathbb{Z}[\alpha, \beta]$, and the claim is that the following works: $\left\{\alpha^i \beta^j\right\}_{\substack{0 \leq i < n \\ 0 \leq j < m}}$, 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

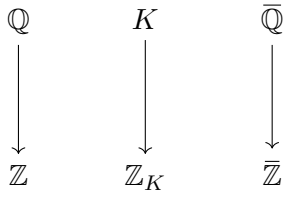
$$\alpha^I \beta^J = r(\alpha)r(\beta),$$

which is what we wanted.

■

■

Remark 4.2.10: We've just filled in another part of the previous picture:



4.3 Rings of Integers and Fraction Fields

Definition 4.3.1 (Ring of Integers)
Define $\mathbb{Z}_K = \overline{\mathbb{Z}} \cap K$, the **ring of integers** of K. Note that this makes sense since the intersection of rings is again a ring.

Remark 4.3.2: Why not just work in $\overline{\mathbb{Z}}$? It doesn't have the factorization properties we want, e.g. there are no irreducible elements. Consider $\sqrt{2}$, we can factor is 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 4.3.3 ***(The ring of integers of*** $\mathbb{Q}$ ***is*** $\mathbb{Z}$ ***).***
$\mathbb{Z}_{\mathbb{Q}} = \mathbb{Z}$.

Proof (of proposition).
$\subseteq$: Easy, since $\mathbb{Z} \subseteq \overline{\mathbb{Z}}$ and $\mathbb{Z} \subseteq \mathbb{Q}$, and is thus in their intersection $\mathbb{Z}_{\mathbb{Q}}$.

$\supseteq$: Let $\alpha \in \mathbb{Z}_{\mathbb{Q}} = \mathbb{Q} \cap \overline{\mathbb{Z}}$, so α is a root of $x^n - a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. 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 4.3.4: We'll want to study $\mathbb{Z}_K$ for various number fields K, but we'll need more groundwork.

Proposition 4.3.5 ***(Easy criterion to check if an integer is algebraic).***
Let $\alpha \in \overline{\mathbb{Q}}$, then

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

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

Proof (?).
$\Longleftarrow$: Trivial, if the minimal polynomial already has integer coefficients, just note that it's already monic and thus $\alpha \in \overline{\mathbb{Z}}$ by definition.

$\Longrightarrow$: 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 $\alpha \in \overline{\mathbb{Z}}$, and factor $f(x) = \prod_{i=1}^{n}(x - \alpha_i) \in \mathbb{C}[x]$. Note that each $\alpha_i \in \overline{\mathbb{Z}}$ 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 4.3.6 ***(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 4.3.7 ***(*** $\mathrm{ff}(\mathbb{Z}_K) = K$ ***).***

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 4.3.8: 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 4.3.9 (?)
Prove the proposition!

Proposition 4.3.10 ***(The ring*** $\overline{\mathbb{Z}}$ ***contains all roots of monic polynomials with integer coefficients).***
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 4.3.11: 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 4.3.12 (Prove the proposition.)
Prove this! One can use the integrality criterion (slightly challenging), or alternatively Galois theory.

5 Quadratic Fields (Lec. 3, Thursday, January 21)

Remark 5.0.1: 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.

5.1 Quadratic Number Fields

Remark 5.1.1: Simplest case: $\mathbb{Q}$, a degree 1 number field, so the next simplest case is degree 2.

Definition 5.1.2 (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 5.1.3: 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 5.1.4 ***(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.

[a] *Squarefree* 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: Well use some extra machinery.

■

5.2 Norm and Trace

Definition 5.2.1 (Norm and Trace)
Let K be a number field with $K_{/\mathbb{Q}}$ Galois. For each $\alpha \in K$ define

$$N(\alpha) \coloneqq \prod_{\sigma \in \mathsf{Gal}(K_{/\mathbb{Q}})} \sigma(\alpha) \qquad \text{the norm}$$

$$\mathrm{Tr}(\alpha) \coloneqq \sum_{\sigma \in \mathsf{Gal}(K_{/\mathbb{Q}})} \sigma(\alpha) \qquad \text{the trace.}$$

Remark 5.2.2: Why use these kind of sum at all? Applying any element in the Galois group just permutes the elements. Note that $N(\alpha), \mathrm{Tr}(\alpha)$ 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: $\mathrm{Tr}(a\alpha + b\beta) = a\,\mathrm{Tr}(\alpha) + b\,\mathrm{Tr}(\beta)$ for all $\alpha, \beta \in K$ and all $a, b \in \mathbb{Q}$.

Remark 5.2.3: What do the norm and trace look like for a quadratic field? We can write $K = \left\{ a + b\sqrt{d} \;\middle|\; a, b \in \mathbb{Q} \right\}$ and there is a unique (non-identity) element $g \in \mathsf{Gal}(K_{/\mathbb{Q}})$ with $\sigma(a + b\sqrt{d}) = a - b\sqrt{d}$. We'll refer to this automorphism as **conjugation**. We can compute

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

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 5.2.4: 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.

5.3 The Field Polynomial

Definition 5.3.1 (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

$$\varphi_\alpha(x) \coloneqq \prod_{\sigma \in \mathsf{Gal}(K_{/\mathbb{Q}})} (x - \sigma(\alpha)) .$$

Remark 5.3.2: 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 5.3.3 ***(The field polynomial detects integrality).***

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

Proof (of proposition).
$\Longleftarrow$: This is easy, since if φ_α is a monic polynomial with integer coefficients, meaning that α is an algebraic integer and thus in $\mathbb{Z}_K$.

$\Longrightarrow$: 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 $\sigma(\alpha) \in \overline{\mathbb{Z}}$. So $\varphi_\alpha(x) \in \overline{\mathbb{Z}}[x]$. We said φ_α has coefficients in $\mathbb{Q}$ too, and thus in $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$. So the problem is reduced to finding out when $\varphi_\alpha(x)$ has integer coefficients. If $\deg(K_{/\mathbb{Q}}) = n$, then

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

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 $\mathrm{Tr}(\alpha), N(\alpha) \in \mathbb{Z}$.

■

Example 5.3.4 ***(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 $\alpha \coloneqq \dfrac{1+\sqrt{5}}{2}$, then $N(\alpha) - 4/4 = -1$ and $\mathrm{Tr}(\alpha) = 1$. These are integers, so $\alpha \in \mathbb{Z}_K$, and in fact α is a root of $x^2 - x - 1 \in \mathbb{Z}[x]$.

5.4 Classification of $\mathbb{Z}_K$

Theorem 5.4.1 ***(Classification of $\mathbb{Z}_K$ for quadratic fields).***
Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic number field. Then

- If $d = 2, 3 \bmod 4$, then $\mathbb{Z}_K = \left\{ a + b\sqrt{d} \;\middle|\; a, b \in \mathbb{Z} \right\}$.
- If $d = 1 \bmod 4$, then $\mathbb{Z}_K = \left\{ \dfrac{1 + b\sqrt{d}}{2} \;\middle|\; a, b \in \mathbb{Z},\ a \equiv b \bmod 2 \right\}$.

Remark 5.4.2: 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 $N(\alpha), \mathrm{Tr}(\alpha) \in \mathbb{Z}$ for both cases.

Assuming now that $N(\alpha), \mathrm{Tr}(\alpha) \in \mathbb{Z}$, 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 $\mathrm{Tr}(\alpha) = 2A$, 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 $A, B \in \dfrac{1}{2}\mathbb{Z}$, 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 $(a')^2 \equiv d(b')^2 \bmod 4$. We proceed by cases.

Case 1: $d = 2, 3 \bmod 4$. If b' is odd then $(b')^2 = 1 \bmod 4$, which holds for any odd number. But then $(a')^2 = d(b')^2 = d \bmod 4$, which is a problem – squares modulo 4 can only be 0 or 1. This is a contradiction, so b' must be even. Then $(b')^2 \bmod 4 = 0$, which forces $a' \equiv 0 \bmod 4$ 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 $d \equiv 1 \bmod 4$, then $(a')^2 \equiv (b')^2 \bmod 4$. We can conclude that a', b' are either both odd or both even, otherwise we'd get $0 \equiv 1 \bmod 4$, and thus we can write $a' \equiv b' \bmod 2$. But this was exactly the condition appearing in the theorem.

■

Remark 5.4.4: Let K be a quadratic number field. Then we can reformulate the previous results as:

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

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

Remark 5.4.5: 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, the it's not always true that $\mathbb{Z}_K = \mathbb{Z}[\ell]$ for ℓ a single element.

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

6.1 Revisiting a Counterexample to Unique Factorization

Remark 6.1.1: 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):

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

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 6.1.2 ***(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 $\bmod 5$ yields $2 \equiv a^2$, but 2 is not a square in $\mathbb{Z}/5\mathbb{Z}$. ↯

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.

6.2 Factorization Theory

Remark 6.2.1: 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 6.2.2 (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 6.2.3 (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 a unit and whenever $\pi = \alpha\beta$ then either α or β is a unit.

[1] $\Longleftarrow$: 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 6.2.4: 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 6.2.5
How do you show something is a UFD?

Answer 6.2.6
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 6.2.7 (Atomic)
For M a cancellative monoid, M is **atomic** if every nonunit element of M is a product of irreducibles.

Proposition 6.2.8 ***(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 6.2.9: 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 6.2.10 (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 6.2.11 ***(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 6.2.12 ***(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 6.2.13: What did this buy us? We didn't have to worry about associates in the above statement, and the only unit is 1.

Remark 6.2.14: Why isn't $\mathbb{Z}[\sqrt{-5}]$ is UFD? It doesn't have enough elements to make unique factorization work!

Example 6.2.15 ***(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 6.2.16 ***(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

$$\begin{aligned} \alpha &= \rho\sigma \\ \beta &= \tau\nu \\ \gamma &= \rho\tau \\ \delta &= \sigma\nu. \end{aligned}$$

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 6.2.17: Let $M_{\text{red}} := \left(\mathbb{Z}[\sqrt{5}] \setminus \{0\}\right)_{\text{red}}$, 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 a 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

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

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

$$IJ \coloneqq \left\langle \left\{ \alpha_i\beta_i \;\middle|\; \alpha_i \in I, \beta_i \in J \right\} \right\rangle = \left\{ \sum \alpha_i\beta_i \;\middle|\; \alpha_i \in I, \beta_i \in J \right\}.$$

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

Remark 6.2.19: Note that the naive definition $IJ \coloneqq \left\{ ij \;\middle|\; i \in I, j \in J \right\}$ is not necessarily an ideal, since it may not be closed under addition. Taking the smallest ideal containing all products fixes this.

Proposition 6.2.20 ***(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 $I = \langle \alpha_1, \cdots, \alpha_j\rangle$ and $J = \langle \beta_1, \cdots, \beta_k\rangle$ then $IJ = \langle \alpha_1\beta_1, \cdots, \alpha_j\beta_k\rangle$ 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 6.2.21: 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

- $I \coloneqq \left\langle 1+\sqrt{-5}, 2\right\rangle$
- $I' \coloneqq \left\langle 1-\sqrt{-5}, 2\right\rangle$
- $J \coloneqq \left\langle 1+\sqrt{-5}, 3\right\rangle$

- $J' \coloneqq \left\langle 1-\sqrt{-5}, 3\right\rangle$

Then

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

We can then write

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

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

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

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.

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

7.1 Setup

Remark 7.1.1: 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 7.1.2 (Euclidean Domain)
A domain R is **Euclidean** if and only if there is a function $\varphi R \setminus \{0\} \to \mathbb{Z}^{\geq 0}$ 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 7.1.3 ***(Examples of Euclidean functions):***

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

Remark 7.1.4: 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 7.1.5
Which quadratic fields K have a Euclidean ring of integers $\mathbb{Z}_K$?

Definition 7.1.6 (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 $\varphi(-) \coloneqq |N(-)|$.

Proposition 7.1.7 ***(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).
$\Longleftarrow$: Let $a, b \in \mathbb{Z}_k$ with $b \neq 0$. Define $\beta \coloneqq a/b \in K$, 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 $N(-), |-|$ are multiplicative, we have

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

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

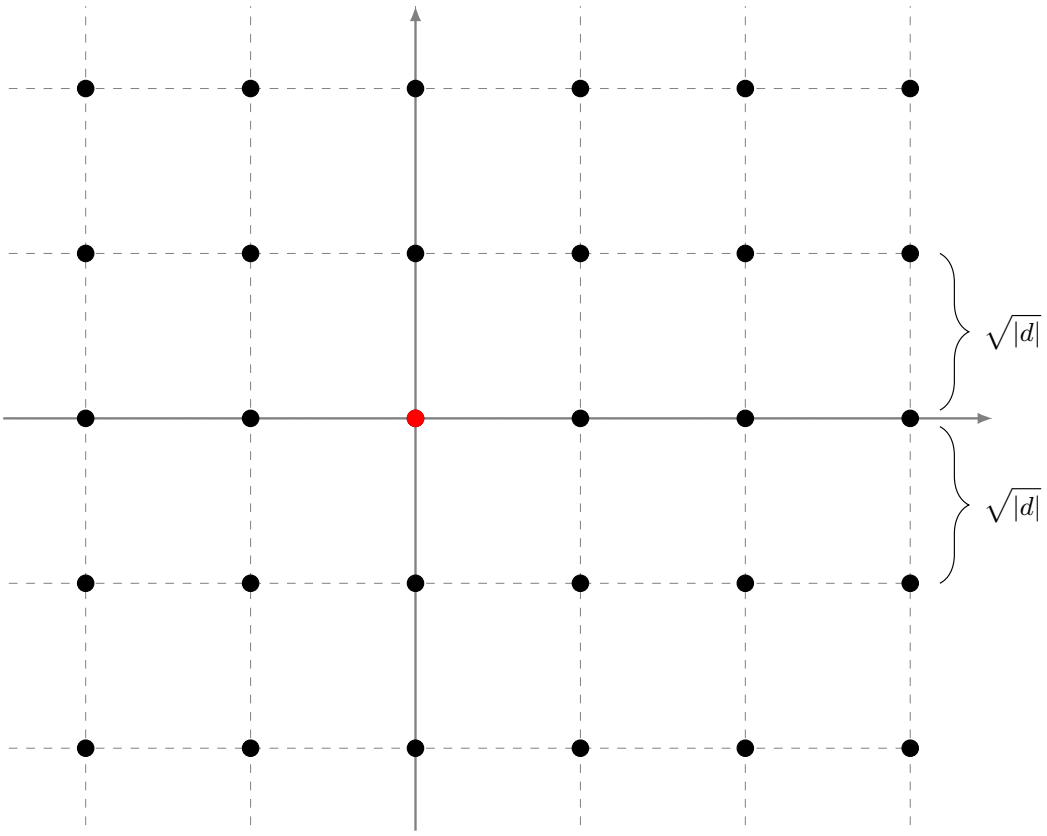
■

7.2 Norm-Euclidean Imaginary Quadratic Fields

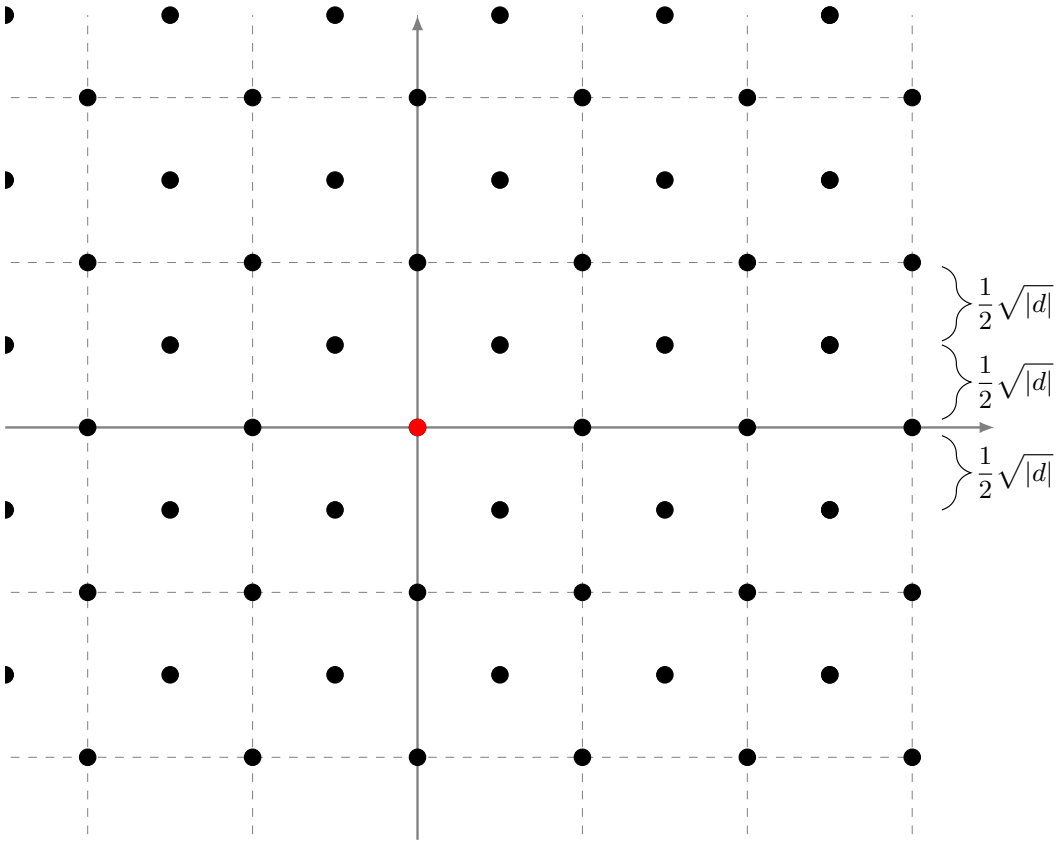
Remark 7.2.1: Suppose $K = \mathbb{Q}(\sqrt{d})$ with $d < 0$ squarefree, so we can write

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

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 $d = 2, 3 \bmod 4$ then $\mathbb{Z}_K = \left\{ a + b\sqrt{d} \;\middle|\; a, b, \in \mathbb{Z} \right\}$:

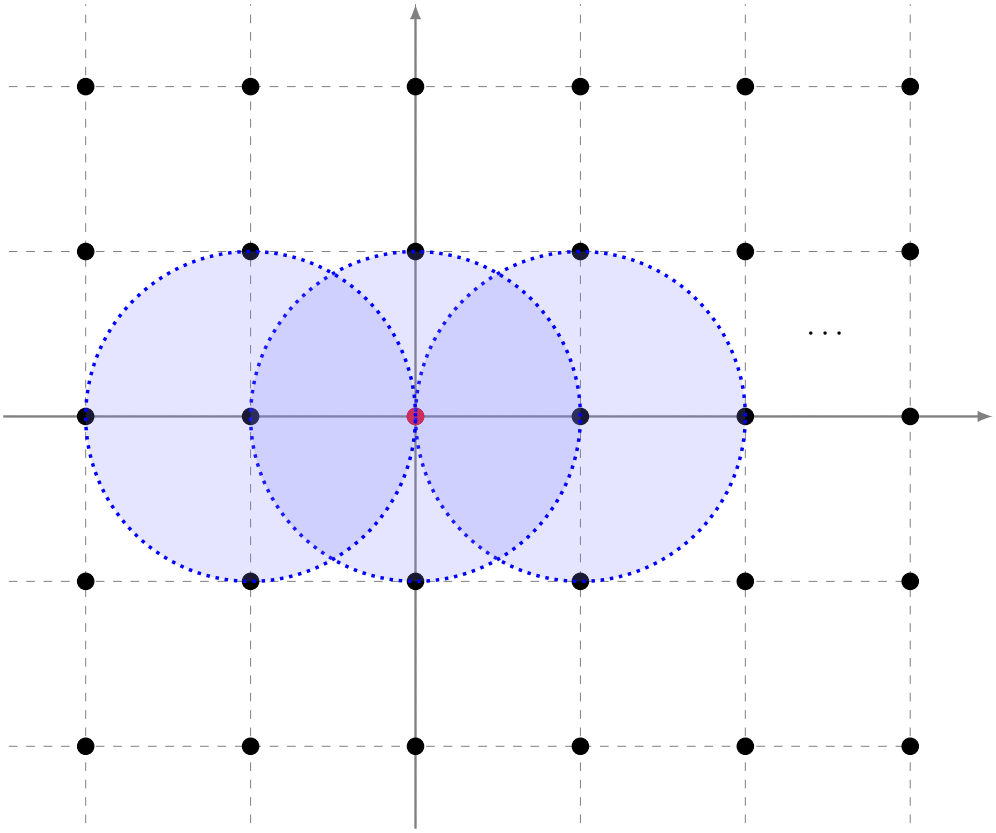


When $d \equiv 1 \bmod 4$, we have $\mathbb{Z}_k = \left\{ \frac{1}{2}(a + b\sqrt{d}) \;\middle|\; a, b, \in \mathbb{Z},\ a \equiv b \bmod 2 \right\}$. On the real axis, if $b = 0$ then a is an even integer and $\{(1/2)a\}$ is all integers. To get the remaining elements, we don't just shift up and down: setting $b = 1$ yields elements that look like $(1/2)a + \sqrt{d}$ where a is odd, so we get the following:

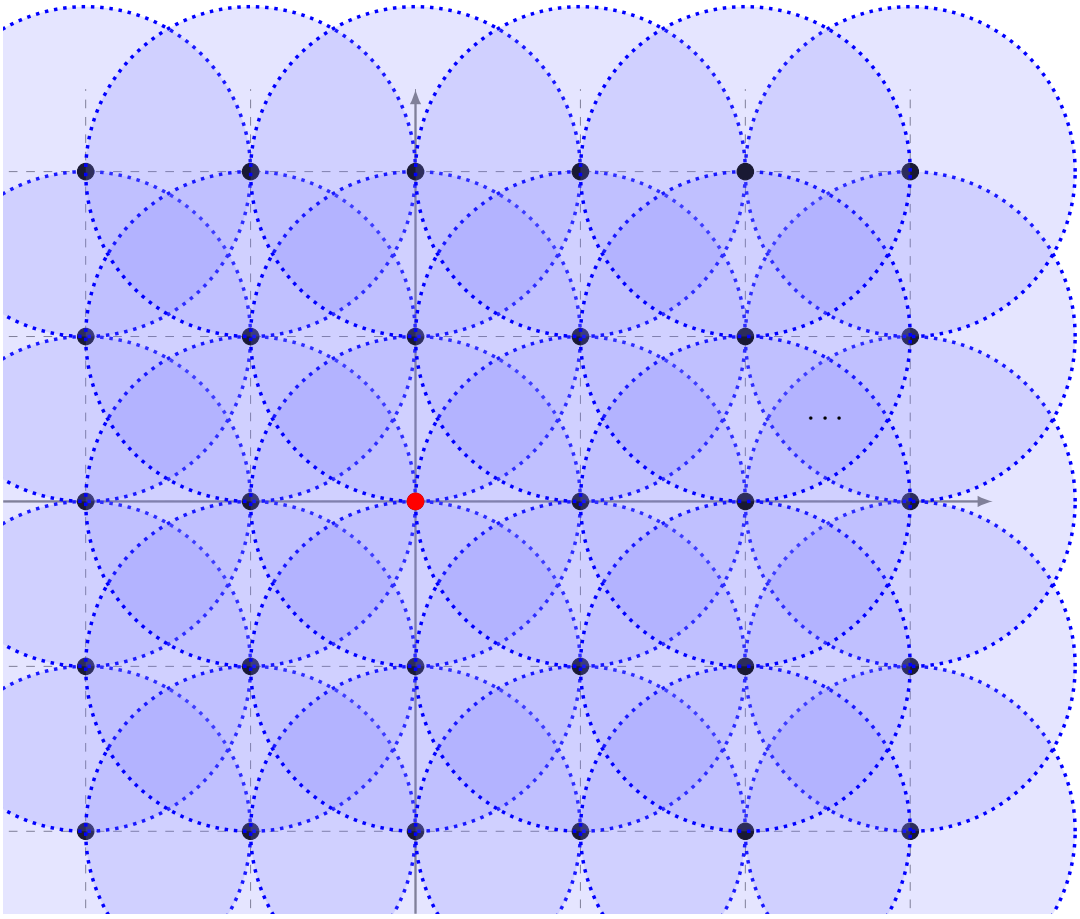


Now we can think of the criterion for an imaginary quadratic field to be norm-Euclidean: what does it mean to be within norm 1 of an element of $\mathbb{Z}_K$? If $z \in K$, we can write $N(z) = z\bar{z} = |z|^2$, and thus reformulate our criterion: K is norm-Euclidean if and only if for all $\beta \in K$ 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 7.2.2 ***(?):*** $\mathbb{Q}(i)$ 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 7.2.3: 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 7.2.4 ***(When quadratic fields are norm-Euclidean).***
K is norm-Euclidean if and only if $d \in \{-1, -2, -3, -7, -11\}$.

Corollary 7.2.5 ***(When rings of integers are PIDs/UFDs).***
For these d, $\mathbb{Z}_K$ is a PID and thus a UFD.

Remark 7.2.6: So we've classified all norm-Euclidean imaginary quadratic fields. What about removing the word "norm"? We restricted to $|N(-)|$ 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 7.2.7 ***(Motzkin).***
For K an imaginary quadratic field, K is Euclidean if and only if $d \in \{-1, -2, -3, -7, -11\}$.

Remark 7.2.8: 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 $-19 \equiv 1 \bmod 4$, 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 7.2.9: We'll prove this theorem! First we need a few lemmas.

Lemma 7.2.10 ***(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 $d = 2, 3 \bmod 4$, 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 $d \equiv 1 \bmod 4$. 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 $1 \bmod 4$, 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 7.2.11: 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 7.2.12 ***(Norm of generator of principal ideal equals size of quotient).*** Let K be any quadratic field and $\alpha \in \mathbb{Z}_K$. Then $\#\mathbb{Z}_k / \langle \alpha \rangle = |N(\alpha)|$.

7.3 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 mod β, we obtain $\alpha = \rho \bmod \beta$, 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 $d = 2, 3 \bmod 4$ then $\beta = a + b\sqrt{d}$ with $a, b \in ZZ$ 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 $d \equiv 1 \bmod 4$, then $\beta = \dfrac{a + b\sqrt{d}}{2}$ where $a, b \in \mathbb{Z}$, $a \equiv b \bmod 2$. Then

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

Now considering that $-d \equiv 1 \bmod 4 \implies -d \in \{-3, -7, -11, \cdots\}$, 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 7.3.1: 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 $K \coloneqq \mathbb{Q}(\sqrt{d})$ is not norm-Euclidean. What are the Euclidean real quadratic fields? The situation is much different, and there are two open conjectures.

Conjecture 7.3.2.
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 7.3.3.
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 7.3.4: 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.

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

8.1 Prime Factorization in $\mathrm{Id}(\mathbb{Z}_K)$

Remark 8.1.1: Today: roughly chapter 6. Recall that if R is a domain, we defined $\mathrm{Id}(R)$ as the set of nonzero ideals of R, which is a monoid. We want to get to the following theorem:

Theorem 8.1.2 ***(Fundamental Theorem of Ideal Theory (for Quadratic Fields)).***
Let K be a quadratic field, then $\mathrm{Id}(\mathbb{Z}_K)$ is a UFM.

Remark 8.1.3: 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 8.1.4 ***(Prime in monoids equals prime in rings for*** $\mathrm{Id}(\mathbb{Z}_K)$***).***
"Prime" in the usual ring-theoretic sense is equivalent to "prime" in the monoidal sense for $\mathrm{Id}(\mathbb{Z}_K)$.

Remark 8.1.5: Recall though that $\mathrm{Id}(\mathbb{Z}_K)$ 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 8.1.6 ***(*** $\mathrm{Id}(\mathbb{Z}_K)$ ***has prime factorization).***
Every nonzero ideal of $\mathbb{Z}_K$ factors uniquely as a product of prime ideals in $\mathbb{Z}_K$.

Remark 8.1.7: Can we explicitly understand what ideals of $\mathbb{Z}_K$ look like for quadratic fields?

Definition 8.1.8 (Standard Bases of Ideals)
Let $K = \mathbb{Q}(\sqrt{d})$, so $\mathbb{Z}_K = \mathbb{Z}[\sqrt{d}]$ if $d = 2, 3 \bmod 4$ or $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ if $d = 1 \bmod 4$. Define $\tau = \sqrt{d}$ or $(1+\sqrt{d})/2$ accordingly and write $\mathbb{Z}_k = \mathbb{Z}[\tau]$.

Remark 8.1.9: 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 8.1.10 ***(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 $b \coloneqq N\alpha(\tau) \in I$.

■

Remark 8.1.11: We wanted a nice description of bases for ideals – here it is!

Proposition 8.1.12 ***(Existence of a standard basis for an ideal).***
Let $I \trianglelefteq \mathbb{Z}_K$ 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 $\left\{b \in \mathbb{Z} \;\middle|\; a + b\tau \in I \text{ for some } a \in \mathbb{Z}\right\} = B\mathbb{Z}$.[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

[a] Why 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 its 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.

[b] The 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 8.1.13: Note that this is only determined up to $A \bmod n$.

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 $1, \tau$.

■

8.2 Ideal Norms

Remark 8.2.1: 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 8.2.2 (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 8.2.3: 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 8.2.4 ***(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 $\left\{ a + b\tau \;\middle|\; 0 \leq a \leq n,\, 0 \leq b \leq B \right\}$ is a complete and irredundant set of representatives for $\mathbb{Z}_K / I$.

■

Remark 8.2.5: 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 8.2.6 ***(The ideal that the norm generates).***
Let $I \trianglelefteq \mathbb{Z}_K$ be nonzero and define $\bar{I} = \left\{ \bar{\alpha} \;\middle|\; \alpha \in I \right\} \trianglelefteq \mathbb{Z}_K$. Then $I\bar{I} = \langle N(I) \rangle$.

Lemma 8.2.7 ***(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 $(x-\tau)(x-\bar{\tau}) = x^2 - \operatorname{Tr}(\tau)x + N(\tau)$, and thus we can write

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

Substituting yields

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

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

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

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 $BN(A'+gt) \in \langle B\rangle\langle A'+\tau, n'\rangle = I$. 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

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

We can now note that $B^2n' = B^2(n/B) = nB = N(I)$. 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 $(A'+\bar{\tau})+(A'+\tau) = \mathrm{Tr}(A'+\tau)$. So let

$$J \coloneqq \langle n, N(A'+\tau)/n', \mathrm{Tr}(A'+\tau)\rangle \trianglelefteq \mathbb{Z},$$

then it's enough to show $J = \langle 1\rangle \trianglelefteq \mathbb{Z}$. 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 $\alpha \coloneqq (A'+\tau)/d \in K$. Taking the trace is $\mathbb{Q}$-linear, so $\mathrm{Tr}(\alpha) = (1/d)\,\mathrm{Tr}(A'+\tau) \in \mathbb{Z}$. This follows because the trace $\mathrm{Tr}(A'+\tau)$ 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 $N(A'+\tau)/n', \mathrm{Tr}(A'+\tau)$ 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 $N\alpha, \mathrm{Tr}\,\alpha \in \mathbb{Z}$, which forces $\alpha \in \mathbb{Z}_K$ since α is a root of $x^2 - \mathrm{Tr}(\alpha) + N\alpha$. 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 8.2.8: 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.

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

9.1 Norms: Multiplicativity and Computations

Remark 9.1.1: 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

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

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 $I \trianglelefteq \mathbb{Z}_K$ 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 9.1.2 ***(The norm is multiplicative).***
Let $I, J \trianglelefteq \mathbb{Z}_K$ be nonzero, then $N(IJ) = N(I)N(J)$.

Proof (of corollary).
Note that $IJ\overline{I}\overline{J} = \langle N(IJ)\rangle$ 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 9.1.3: 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 9.1.4 ***(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 $N(\langle\alpha\rangle = \pm N\alpha$.

■

9.2 Unique Factorization for Ideals

Lemma 9.2.1 ***(Principal Multiple Lemma).***
Let $I \trianglelefteq \mathbb{Z}_K \setminus \{0\}$, then there is another ideal $\tilde{I} \trianglelefteq \mathbb{Z}_K \setminus \{0\}$ such that $I\tilde{I}$ is principal.

Proof (of Principal Multiple Lemma).
Take $\tilde{I} \coloneqq \bar{I}$, since we proved that this is principal and generated by the norm.
■

Remark 9.2.2: 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 9.2.3 ***(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 9.2.4 (Dilation of Ideals)
If $I \trianglelefteq \mathbb{Z}_K$, for any $\alpha \in K$ define

$$\alpha I \coloneqq \left\{ \alpha\beta \;\middle|\; \beta \in I \right\},$$

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 9.2.5: 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 $I \coloneqq 2\mathbb{Z}$ take $\alpha \coloneqq 1/5$. 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 9.2.6: This was the easy case, when I was principal. What if I is not principal?

Proposition 9.2.7 ***(The monoid*** $\mathrm{Id}(\mathbb{Z}_K)$ ***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.
■

9.2.1 Proving Unique Factorization

Theorem 9.2.8 ***(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 $\tilde{I}H \subseteq \langle \alpha \rangle$. 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 9.2.9: We now want to prove that $\mathrm{Id}(\mathbb{Z}_K)$ 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 9.2.10: We'll use the fact that $\mathrm{Id}(\mathbb{Z}_K)$ 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 9.2.11 ***(Unique Factorization).***

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

Remark 9.2.12: 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. ↯

■

Proof (of 2: Euclid's Lemma).
Suppose P is irreducible in $\mathrm{Id}(\mathbb{Z}_K)$ 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 9.2.13: Now running the exact same proof as for $\mathbb{Z}$ yields unique factorization.

Exercise 9.2.14 (?)
Let P be a nonzero ideal of $\mathrm{Id}(\mathbb{Z}_K)$, then P is monoidally prime in $\mathrm{Id}(\mathbb{Z}_K)$ if and only if P is prime in the usual sense of prime ideals.

Hint: use "to divide is to contain".

9.3 Preview: Ramification

Remark 9.3.1: 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 9.3.2 (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 9.3.3 ***(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 $P \cap Z \neq \{0\}$, 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 9.3.4: 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 $\mathbb{Z}_K$?

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

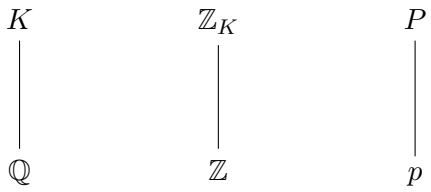
10.1 Dedekind-Kummer Mirroring

Remark 10.1.1: Today: chapter 7. Let K be a quadratic number field. Recall that if $P \trianglelefteq \mathbb{Z}_K$ 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 10.1.2 ***(Inert, Split, and Ramified Primes)***

a. $g = 1$ and $P_1 = \langle g \rangle$ and $\langle p \rangle$ is prime. In this case we say p **is inert**.

b. If $g = 2$ and $P_1 \neq P_2$, then we say p **is split**.

c. 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:

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

Theorem 10.1.3 ***(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 irreducibles, then p is inert. Otherwise,

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

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

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

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

Example 10.1.4 ***(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,

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

We also have

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

which is the split case, so

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

Taken mod 5, we have

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

so

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

Similarly,

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

so $\langle 11\rangle$ is inert.

Lemma 10.1.5 ***(Characterization of $\mathbb{Z}_K$ as a quotient of a polynomial ring).*** There is a surjective morphism

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

so by the first isomorphism theorem,

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

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 $\mathbb{Z}[x] / \left\langle \min_\tau(x), p\right\rangle \cong$

$\mathbb{F}_p[x]/\left\langle \min_\tau(x) \bmod p \right\rangle$. In this case, if $\min_\tau$ 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

$$\min_\tau(x) = (x-a)(x-b) \bmod p.$$

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

$$\begin{aligned}
\mathbb{Z}_K/P^1 &\cong \frac{\mathbb{Z}[x]/\langle \min_\tau(x) \rangle}{\langle p, x-a \rangle} \\
&\cong \mathbb{Z}/p\mathbb{Z}[x]/\left\langle \min_\tau(x), x-a \right\rangle \\
&\cong \mathbb{Z}/p\mathbb{Z}[x]/\left\langle \min_\tau(x), x-a \right\rangle \\
&\cong \mathbb{Z}/p\mathbb{Z}[x]/\langle x-a \rangle && \text{since } x-a \mid \min_\tau(x) \\
&\cong \mathbb{Z}/p\mathbb{Z}.
\end{aligned}$$

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

$$P_1P_2 = \langle p, p(\tau-a), p(\tau-b), (\tau-a)(\tau-b) \rangle .$$

Note that

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

for some $G \in \mathbb{Z}[x]$. Plugging in τ, the LHS is zero, while on the RHS yields $\cdots + pG(\tau)$. 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 $P_1P_2 \subseteq \langle p \rangle$ and $\langle p \rangle \mid P_1P_2$. Write $P_1P_2 = \langle p \rangle I$ 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 $p^2N(I)$ which forces $N(I) = 1 \iff I = \langle 1 \rangle = \mathbb{Z}_K$ (the entire ring)

We now want to show $P_1 = P_2 \iff a \equiv b \bmod p$. 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 $a \not\equiv b \bmod p$, 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 $a \equiv b \bmod p$.

■

Question 10.1.6
Can we be more explicit about how $\min_\tau$ factors?

Proposition 10.1.7 ***(Characterization of inert/split/ramified primes).***
Let p be an odd prime, then

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

Proposition 10.1.8 ***(Inert/Split/Ramified primes for quadratic fields).***

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

Remark 10.1.9: The proof follows from looking at how $\min_\tau(x)$ factors $\bmod 2$, and there aren't many possibilities.

10.2 Units in $\mathbb{Z}_K$

Remark 10.2.1: Roughly chapter 8. For the imaginary quadratic case, we can write down the unit group explicitly.

Proposition 10.2.2 ***(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 10.2.3: "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 10.2.4 ***(Existence of the fundamental unit).***
Suppose $d > 0$, then there is a unit $\epsilon_0 > 1 \in \mathbb{Z}_K$ such that $U(\mathbb{Z}_K) = \left\{ \pm \epsilon_0^k \;\middle|\; k \in \mathbb{Z} \right\}$. Moreover ϵ_0 is unique, and we'll refer to this as the **fundamental unit**.

Corollary 10.2.5 ***(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 10.2.6: Here the $\mathbb{Z}/2\mathbb{Z}$ corresponds to the $\pm$ and the $\mathbb{Z}$ to the exponent.

Example 10.2.7 ***(of the fundamental unit):***

- For $d = 2$, we have $\varepsilon_0 = 1 + \sqrt{2}$. This is a unit because it has inverse $\sqrt{2} - 1$.
- For $d = 43$, it turns out that $\varepsilon_0 = 531\sqrt{43}$.

Lemma 10.2.8 ***(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 10.2.9: Note that norms were positive in the imaginary quadratic case, but can be negative for real quadratics.

Proof (of computation of norm).
$\Longleftarrow$: This means $\epsilon\bar{\epsilon} = \pm 1$, so one of $\pm\bar{\epsilon}$ is the inverse.
$\Longrightarrow$: Write $\epsilon\epsilon^{-1} = 1$ and take norms of both sides.
■

Remark 10.2.10: Our strategy: show that the group of positive units $U(\mathbb{Z}_K)^+$ is infinite cyclic. If we get a generator $\varepsilon_0 > 1$, replace it with its reciprocal, and note that we don't want $\varepsilon_) = 1$ 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

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

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

Proposition 10.2.11 ***(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 $\log(\varepsilon)$ 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 10.2.12
What do the discrete subgroups of $\mathbb{G}_a(\mathbb{R})$ look like?

Answer 10.2.13
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.

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

11.1 Review

Remark 11.1.1: Today: chapter 8. We'll continue with the statements from last time:

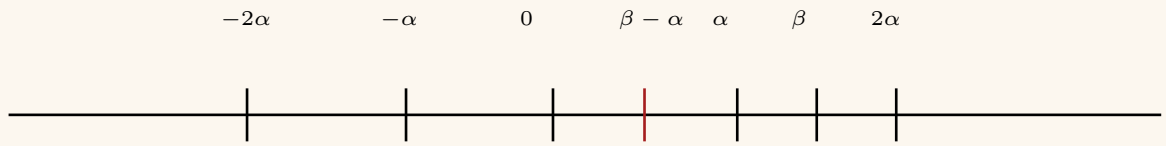
Proposition 11.1.2 ***(Subgroups of $\mathbb{R}$ are either discrete or infinite cyclic).***
A discrete subgroup $\Lambda \leq \mathbb{R}$ is either 0 or infinite cyclic, where *discrete* means having finite intersection with every interval $[-x, x]$.

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 11.1.3: 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 $\epsilon \neq 1$.

11.2 An Aside: Diophantine approximation

Remark 11.2.1: 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 11.2.2 ***(Dirichlet's Approximation Theorem).***
There is a $q \leq Q \in \mathbb{Z}^+$ with

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

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

Remark 11.2.3: 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 $\{qa\} \coloneqq qa - \lfloor qa \rfloor \in [0,1)$. 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

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

for all 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 $q \coloneqq q_2 - q_1$. 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 11.2.4 ***(Infinitude of elements of bounded norm).***
There are infinitely many pairs of positive integers (p, q) such that

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

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

Remark 11.2.5: 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

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

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

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

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

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

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 ay most *finitely* many starting values for Q. Pick a Q, then produce q satisfying the bound. Then $\left\|q\sqrt{d}\right\| \neq 0$ 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

$$\left\|q\sqrt{d}\right\| \leq \frac{1}{Q+1} \overset{Q\to\infty}{\to} 0,$$

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

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

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

Lemma 11.2.7 ***(Finitely many ideals of bounded norm).***
For all real $x > 0$ there are finitely many nonzero ideals $I \trianglelefteq \mathbb{Z}_K$ with $N(I) \coloneqq |\mathbb{Z}_K/I| \leq x$.

Proof (of lemma).
Suppose $N(I) \coloneqq m \leq x$ 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 $m = 1 + 1 + \cdots + 1$, 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 $I_{p,q} \coloneqq \left\langle p + q\sqrt{d} \right\rangle$ where (p, q) is a pair of positive integers such that $\left|p^2 - dq^2\right| < 1 + 2\sqrt{d}$. 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 $\left\langle p + q\sqrt{d} \right\rangle = \left\langle p' + q'\sqrt{d} \right\rangle$. If two ideals are equal, the generators differ by a unit, and so

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

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 11.2.8: 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 11.2.9 ***(of the fundamental unit):*** Take $d = 2$, what is ε_0? We have $U(\mathbb{Z}_K) = \left\{\pm\varepsilon_0^k \;\middle|\; k \in \mathbb{Z}\right\}$, 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 $\varepsilon_0 = 1 + \sqrt{2}$.

11.3 Class Groups and the Class Number

Remark 11.3.1: This is now chapter 9. Let K be a quadratic field.

Definition 11.3.2 (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 11.3.3: It's easy to check that this is an equivalence relation, so we'll use $I \approx J$.

Definition 11.3.4 (Class Group)
The **class group** of $\mathbb{Z}_K$ is defined as

$$\mathrm{Cl}(\mathbb{Z}_K) \coloneqq \mathrm{Id}(\mathbb{Z}_K)/\approx .$$

Remark 11.3.5: 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 11.3.6: This is an abelian group, wouldn't it be nice if it were finite? This is one of the big theorems of number theory: $\mathrm{Cl}(\mathbb{Z}_K)$ is finite. We can thus define the following:

Definition 11.3.7 (Class Number)
The **class number** of K is defined as:

$$h_k \coloneqq |\mathrm{Cl}(\mathbb{Z}_K)|.$$

Lemma 11.3.8 ***(Comparison bound between element norm and ideal norm).***
There is a constant C depending on K such that for every $I \in \mathrm{Id}(\mathbb{Z}_K)$ there is a nonzero $\alpha \in I$ such that

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

In fact, one can take

$$C \coloneqq 1 + \mathrm{Tr}(\tau) + |N(\tau)|.$$

Remark 11.3.9: 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:

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

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

■

Proposition 11.3.10 ***(Class representatives of small norm).***
Every ideal class contains an ideal I of norm $N(I) \leq C$.

Corollary 11.3.11 ***(Class numbers are finite).***
$h_K < \infty$.

Remark 11.3.12: 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 $I \in \mathrm{Id}(\mathbb{Z}_K)$, 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 11.3.13 ***(?):*** What we'll look at next: $\mathrm{Cl}(\mathbb{Z}[\sqrt{-5}])$. 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 lets 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*:

- $\langle 2\rangle = P_1^2$, $P_1 \coloneqq \left\langle 2, 1+\sqrt{-5}\right\rangle$
- $\langle 3\rangle = P_2P_3, P_2 \coloneqq \left\langle 3, 1-\sqrt{-5}\right\rangle, P_3 \coloneqq \left\langle 1+\sqrt{-5}\right\rangle$
- $\langle 5\rangle = P_4^2, P_4 \coloneqq \left\langle \sqrt{-5}\right\rangle$

This allows us to conclude that

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

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

12 Class Groups (Lec. 10, Thursday, February 18)

12.1 Computing Class Groups

Remark 12.1.1: 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**

$$\mathrm{Cl}(\mathbb{Z}_K) \coloneqq \mathrm{Id}(\mathbb{Z}_K)/\approx\,.$$

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 12.1.2 ***(Computing the Class Group):*** Let $K = \mathbb{Q}(d)$ where $d \coloneqq \sqrt{-5}$. 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

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

We conclude that $\mathrm{Cl}(\mathbb{Z}_K) = \langle P_1, \cdots, P_4 \rangle$. What are the relations? Consider P_4, and note that $\left\langle \sqrt{-5} \right\rangle \approx \langle 1 \rangle$ 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

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

and so these are inverses and we can get rid of P_3. So $\mathrm{Cl}(\mathbb{Z}_K) = \langle [P_1] \rangle$, which is a cyclic group. The generator has to have order 1 or 2, since $P_1^2 = \langle 1 \rangle$. 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 $I \in \mathrm{Id}(\mathbb{Z}_K)$ 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 $\mathrm{Cl}(\mathbb{Z}_K) \cong \mathbb{G}_a(\mathbb{Z}/2\mathbb{Z})$.

Remark 12.1.3: What is the class group useful for? We'll tie this into Diophantine equations.

Example 12.1.4*(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 $\mathrm{Id}(\mathbb{Z}_K)$, 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:

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

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, $N(P) \mid N(\left\langle y+\sqrt{-5} \right\rangle) = y^2 + 5$. We also know P contains both factors,

so it contains $(y+\sqrt{-5})-(y-\sqrt{-5}) = 2\sqrt{-5}$, so $N(P) \mid N(\left\langle 2\sqrt{-5}\right\rangle) = 20$. 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 $1 \bmod 8$, so $y^2+5 \equiv 6 \bmod 8$, which is not a cube in $\mathbb{Z}/8$ since any cube is $0 \bmod 8$.
- 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 $N(P) \mid 1$, forcing $P = \langle 1\rangle$, a contradiction. ■

Thus we can write

$$\left\langle y+\sqrt{-5}\right\rangle = I^3$$
$$\left\langle y-\sqrt{-5}\right\rangle = J^3.$$

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 $\mathrm{Cl}(\mathbb{Z}_K) \cong \mathbb{G}_a(\mathbb{Z}/2\mathbb{Z})$, so this can only happen if $[I] = [J] = e$ and I, J must be principal. So we can write $I = \left\langle a+b\sqrt{-5}\right\rangle$ for some $a, b \in \mathbb{Z}$. Thus

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

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 12.1.5: 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.

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

Remark 12.2.1: 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 12.2.2 ***(Class number 1 iff UFD).***

Recall that the class number is defined as $h_K \coloneqq \#\mathrm{Cl}(\mathbb{Z}_K)$. 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 12.2.3
Can anything be said if $h_K = 2$, even though we know $\mathbb{Z}_K$ is not a UFD?

Theorem 12.2.4 ***(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 12.2.5: 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 12.2.6 ***(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 $P_1P_2 = \langle\omega\rangle$ 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:

$$\langle\pi\rangle = (P_1P_2)P_3\cdots P_g = \langle\pi\rangle\, P_3\cdots P_g$$
$$\implies \langle 1\rangle = P_3\cdots P_g,$$

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 12.2.7*(?):* Much like the previous example, we have

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

Suppose that P factors as

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

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 12.2.9: See the book for the other direction!

Theorem 12.2.10*(Landau).*
Every ideal class contains infinitely many prime ideals.

Remark 12.2.11: 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 12.2.12: 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*.

12.3 Elasticity

Definition 12.3.1 (Elasticity of a Ring)
Let $\alpha \in \mathbb{Z}_K$ where $\alpha \neq 0$ and is not a unit. Define

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

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

$$\rho(K) \coloneqq \sup_{\alpha} \rho(\alpha).$$

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

Remark 12.3.2: Note that $h_K = 1, 2 \iff \rho(K) = 1$, and $h_K > 2 \implies \rho(K) > 1$.

Theorem 12.3.3 ***(Elasticity in terms of the Davenport constant).***
For $h_K \geq 2$,

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

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

Fact 12.3.5
$D(G) \to \infty$ as $|G| \to \infty$.

Corollary 12.3.6 ***(?).***
If $h_K \to \infty$ for a sequence of number fields, then $\rho(K) \to \infty$.

Remark 12.3.7: This just follows from the above facts, since $h_K \to \infty$ means the size of the group

$G \coloneqq \mathrm{Cl}(\mathbb{Z}_K)$ goes to infinity, which is a constant times $\rho(K)$. So as the class group gets larger, factorization gets worse.

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

Remark 13.0.1: Today: chapters 11 and 12.

13.1 Ch. 11: Prime Producing Polynomials and Unique Factorization

Remark 13.1.1: 18th century observation by Euler about the following polynomial:

$$f(x) \coloneqq x^2 - x + 41.$$

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 $x = 1, \cdots, 40$, 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

$$f_q(x) \coloneqq x^2 - x + q.$$

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 13.1.2 ***(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]

[a] Note that this is equal to $\mathbb{Z}_K$ when $K \coloneqq \mathbb{Q}(\sqrt{d})$.

Example 13.1.3 ***(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 ($\Longleftarrow$).

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

Assume $\mathbb{Z}[\tau]$ is a UFD, where $\tau \coloneqq \frac{1+\sqrt{d}}{2}$. Toward a contradiction, suppose $f_q(x)$ is composite

for some $0 < x < q$. We can write

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

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 $f \bmod p$. So $\min_{\tau}$ has a root modulo p. Recall that studying how $\langle p \rangle$ factors into ideals of $\mathbb{Z}_K$ involved studying how $\min_{\tau}$ 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

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

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. ↯

■

Remark 13.1.4: The forward direction is harder here.

Proof ($\implies$).
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, $\min_\tau$ has a root mod 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

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

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

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

This contradicts $f_q(x)$ being prime. ↯

■

So assuming $f_q(x)$ is prime for $1 \le x \le \frac{1}{2}\sqrt{\frac{|d|}{3}} + \frac{1}{2}$, 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 13.1.5 ***(When the class group is generated by small primes).***
Let d be a negative squarefree integer with $d \equiv 1 \bmod 4$ (such as the d we are looking at). Then $\mathrm{Cl}(\mathbb{Z}_K)$ is generated as a group by $[P]$ where P runs over all prime ideals above primes $p \le \sqrt{\frac{|d|}{3}}$.

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

■

13.2 Proof of Rabinowitz's Theorem

Remark 13.2.1: It just remains to prove the above theorem. We'll use the following:

Proposition 13.2.2 ***(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 $t \le \sqrt{\frac{|d|}{3}}$ and a $\xi \in \mathbb{Z}_K$ with norm $N(t\theta - \xi) < 1$.

Remark 13.2.3: 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 $d \equiv 1 \bmod 4$ 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 13.2.4: 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 $T \coloneqq \lfloor D \rfloor !$, 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 $J \coloneqq (T/\beta)\, I$, where noting that $T \in \mathbb{Z}^{>0}$, this is just a dilation of I. Then $J \subseteq \mathbb{Z}_K$, since

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

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 13.2.5:

Remark 13.2.6: 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 13.2.7 ***(Baker-Heegner-Stark).***
$\mathbb{Z}_K$ is not a UFD if $K \coloneqq \mathbb{Q}(\sqrt{d})$ with d squarefree with $d < -163$.

Remark 13.2.8: 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 $\mathrm{Cl}(\mathbb{Q}(\sqrt{d})) \approx d^{1/2}$, 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

[2]Note 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.

into the asymptotic statement.

Remark 13.2.9: 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 13.2.10.
The real quadratic field $\mathbb{Q}(\sqrt{d})$ is a UFD most of the time.

13.3 Lattice Points

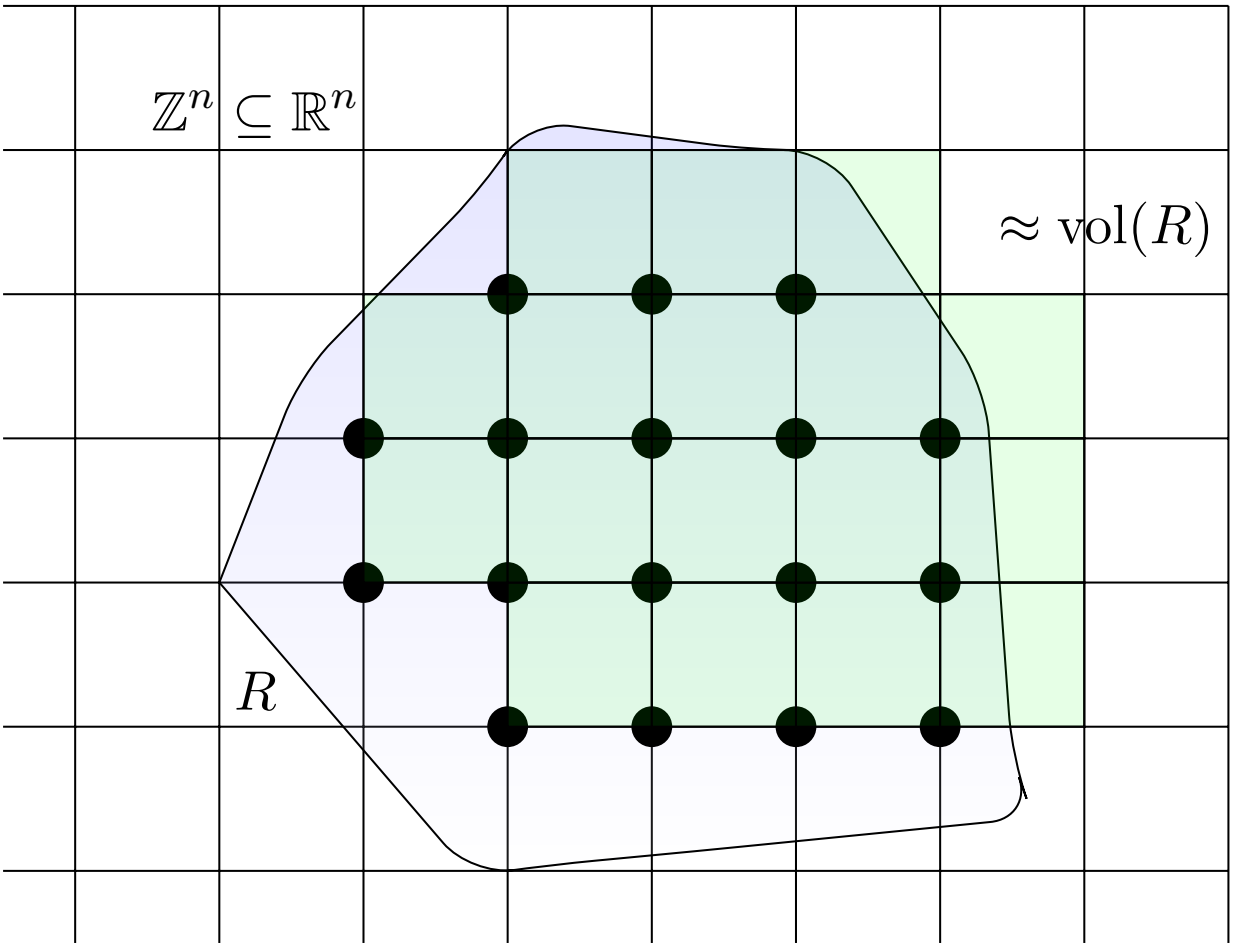
Remark 13.3.1: This corresponds to chapter 12. Everything we've done up until now has been for quadratic fields. After this chapter, we'll start anew and rebuild everything for general number fields.

Definition 13.3.2 (Lattice Point)
A **lattice point** in $\mathbb{R}^n$ is a point in $\mathbb{Z}^n$.

Question 13.3.3
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 13.3.4: 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:



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

$$tR \coloneqq \left\{ t\mathbf{x} \;\middle|\; \mathbf{x} \in R \right\}.$$

Theorem 13.3.5 ***(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

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

[a] This 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

$$\int \chi_R(\mathbf{w})\,d\mathbf{w} \coloneqq \mathrm{vol}(R).$$

■

Remark 13.3.6: 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.

14 Lattice Points (Lec. 12, Monday, March 01)

14.1 Minkowski (Version 1)

Remark 14.1.1: Basic heuristic from last time: counting the lattice points in a region R should be approximately $\mathrm{vol}(R)$. We turned this into a theorem for certain regions:

Theorem 14.1.2 ***(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

$$\frac{1}{t^n}L_{tR} \overset{t\to\infty}{\to} \mathrm{vol}(R).$$

Remark 14.1.3: Most of today: Minkowski's theorem, which will guarantee a lattice point under some conditions.

Theorem 14.1.4 ***(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 14.1.5: 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 $m >> 1 \in \mathbb{Z}^{\geq 0}$, this yields $L_{mR} > (2m)^n$. Consider $\mathbb{Z}^n$ and taking all coordinates $\bmod 2m$. 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.

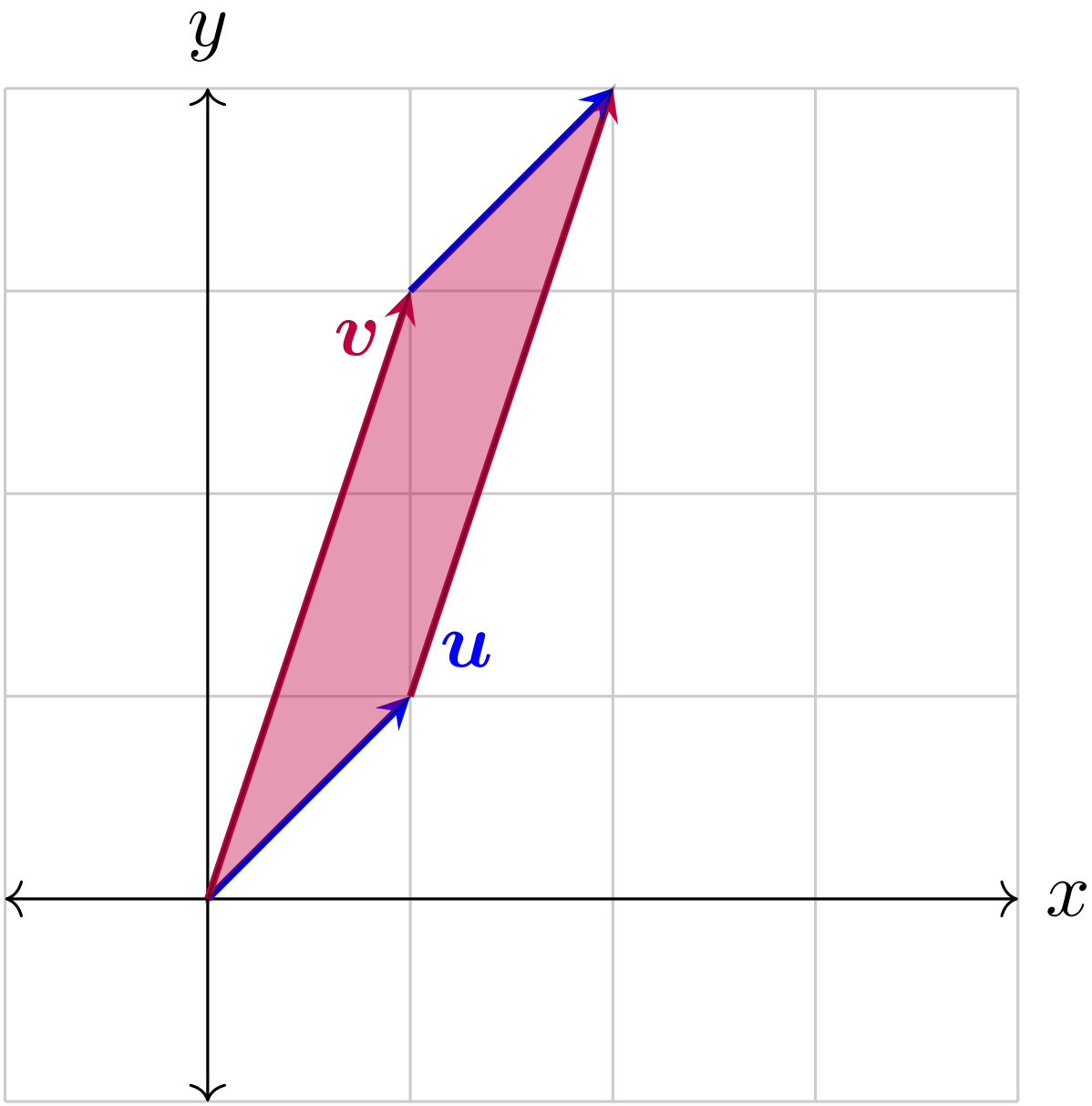
■

14.2 Minkowski (Version 2)

Definition 14.2.1 (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 14.2.2 *($n = 2$):*

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



- $\Lambda \coloneqq \mathbb{Z}[1,0]^t$, 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:

- $\Lambda \coloneqq \mathbb{Z}\left[\sqrt{2},0\right]^t + \mathbb{Z}\left\{1,0\right\}^t$, 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 14.2.3: 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 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.

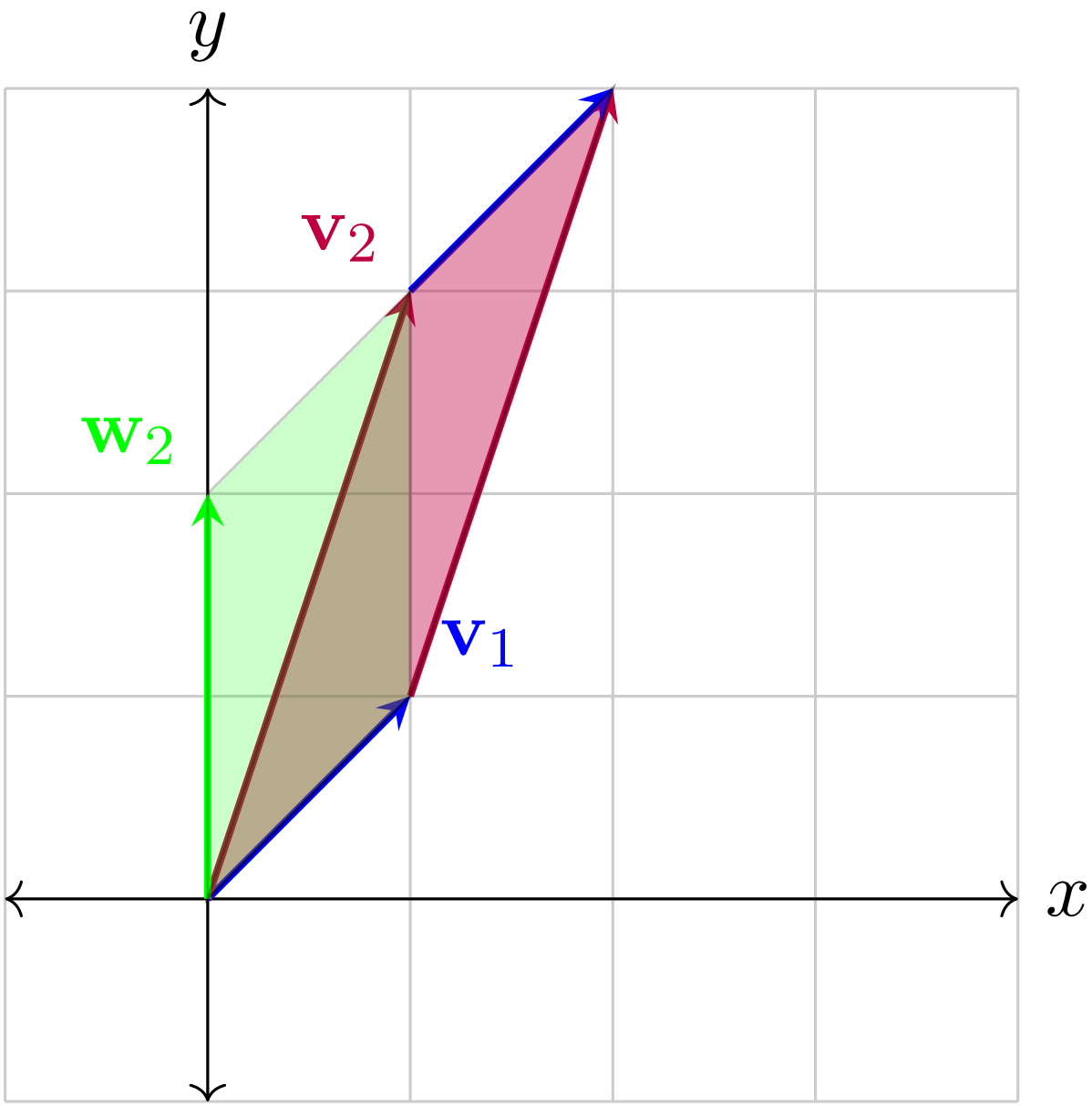
Definition 14.2.4 (Full Lattices)
If $d = n$, we'll call Λ a **full lattice**.

Definition 14.2.5 (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

$$\left\{ \sum_{i=1}^{n} c_n \mathbf{v}_n \;\middle|\; 0 \le c_i \le 1 \right\}.$$

Note that this depends on the choice of generating set.

Example 14.2.6 ***(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 14.2.7 ***(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 $M_v = \left[\mathbf{v}_1^t, \cdots, \mathbf{v}_n^t\right]$ 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

$$M_v = M_w A \qquad M_w = M_v A'$$

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 $A, A' \in \mathrm{Mat}(n \times n, \mathbb{Z})$, 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 14.2.8 (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:

$$\mathrm{covol}(\Lambda) \coloneqq |\det M_v|.$$

Theorem 14.2.9 ***(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

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

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

Remark 14.2.10: Taking $\Lambda \coloneqq \mathbb{Z}^n$ 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 $\mathbf{v}_1, \cdots, \mathbf{v}_n$ be n generators for Λ, then define a linear transformation

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

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

standard lattice, and

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

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

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

■

14.2.1 Application: The 4 Square Theorem

Theorem 14.2.11 ***(4 Square Theorem (Lagrange)).***
Every positive integer is a sum of 4 squares of integers.

Lemma 14.2.12 ***(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

$$A^2 + B^2 + 1 \equiv 0 \bmod m,$$

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 $\bmod m$, 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 $\mathbb{Z}/p$:

$$S_1 \coloneqq \left\{A^2 \bmod p\right\}$$
$$S_2 \coloneqq \left\{-1 - B^2 \bmod p\right\}.$$

Note that $\#S_1 = \dfrac{p+1}{2}$, since the number of nonzero squares is half the number of elements, so $\dfrac{p-1}{2}$, 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 $\dfrac{p+1}{2} > \dfrac{p}{2}$, but $|\mathbb{Z}/p| = p$, so these two sets can't be disjoint. So there is some $A^1 = -1 - B^2 \bmod p$.

■

Proof (of the 4 Square Theorem).
Suppose m is squarefree. Choose A, B as in the lemma, so $A^2 + B^2 \equiv -1 \bmod m$, and define

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

$$\Lambda \coloneqq \left\{(\alpha, \beta) \in \mathbb{Z}[i] \;\middle|\; \alpha \equiv \beta\gamma \bmod m\right\}.$$

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

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

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

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

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

$$a^2 + b^2 + c^2 + d^2 = \equiv 0 \bmod m.$$

Being congruent to $0 \bmod m$ 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 $(\alpha, \beta) \rightleftharpoons (a, b, c, d)$.

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

See the book for a proof of this claim!

Now let

$$R \coloneqq \left\{[x, y, z, w] \in \mathbb{R}^4 \;\middle|\; x^2 + y^2 + z^2 + w^2 < 2m\right\},$$

which is a convex and centrally symmetric region. A multivariable Calculus exercise shows $\operatorname{vol}(R) = 2\pi^2 m^2$, and $2\pi^2 > 2^4 \operatorname{covol}(\Lambda)$. 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 14.2.13: 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!

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

15.1 Recasting Old Definitions

Remark 15.1.1: 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 $N\alpha \coloneqq \prod_{\sigma\in G} \sigma(\alpha)$ and $\operatorname{Tr}\alpha \coloneqq \sum_{\sigma\in G} \sigma(\alpha)$. 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 15.1.2 (Field Polynomial)
If $\alpha \in K$ then define its **field polynomial**

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

Proposition 15.1.3 ***(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 $n \coloneqq [K : F[\alpha]]$.

Remark 15.1.4: Note that the first claim follows from the second since $\min_\alpha(x) \in \mathbb{Q}[x]$.

Lemma 15.1.5 ***(Number of embeddings of subfields).***
Let K be a number field with $[K:\mathbb{Q}] = n$ and $F \le K$ 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 15.1.6: The field polynomial gives us a way to determine whether an element of a number field is in its ring of integers:

Proposition 15.1.7 ***(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).
$\Longleftarrow$: 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.
$\Longrightarrow$: 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 15.1.8 (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

$$N(\alpha) \coloneqq (-1)^n a_0 \in \mathbb{Q}$$
$$\mathrm{Tr}(\alpha) \coloneqq -a_{n-1} \in \mathbb{Q}.$$

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

[a] These 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 15.1.9: 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 $N(-)$ is multiplicative and $\mathrm{Tr}(-)$ is $\mathbb{Q}$-linear.

15.2 Discriminants

Remark 15.2.1: Let K be a number field and $[K : \mathbb{Q}] = n$. Pick an arbitrary ordering of embeddings $\sigma_1, \cdots, \sigma_n : K \hookrightarrow \mathbb{C}$.

Definition 15.2.2 (Tuple Discriminant)
For any n-tuple $(w_1, \cdots, w_n) \in K^n$ define the **tuple discriminant** as

$$\Delta(w_1, \cdots, w_n) \coloneqq \det(D_{w_1, \cdots, w_n})^2$$

where

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

Remark 15.2.3: 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

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

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 $\Delta(w_1, \cdots, w_n) \in \mathbb{Q}$. 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 $\Delta(w_1, \cdots, w_n) \in \mathbb{Z}$.

Why is this called the discriminant?

Theorem 15.2.4 ***(The discriminant detects $\mathbb{Q}$-bases).***
Let $w_1, \cdots, w_n \in K$, then

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

Remark 15.2.5: So this *discriminates* between bases and non-bases.

Proof (of theorem).
$\impliedby$: Suppose $\Delta(w_1, \cdots, w_n) \neq 0$. Note that the n elements $w_1, \cdots, w_n$ 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 $\det(D)^2 = 0$.

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

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

Introduce an element $\beta \coloneqq \sum_{j=1}^{n} c_j w_j \in K^\times$, 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

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

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 $\alpha \coloneqq \beta^{-1}$, 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.
■

15.3 Integral Bases

Theorem 15.3.1 ***(Integral Basis Theorem).***
For K any number field of degree n, $\mathbb{Z}_K \in \mathbb{Z}$-Mod is free of rank n.

Observation 15.3.2
Suppose $(w_1, \cdots, w_n), (\theta_1, \cdots, \theta_n) \in K$ where $[w_1, \cdots, w_n] = [\theta_1, \cdots, \theta_n]M$ for some matrix $M \in \operatorname{Mat}(n \times n, \mathbb{Q})$. Then

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

Proof (of observation).
Applying the embeddings σ_i yields an equality $D_{w_1,w_2,\cdots,w_n} = D_{\theta_1,\theta_2,\cdots,\theta_n} M$. Now taking determinants and squaring yields the result.

■

Proof (of integral basis theorem).
Choose $w_1, w_2, \cdots, w_n \in \mathbb{Z}_K$ such that

1. $\Delta(w_1, w_2, \cdots, w_n) \neq 0$
2. $|\Delta(w_1, w_2, \cdots, w_n)|$ 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 $\Delta(w_1, w_2, \cdots, w_n) \in \mathbb{Z}$, 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 $w_1, w_2, \cdots, w_n$ 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 $\operatorname{span}_{\mathbb{Z}} \{w_1, w_2, \cdots, w_n\} = \mathbb{Z}_K$. 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

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

where $[-]$ denotes taking the integer part. We can write $\beta = \{c_1\}\, w_1 + c_2 w_2 + \cdots + c_n w_n$. Observe that the tuple

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

noting that the first column describes how to write β as a linear combination of the w_i. Taking discriminants yields

$$\Delta(\beta, w_2, \cdots, w_n) = \Delta(w_1, w_2, \cdots, w_n) \det(M)^2 = \Delta(w_1, w_2, \cdots, w_n) \{c_1\}^2,$$

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

$$0 < |\Delta(\beta, w_2, \cdots, w_n)| < |\Delta(w_1, w_2, \cdots, w_n)|,$$

which contradicts the minimality of the w_i. ↯

■

Remark 15.3.3: Note that this is non-constructive, finding a basis is another question!

15.4 Discriminant of Number Fields

Definition 15.4.1 (Discriminant of a Number Field)
Let K be a number field, then the **discriminant** of K is defined as

$$\Delta_K \coloneqq \Delta(w_1, w_2, \cdots, w_n),$$

where $\{w_i\}$ is any $\mathbb{Z}$-basis for $\mathbb{Z}_K$.

Remark 15.4.2: Is this actually an invariant of K, since we made a choice of basis? Given two $\mathbb{Z}$-bases for $\mathbb{Z}_K$, say $w_1, w_2, \cdots, w_n, \theta_1, \theta_2, \cdots, \theta_n$, then

$$[w_1, w_2, \cdots, w_n] = [\theta_1, \theta_2, \cdots, \theta_n]M \qquad M \in \mathrm{GL}(n, \mathbb{Z}).$$

Hence

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

using that invertible matrices have unit determinants, which in $\mathbb{Z}$ are just ± 1.

Remark 15.4.3: Why do we care? The discriminant measures the complexity of the number field and carries arithmetic information:

Theorem 15.4.4 ***(Hermite).***
For every $X > 0$, there are only finitely many number fields such that $|\Delta_K| \leq X$.

Remark 15.4.5: 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 15.4.6 ***(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, $\Delta(-) < \infty$, and so only finitely many such primes can occur.

16 Discriminants and Norms (Lec. 14, Saturday, March 13)

Example 16.0.1 ***(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 $d = 2, 3 \bmod 4$ 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 $d = 1 \bmod 4$, then we can take a basis $(1, \frac{1+\sqrt{d}}{2})$, and

$$\Delta_K = \left(\begin{bmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{bmatrix}\right)^2 = (-\sqrt{d})^2 = d.$$

So we have

$$\Delta_K = \begin{cases} d & d = 1 \bmod 4 \\ 4d & d = 2, 3 \bmod 4. \end{cases}$$

Remark 16.0.2: Note that $\Delta_{\mathbb{Q}} = 1$ if you trace through the computation.

16.1 Norms of Ideals

Definition 16.1.1 (Norm of an ideal)
Let $I \trianglelefteq \mathbb{Z}_K$ be a nonzero ideal, then define $N(I) \coloneqq \#\mathbb{Z}_K/I$.

Remark 16.1.2: 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 16.1.3 ***(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!

$$\begin{aligned} N\alpha &\coloneqq \prod_{\sigma: K \hookrightarrow \mathbb{C}} \sigma(\alpha) \\ &= \alpha \prod_{\substack{\sigma: K \hookrightarrow \mathbb{C} \\ \sigma \neq \mathbb{1}_K}} \sigma(\alpha) \\ &\coloneqq \alpha C, \end{aligned}$$

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 16.1.4 ***(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 $\mathbb{Z}_K \langle m \rangle \coloneqq \mathbb{Z}_K/m\mathbb{Z}_K \cong_{\mathbb{Z}\text{-Mod}} \mathbb{Z}^n/m\mathbb{Z}^n \cong (\mathbb{Z}/m\mathbb{Z})^n$ 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 $m \coloneqq \pm N\alpha$, 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 16.1.5 ***(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 16.1.6 ***(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 16.1.7: This will follow from the following proposition:

Proposition 16.1.8 ***(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 $\operatorname{rank}_{\mathbb{Z}} H = n$. Suppose that $\omega_1, \cdots, \omega_n$ is a $\mathbb{Z}$-basis for M and $\theta_1, \cdots, \theta_n$ a $\mathbb{Z}$-basis for H. We can thus write $[\theta_1, \cdots, \theta_n] = [\omega_1, \cdots, \omega_n]A$ for some $A \in \operatorname{Mat}(n \times n, \mathbb{Z})$. 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 $S, T \in \mathrm{GL}_n(\mathbb{Z})$ with

$$SAT = \operatorname{diag}(a_1, \cdots, a_n) \qquad a_i \in \mathbb{Z}.$$

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 $\omega_1, \cdots, \omega_n$ be a $\mathbb{Z}$-basis for $\mathbb{Z}_K$, then $\alpha\omega_1, \cdots \alpha\omega_n$ 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

$$[\alpha\omega_1, \cdots, \alpha\omega_n] = [\omega_1, \omega_n]A \implies \#\mathbb{Z}_K/\langle a\rangle = |\det(A)|,$$

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

$$\begin{aligned}
\Delta(\alpha\omega_1, \cdots, \alpha\omega_n) &= \Delta(\omega_1, \cdots, \omega_n)\det(A)^2 \\
\implies \det(A)^2 &= \frac{\Delta(\alpha\omega_1, \cdots, \alpha\omega_n)}{\Delta(\omega_1, \cdots, \omega_n)} \\
&= \frac{\det(D_{\alpha\omega_1, \cdots, \alpha\omega_n})^2}{\det(D_{\omega_1, \cdots, \omega_n})^2} = \left(\frac{\det(D_{\alpha\omega_1, \cdots, \alpha\omega_n})}{\det(D_{\omega_1, \cdots, \omega_n})}\right)^2.
\end{aligned}$$

Recall that these matrices were formed by taking the jth tuple element for the jth column and letting the column entries be the images under all embeddings. Just looking at the first rows in each, we'll have

$$[\sigma_1(\alpha\omega_1), \cdots, \sigma_1(\alpha\omega_n)] \qquad [\sigma_1(\omega_1), \cdots, \sigma_1(\omega_n)].$$

In general, the ith row of the first matrix will be $\sigma_i(\alpha)$ times the ith 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.

■

16.2 Ch. 14: Integral Bases

Question 16.2.1
Given K a number field, can you find an explicit $\mathbb{Z}$-basis for $\mathbb{Z}_K$?

Remark 16.2.2: 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 16.2.3
Let K be a number field with $[K:\mathbb{Q}] = n$ and suppose $\theta_1, \cdots, \theta_n$ 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 16.2.4: We know there is *some* $\mathbb{Z}$-basis for $\mathbb{Z}_K$, so let $\omega_1, \omega_2, \cdots, \omega_n$ be one. Then express the θ in terms of the ω:

$$\begin{aligned} [\theta_1, \theta_2, \cdots, \theta_n] &= [\omega_1, \omega_2, \cdots, \omega_n]A \\ \implies \Delta(\theta_1, \theta_2, \cdots, \theta_n) &= \Delta(\omega_1, \omega_2, \cdots, \omega_n)\det(A)^2. \end{aligned}$$

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

$$|\det(A)| = [\mathbb{Z}_K : H], \qquad H \coloneqq \operatorname{span}_{\mathbb{Z}}\{\theta_i\}.$$

Thus

$$\Delta(\theta_1, \theta_2, \cdots, \theta_n) = \Delta(\omega_1, \omega_2, \cdots, \omega_n)[\mathbb{Z}_K : H]^2.$$

We can thus form a simple condition for when $H = \mathbb{Z}_K$:

Corollary 16.2.5 ***(A sufficient condition).***
If $\Delta(\theta_1, \theta_2, \cdots, \theta_n$ is squarefree, then $\theta_1, \theta_2, \cdots, \theta_n$ are a $\mathbb{Z}$-basis of $\mathbb{Z}_K$.

Remark 16.2.6: 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 $d = 2, 3 \bmod 4$ that $\Delta_K = 4d$, which is not squarefree.

Example 16.2.7 ***(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 $\left\{\theta^j \;\middle|\; 0 \le j \le 4\right\}$, 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

$$\begin{aligned}
\Delta(1, \theta, \theta^2, \theta^3, \theta^4) &:= \det(\left[\sigma_i(\theta^{j-1})\right])^2 \\
&= \det(\left[\sigma_i(\theta)^{j-1}\right])^2 && \text{since the } \sigma_i \text{ are embeddings} \\
&= \prod_{1 \le i < j \le 5} (\sigma_j(\theta) - \sigma_i(\theta))^2 && \text{since this is a Vandermonde matrix} \\
&= \Delta(f),
\end{aligned}$$

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 16.2.8 ***(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

$$\mathbb{Z}_K \subseteq \frac{1}{2}\mathbb{Z}[\alpha] = \left\{ \frac{c_0 + c_1\alpha + c_2\alpha^2}{2} \;\middle|\; c_i \in \mathbb{Z} \right\}.$$

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 $\mathbb{Z}_K \supseteq \mathbb{Z}[\alpha]$. One can check that $\dfrac{\alpha + \alpha^2}{2} \in \mathbb{Z}_K \setminus H$. So the original candidate basis was wrong, but we can take $1, \alpha, \dfrac{\alpha + \alpha^2}{2}$ instead, which is an integral basis.

Remark 16.2.9: 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 16.2.10: Next time: integral bases for cyclotomic fields.

17 Cyclotomic Fields (Lec. 15, Saturday, March 13)

Remark 17.0.1: This is chapter 14 continued.

Definition 17.0.2 (Cyclotomic Fields)
A **cyclotomic field** is a number field $\mathbb{Q}(\zeta_m)$ where $\zeta_m \coloneqq e^{2\pi i/m}$, a primitive mth root of 1.

Remark 17.0.3: The Kronecker-Webber theorem: any *abelian extension* $K/\mathbb{Q}$ (so $\mathsf{Gal}(K/\mathbb{Q}) \in \mathsf{Ab}$) 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 17.0.4 ***(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 17.0.5: 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 $f(x) \coloneqq \sum a_i x^i$ but $p^2 \nmid a_0$, then f is irreducible over $\mathbb{Q}$.

Lemma 17.0.6 ***(The minimal polynomials of roots of unity).***
The minimal polynomial of ζ_p over $\mathbb{Q}$ is

$$\Phi_p(x) \coloneqq x^{p-1} + x^{p-2} + \cdots + x + 1,$$

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 17.0.7 ***(Eisenstein primes don't divide the extension degree).***
Let $\alpha \in \bar{\mathbb{Z}}$ be an algebraic integer such that

$$\min_{\alpha}(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \qquad \in \mathbb{Z}[x]$$

is Eisenstein at the prime p. Let $K \coloneqq \mathbb{Q}(\alpha)$, 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

$$\alpha^n = -(a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0) \equiv 0 \bmod p \text{ in } \mathbb{Z}_K,$$

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 $p\beta = b_0 + b\alpha + \cdots + b_{n-1}\alpha^{n-1}$ 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:

$$p\beta \equiv 0 \equiv b_i\alpha^i + \cdots + b_{n-1}\alpha^{n-1} \bmod p.$$

Now multiply by α^{n-1-i} to obtain

$$0 \equiv b_i\alpha^{n-1} + \cdots \equiv b_i\alpha^{n-1} \bmod p,$$

where p divides all of the other terms since they all contain a factor of $\alpha^n \equiv 0 \bmod p$. So $b_i\alpha^{n-1}/p \in \mathbb{Z}_K$, and by a previous theorem, this forces $N(b_i\alpha^{n-1}/p) \in |ZZ$. 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. ↯

■

Remark 17.0.8: 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

$$\Delta(f) \coloneqq \prod_{i<j}(\alpha_j - \alpha_i)^2.$$

We won't discuss the theory, but we'll use a few facts.

Fact 17.0.9
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,

  $$\Delta(f) \bmod q = \Delta(f \bmod q),$$

  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 $f \bmod q \in \mathbb{F}_q[x]$ 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 $\zeta \coloneqq \zeta_p$. We want to show $1, \zeta, \cdots, \zeta^{p-2}$ forms an integral basis, from last time we have

$$\Delta(1, \zeta, \cdots, \zeta^{p-2}) = \Delta_K [\mathbb{Z}_K : \mathbb{Z}[\zeta]]^2 \implies [\mathbb{Z}_K : \mathbb{Z}[\zeta]]^2 \mid \Delta(1, \zeta, \cdots, \zeta^{p-2}).$$

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. $q \mid \Delta(x^{p-1} + \cdots + x + 1)$. So this is zero mod q, and thus $\Delta(x^{p-1} + \cdots + x + 1 \bmod q) \equiv 0$. The discriminant was a product of roots, so it can only be zero if two roots coincide, so there is a multiple root of $x^{p-1} + \cdots + x + 1 \bmod q$ 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 $\Delta_a \coloneqq \Delta_{\mathbb{Q}(\zeta_a)}, \Delta_b \coloneqq \Delta_{\mathbb{Q}(\zeta_b)}$ 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 $\Delta_a \mid a^?$ divides some power of a, and the same for b, and so a, b coprime will make $a^?, b^?$ 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 $\mathbb{Z}_{K_1K_2} = \mathbb{Z}_{K_1}\mathbb{Z}_{K_2}$, 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 17.0.10: The hard part is the lemma in (3). Also, questions about discriminants tend to come up during oral exams that include algebraic number theory.

17.1 Ideal Theory in General Number Rings (Ch. 15)

Remark 17.1.1: 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. $\mathrm{Id}(\mathbb{Z}_K)$ to be a UFM as a monoid,
2. $\mathrm{Cl}(\mathbb{Z}_K)$ 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 17.1.2 (Class Group of a Number Ring)

$$\mathrm{Cl}(\mathbb{Z}_K) \coloneqq \mathrm{Id}(\mathbb{Z}_K)/\sim,$$

where $\sim$ denotes dilation equivalence.

Remark 17.1.3: Our strategy:

- Prove $\mathrm{Cl}(\mathbb{Z}_K)$ is finite.
- Prove $\mathrm{Cl}(\mathbb{Z}_K)$ 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 17.1.4 ***(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 17.1.5: 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 17.1.6 ***(The class group is finite).***

$$\#\mathrm{Cl}(\mathbb{Z}_K) < \infty.$$

Proof (that the class group is finite).
Very similar to how it goes for quadratic fields. As before, let $I \in \mathrm{Id}(\mathbb{Z}_K)$ 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 $J \coloneqq \dfrac{T!}{\beta} I \subseteq \mathbb{Z}_K$, which is a dilation of I and thus $J \trianglelefteq \mathbb{Z}_K$ as well. By definition, $I \sim J$, i.e. $[I] = [J] \in \mathrm{Id}(\mathbb{Z}_K)$, 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:

$$\left\{ \begin{matrix} \text{Ideals of } \mathbb{Z}_K \\ \text{containing } \langle T! \rangle \end{matrix} \right\} \rightleftharpoons \left\{ \text{Ideals of } \mathbb{Z}_K / \langle T! \rangle \right\},$$

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 $\mathbb{Z}_K \cong_{\mathsf{Ab}} \mathbb{Z}^n$, 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]

■

[a] In fact, we've already proved that $\mathbb{Z}_K / I$ for any nonzero ideal I is finite.

Remark 17.1.7: We now want to establish the cancellation law in $\mathrm{Id}(\mathbb{Z}_K)$, then the principal multiple lemma, and then everything else will follow as in the quadratic case.

18 Ideal Theory in Number Fields Continued (Lec. 16, Tuesday, March 30)

18.1 Setting up the Theory

Remark 18.1.1: 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 $\mathrm{Cl}(\mathbb{Z}_K)$ is a finite monoid,
- Prove $\mathrm{Cl}(\mathbb{Z}_K)$ 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 18.1.2 ***(When ideals are left identities under multiplication).***
Let $I, J \in \mathrm{Id}(\mathbb{Z}_K)$, then if $IJ = J$ then $I = \langle 1 \rangle$.

Remark 18.1.3: 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 $J = \langle \beta_1, \cdots, \beta_n \rangle$, 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 $A \in \mathrm{Mat}(m \times m, I)$ with entries $A_{ij} \in I$ such that

$$[\beta_1, \cdots, \beta_m] = [\beta_1, \cdots, \beta_m]A.$$

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

$$0 \equiv \det(A - \mathbb{1}) \equiv \det(-\mathbb{1}) \equiv \pm 1 \bmod I,$$

but this can only occur if $1 \in I$, making $\langle 1 \rangle = I$.

■

Lemma 18.1.4 ***(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 18.1.5: 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 18.1.6 ***(Principal Multiple Lemma).***
For all $I \in \mathrm{Id}(\mathbb{Z}_K)$ there is a $J \in \mathrm{Id}(\mathbb{Z}_K)$ such that IJ is principal.

Proof (of principal multiple lemma).
Consider $[I], [I]^2, \cdots \in \mathrm{Cl}(\mathbb{Z}_K)$. 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 $J \coloneqq I^{\ell-k-1}$.

■

Remark 18.1.7: Note that the logical order in which these theorems are proved is slightly reversed.

Corollary 18.1.8 ***(Class groups are finite and*** Id ***is a cancellative monoid).***

a. $\mathrm{Cl}(\mathbb{Z}_K)$ is a group, and thus a finite abelian group.

b. $\mathrm{Id}(\mathbb{Z}_K)$ 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 18.1.9 ***(The monoid*** Id ***is atomic).***
$\mathrm{Id}(\mathbb{Z}_K)$ 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

$$\mathbb{Z}_K/J \to \mathbb{Z}_K/I.$$

This has nontrivial kernel since $I \setminus J \neq \emptyset$, so $|\mathbb{Z}_K/J| > |\mathbb{Z}_K/I|$.

■

Lemma 18.1.10 ***(Analog of Euclid's Lemma).***
Irreducibles in $\mathrm{Id}(\mathbb{Z}_K)$ are prime.

Proof (of lemma).
Same as before! Literally use the exact same words, we've set it up this way.
■

Theorem 18.1.11 ***(The monoid*** Id ***is a unique factorization monoid).***
$\mathrm{Id}(\mathbb{Z}_K)$ is a UFM, or equivalently every nonzero ideal factors uniquely as a product of prime ideals.

18.2 Modern Approach

Question 18.2.1
What is the widest class of domains for which the previous theorem holds?

Definition 18.2.2 (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 $K = \mathrm{ff}(R)$, 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.

[a] Compare to the classical rational root theorem.

Theorem 18.2.3 ***(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 18.2.4 ***(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 $\alpha \in \overline{\mathbb{Z}_K} \cap K \coloneqq \mathbb{Z}_K$.

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 $N(P) < \infty$.

■

18.3 Norms Revisited

Remark 18.3.1: 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 18.3.2 ***(The norm is multiplicative).***

$$N(IJ) = N(I)N(J) \qquad \forall I, J \in \mathrm{Id}(\mathbb{Z}_K).$$

Remark 18.3.3: If $I, J \in \mathrm{Id}(\mathbb{Z}_K)$, 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

$$\begin{aligned}\psi : \mathbb{Z}_K/p &\to I/IP \\ \alpha \bmod p &\mapsto \alpha\beta \bmod IP.\end{aligned}$$

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 $\alpha \bmod P \in \ker\psi$, 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 $\alpha \bmod P = 0$, 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, $\operatorname{im}\psi = (\langle\beta\rangle + IP)/IP$. 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

$$\begin{aligned}\operatorname{im}(\psi) &= \frac{\langle\beta\rangle + IP}{IP} \\ &= \frac{\gcd(\langle\beta\rangle, IP)}{IP} \\ &= I/IP.\end{aligned}$$

■

Remark 18.3.5: 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 18.3.6 (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 18.3.7 (Arithmetic of ideals)
Check that

- $(IJ)S = (IS)(JS)$,
- $(\alpha R)S = \alpha S$.

Theorem 18.3.8 ***(Norm is generated by product of conjugates).***
Let $I \in \mathrm{Id}(\mathbb{Z}_K)$ 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 18.3.9: This shows why the norm is multiplicative, and why $N(\langle\alpha\rangle) = |N(\alpha)|$.

18.4 Applications of Finiteness of Class Group

Question 18.4.1
Where do ideals come from?

Remark 18.4.2: 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 18.4.3 ***(Dedekind's theorem on the actuality of ideals).***
Let K be a number field and $I \trianglelefteq \mathrm{Id}(\mathbb{Z}_K)$. Then there is a $\beta \in \overline{\mathbb{Z}}$ such that $I = \beta\overline{\mathbb{Z}} \cap K$, or equivalently $I = \beta\overline{\mathbb{Z}} \cap \mathbb{Z}_K$.

Remark 18.4.4: Example of a non-principal ideal: in $\mathbb{Z}[\sqrt{-5}]$, the ideal $I \coloneqq \left\langle 2, 1+\sqrt{-5}\right\rangle$ 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 $\overline{\mathbb{Z}}$) 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 $\overline{\mathbb{Z}}$ instead.

Lemma 18.4.5 ***(Ideals become principal after extending).***
Let K be a number field and $I \in \mathrm{Id}(\mathbb{Z}_K)$. 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 $m \coloneqq \#\mathrm{Cl}(\mathbb{Z}_K)$. Then $I^m = \alpha\mathbb{Z}_K$ is principal since m is the order of this group. Let $\beta \coloneqq \sqrt[m]{\alpha} \in \mathbb{C}$ and let $L \coloneqq K(\beta)$. Here β is an algebraic integer since it's an mth 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 mth power? By unique factorization, they must be the same, so $I\mathbb{Z}_L = \beta\mathbb{Z}_L$.

To be continued.

■

19 Ch. 16, Continued (Thursday, May 13)

19.1 Actuality of Ideals

Theorem 19.1.1 ***(Dedekind, Actuality of ideals).***
If I is a nonzero ideal of $\mathbb{Z}_K$ for K a number field, then there is an $\alpha \in \overline{\mathbb{Z}}$ such that

$$I = (\alpha\overline{\mathbb{Z}}) \cap \mathbb{Z}_K.$$

Lemma 19.1.2 ***(?).***
Let I be a nonzero ideal of $\mathbb{Z}_K$, then there is an extension of number fields L/K such that $I\mathbb{Z}_L$ is principal ,say $I\mathbb{Z}_L = \alpha\mathbb{Z}_L$.

Proof (Idea).
We've already proved this, but the idea was that we can take m to be the order of the class group to obtain $I^m = \beta\mathbb{Z}_K$. Then if $L = K(\beta^{1/m})$ we will have $I\mathbb{Z}_L = \beta^{1/m}\mathbb{Z}_L$.

■

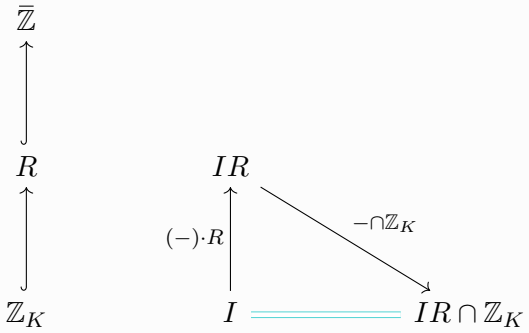
Remark 19.1.3: How we'll use this to prove the theorem: the lemma shows that after passing to a suitable extension we can find α, and the claim is that this α works. We'll need one more result:

Lemma 19.1.4 ***(Paul's up-down lemma).***
Let K be a number field and $I \trianglelefteq \mathbb{Z}_K$ be a nonzero ideal. Let $R \leq \overline{\mathbb{Z}}$ be a subring containing $\mathbb{Z}_K$, then

$$IR \cap \mathbb{Z}_K = I \trianglelefteq \mathbb{Z}_K.$$

The picture: we can lift ideals from $\mathbb{Z}_K$ to R and intersect them with $\mathbb{Z}_K$ to come back down,

and the claim is that this lands where you started:



Link to Diagram

Proof (?).
Follow your nose! The containment $I \subseteq IR \cap \mathbb{Z}_K$ is clear, since I is contained in both terms. For the reverse containment, we'll first do it for I principal, and then reduce to that case. So suppose $I = \alpha\mathbb{Z}_K$, then $IR = \alpha R$. Take $\beta \in IR \cap \mathbb{Z}_K$, then $\frac{\beta}{\alpha \in R \cap K \subseteq \overline{\mathbb{Z}} \cap K = \mathbb{Z}_K}$. Then $\beta \in \alpha\mathbb{Z}_K$, which is what we wanted to show.

We'll reduce to the principal case by using a familiar trick. Pick $m \in \mathbb{Z}^{\geq 0}$ so that I^m is principal, then $I^m R \cap \mathbb{Z}_K = I^m$ by the previous case. Taking $\gamma \in IR \cap \mathbb{Z}_K$, we'll show it must be in I. We know $\gamma^m \in (IR)^m = I^m R$, and thus we have $\gamma^m \in I^m R \cap \mathbb{Z}_K = I^m$. Now using unique factorization and to contain is to divide, this implies that $I^m \mid \langle \gamma^m \rangle = \langle \gamma \rangle^m$. So $I \mid \langle \gamma \rangle$ and thus $\gamma \in I$.

■

Proof (of theorem).
Choose an extension L/K with $I\mathbb{Z}_L = \alpha\mathbb{Z}_M$ principal. consider $I\overline{\mathbb{Z}}$. We have $I\overline{\mathbb{Z}} = (I\mathbb{Z}_L)\overline{\mathbb{Z}}$ – this just says that extending I to $\overline{\mathbb{Z}}$ can be done in two steps, first extending to $\mathbb{Z}_L$. Concretely, these extensions are linear combinations of elements in I with coefficients in $\mathbb{Z}_L$, so extending in stages yields the same thing. We have

$$\begin{aligned} I\overline{\mathbb{Z}} &= (I\mathbb{Z}_L)\overline{\mathbb{Z}} \\ &= (\alpha\mathbb{Z}_L)\overline{\mathbb{Z}} \\ &= \alpha\overline{\mathbb{Z}}. \end{aligned}$$

Now apply the up-down lemma to $R = \overline{\mathbb{Z}}$ to obtain

$$I = I\overline{\mathbb{Z}} \cap \mathbb{Z}_K,$$

which is equal to $\alpha\overline{\mathbb{Z}} \cap \mathbb{Z}_K$.

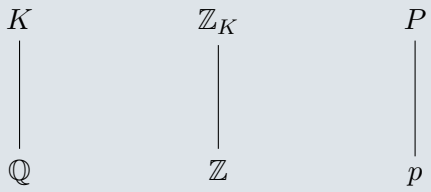
■

Remark 19.1.5: Is is true that in $\overline{\mathbb{Z}}$ that every ideal is principal? The answer is no, since this would force it to be a UFD, but $\overline{\mathbb{Z}}$ has irreducibles at all since there are no irreducibles. One *can*

prove that every finitely generated ideal of $\overline{\mathbb{Z}}$ is principal. One can also prove a variant of Gauss' lemma for $\overline{\mathbb{Z}}$: one can take the greatest common divisor to be the generator of a principal ideal.

20 Ch. 17: Prime Decomposition and General Number Rings

Definition 20.0.1 (lies above)
If $P \trianglelefteq \mathbb{Z}_K$ is nonzero, then P **lies above** a rational prime $p \in \mathbb{Z}$ if $p \in P$. We also say p **lies below** P.
The picture:



Link to Diagram

Remark 20.0.2: As in the quadratic field setting, every P lies above some uniquely determined p in the sense that $P \cap \mathbb{Z} = p\mathbb{Z}$. The proof here goes through in the same way. Note that since $p \in P \implies \langle p \rangle \in P$, we have $\langle p \rangle \mid P$. How do rational primes decomposes in $\mathbb{Z}_K$? I.e., how does $\langle p \rangle$ factor into prime ideals?

Remark 20.0.3: There are two main theorems: one describes how these prime ideals factor, and the second (Dedekind-Kummer) will produce the factorization.

Theorem 20.0.4 ***(efg theorem).***
Let K be a number field of degree $[K : \mathbb{Q}] = n$ and let p be a rational prime. Factor

$$\langle p \rangle = \prod_{i=1}^{g} P_j i e_i,$$

where the P_i are distinct primes ideals and $e_i > 0$. Then for each i we have $N(P_i) = p^{f_i}$ for some $f_i > 0$, and

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

Before the proof, it's helpful to introduce some notation.

Definition 20.0.5 (Residual degree and ramification index)
In the setup above, call $f_i = f(P_i/p)$ the **residual degree** of P_i/p and $e_i = e(P_i/p)$ the

ramification index.

Proof (of theorem).
Consider the homomorphisms

$$\begin{aligned}\varphi : \mathbb{Z} &\to \mathbb{Z}_K/P_i \\ a &\mapsto a \bmod P_i.\end{aligned}$$

We have $\ker\varphi = P_i \cap \mathbb{Z}$, and since P lies over p, this equals $p\mathbb{Z}$. So there is an induced injection $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathbb{Z}_K/P_i$, where $a \bmod p \mapsto a \bmod P_i$. Thus $\mathbb{Z}_K/P_i \in \mathsf{Vect}_{\mathbb{F}_p}$ is an $\mathbb{F}_p$-vector space. We want to show the size of the right-hand side, which is the size of P_i, is a power of p. But any finite-dimensional vector space over $\mathbb{F}_p$ has dimension p^ℓ for some ℓ. Let $f_i := \dim_{\mathbb{F}_p}(\mathbb{Z}_K/P_i)$, then $N(P_i) = \#\mathbb{Z}_K/P_i = p^{f_i}$.

Now proving that $\sum e_i f_i = n$ is an easy corollary: go back to the factorization and take norms of both sides. Noting $N(\langle p\rangle) = p^n$ since $\mathbb{Z}_K \in \mathsf{Ab}_n^{\mathsf{Free}}$, we have

$$\begin{aligned}p^n &= N(\langle p\rangle) \\ &= \prod_{i=1}^{g} N(P_i)^{\ell_i} \\ &= \prod_{i=1}^{g} p^{e_i f_i} \\ &= p^{\sum_i e_i f_i},\end{aligned}$$

and the result follows by comparing exponents.

■

Observation 20.0.6
Each $\mathbb{Z}_K/P_i$ is a field. Since $P_i \in \operatorname{Spec}\mathbb{Z}_K$, so $\mathbb{Z}_K/P_i$ is an integral domain. It's finite by the above argument, using that norms are finite, so it's in fact a field. It contains $\mathbb{Z}/p\mathbb{Z}$, and is thus an extension over it, and the extension degree $[\mathbb{Z}_K/P_i : \mathbb{Z}/p\mathbb{Z}] = f_i$. So f_i are called the residual degrees since they're the degrees of extensions of residue fields.

Definition 20.0.7 (Inert, split, ramified)
More terminology:

- If $\langle p\rangle$ is prime, the p is **inert**.
- If $g = n$, which forces $e_i = f_i = 1$ for all i, then p **splits completely**.
- If $e_i > 1$ for any i, then p **ramifies**.

Remark 20.0.8: How do we actually determine the prime factors?

Theorem 20.0.9 ***(Dedekind-Kummer).***
Let K be a number field of degree n and suppose $K = \mathbb{Q}(\alpha)$ where $\alpha \in \overline{\mathbb{Z}}$. This can be done by using the primitive element and scaling by an integer. Let p be a rational prime, and suppose $p \nmid [\mathbb{Z}_K : \mathbb{Z}[\alpha]]$. Then the prime ideal factorization of $\langle p \rangle$ mirrors the factorization of $\min_\alpha(x) \bmod p$.

More precisely, supposing

$$\min_\alpha(x) = \prod_{i=1}^{g} p_i(x)^{e_i} \bmod p \qquad\qquad p_i \in \mathbb{Z}[x],$$

where the p_i are the irreducible factors of $\min_\alpha(x)$ in $\mathbb{F}_p[x]$. Then

$$\langle p \rangle = \prod_{i=1}^{g} P_i^{e_i} \qquad\qquad P_i \coloneqq \langle p, p_i(\alpha) \rangle .$$

These $P_i \in \operatorname{Spec} \mathbb{Z}_K$ are distinct, and the residual degrees are given by $f_i = \deg(p_i)$.

Remark 20.0.10: So as long as this condition holds, we factor P by factoring a minimal polynomial mod p. Note that if one can find an $\alpha \in \mathbb{Z}_K$, the condition holds vacuously since the index is 1. This always holds for quadratic fields, since $\mathbb{Z}_K = \mathbb{Z}[\tau]$, so this recovers the factorization statement in that setting. In an annoying twist of fate, not every number field can be written as $\mathbb{Z}[\alpha]$ for some single α, and so this theorem necessarily excludes some primes. Is there some easy way to check the divisibility condition? The answer is yes, coming from the discriminant.

Proposition 20.0.11 ***(?).***
Suppose $K = \mathbb{Q}(\alpha)$ where $\alpha \in \overline{\mathbb{Z}}$. If $p^2 \nmid \Delta(\min_\alpha(x))$, then $p \nmid [\mathbb{Z}_K : \mathbb{Z}[\alpha]]$.

Remark 20.0.12: A while ago we showed that

$$\Delta(\min_\alpha(x)) = \Delta(1, \alpha, \alpha^2, \cdots, \alpha^{n-1}) = \Delta_K \cdot [\mathbb{Z}_K : \mathbb{Z}[\alpha]]^2.$$

Note that we're done if this is true: if p divides the index, p^2 divides the last term, meaning p^2 divides the first.

Example 20.0.13 ***(?):*** Let $K = \mathbb{Q}(\alpha)$ where α is a root of the irreducible polynomial $f(x) = x^3 - x^2 - 2x + 8$. Recall that we used this example when looking at integral bases. By a computation, $\Delta(f(x)) = -4 \cdot 503$, and the only squared prime dividing this is $p = 2$. We can thus apply Dedekind-Kummer for all $p \neq 2$.

- Mod 3, f is irreducible. So $\langle 3 \rangle$ is prime and 3 is inert.
- Mod 5, $f(x) \equiv (x+1)(x^2-2)$. So $\langle 5 \rangle = P_1 P_2$ where $P_1 = \langle 5, \alpha + 1 \rangle$ and $P_2 = \left\langle 5, \alpha^2 - 2 \right\rangle$. Thus $f_1 = \deg(x+1) = 1, f_2 = \deg(x^2-2) = 2$.
- Mod 59, $f(x) \equiv (x+11)(x+20)(x+25)$. So $\langle 59 \rangle = P_1 P_2 P_3$ where e.g. $P_1 = \langle 5, \alpha + 11 \rangle$ and

so on. Note that $g = 3 = n$, so 59 splits completely.

- Mod 503, $f(x) \equiv (x + 259)(x + 354)^2$. So $\langle 503 \rangle = P_1 P_2^2$, and thus 503 ramifies since an exponent is larger than 1.

Note that $\Delta(f(x)) = 0 \bmod 503$, so $f \in \mathbb{F}_{503}[x]$ has a repeated root in an extension. We can run this backward to show that 503 is the only odd prime that ramifies: Dedekind-Kummer says this can only happen if f has a repeated root mod p. In this case, $\Delta(f) \bmod p = 0$, so $p \mid 4 \cdot 503$. Note that if you try to apply this theorem mod 2, this results in the wrong answer!

Lemma 20.0.14*(?).*
Let $K = \mathbb{Q}(\alpha)$ be a number field where $\alpha \in \overline{\mathbb{Z}}$. Suppose $p \nmid [\mathbb{Z}_K : \mathbb{Z}[\alpha]]$. Then the inclusion $\iota : \mathbb{Z}[\alpha] \hookrightarrow \mathbb{Z}_K$ induces an isomorphism

$$\bar{\iota} : \frac{\mathbb{Z}[\alpha]}{p\mathbb{Z}[\alpha]} \xrightarrow{\sim} \mathbb{Z}_K / p\mathbb{Z}_K.$$

Proof (?).
Start by showing $p\mathbb{Z}_K \cap \mathbb{Z}[\alpha] = p\mathbb{Z}[\alpha]$. The reverse containment is clear, so let $\beta \in p\mathbb{Z}_K \cap \mathbb{Z}[\alpha]$. Then $\beta/p \in \mathbb{Z}_K$, so look at its image in $\mathbb{Z}_K/\mathbb{Z}[\alpha]$. The order of the image divides p, , since $p(\beta/p) = \beta \in \mathbb{Z}[\alpha]$. But we assumed that p doesn't divide the size of this quotient, forcing the order to be 1 and thus $\beta/p \in \mathbb{Z}[\alpha] \implies \beta \in p\mathbb{Z}[\alpha]$.

■

Remark 20.0.15: The map $\bar{\iota}$ is well-defined because $\iota(p\mathbb{Z}[\alpha]) \subseteq p\mathbb{Z}_K$, and is obviously a homomorphism. We want it to be an isomorphism, so what's the kernel? We've just shown that $\ker \bar{\iota} = 0$, and comparing cardinality makes it a surjection. Both have cardinality p^n, since both are free abelian groups of rank n.

Remark 20.0.16: This is useful because the Dedekind-Kummer theorem describes the left-hand side, but we want to study the right-hand side instead. The theorem says they're isomorphic!

21 Ch. 17: Dedekind-Kummer (Thursday, May 13)

Remark 21.0.1: Big theorem, Dedekind-Kummer: we have a factorization of p for all but finitely many primes p. e supposed that $p \nmid [\mathbb{Z}_K : \mathbb{Z}[\alpha]]$, and there are only finitely many p that violate this condition. The claim was that if $\min_\alpha(x)$ factors into distinct irreducibles $p_i(x)$ in $\mathbb{F}_p[x]$, then setting $P_i \coloneqq \langle p, p_i(\alpha) \rangle$. Then there is a factorization of ideals $\langle p \rangle = \prod P_i^{e_i}$ mirroring the factorization of the minimal polynomial.

We had a lemma that under these hypotheses, the inclusion $\iota : \mathbb{Z}[\alpha] \hookrightarrow \mathbb{Z}_K$ induces an isomorphism

on quotients

$$\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \xrightarrow{\sim} \mathbb{Z}_K/p\mathbb{Z}_K.$$

So mod p, these two are the same.

Proof (of Dedekind-Kummer).
For notation, set $m(x) \coloneqq \min_{\alpha}(x)$. By assumption, we have a factorization $m(x) = \prod_{i=1}^{g} p_i(x)^{e_i} \bmod p$, and we set $P_i \langle p, p_i(g\alpha)\rangle$. We'll first show that the P_i are prime ideals by modding to get a domain, and we'll compute residue degrees. Considering

$$\begin{aligned}
\mathbb{Z}_K/P_i &= \mathbb{Z}_K/\langle p, p_i(\alpha)\rangle \\
&\cong (\mathbb{Z}_k/\langle p\rangle)/\langle p_i(\alpha) \bmod p\rangle \\
&\cong (\mathbb{Z}[\alpha]/\langle p\rangle)/\langle p_i(\alpha) \bmod p\rangle \\
&\cong \mathbb{Z}[\alpha]/\langle p, p_i(\alpha)\rangle \\
&\cong (\mathbb{Z}[x]/\langle m(x)\rangle)/\langle p \bmod m(x), p_i(x) \bmod m(x)\rangle \\
&\cong (\mathbb{Z}[\alpha]/\langle p\rangle)/\langle m(x) \bmod p, p_i(x) \bmod p\rangle \qquad \cong \mathbb{F}_p[x]/\langle p_i(x) \bmod p\rangle .
\end{aligned}$$

where we've used that $p_i(x) \mid m(x) \bmod p$ by assumption. This is a field of size $p^{\deg p_i(x)}$, which proves that P_i is prime of degree is $f(P_i/p) = \deg p_i(x)$.
We'll now show the P_i are distinct, and in fact comaximal in the sense that $P_i + P_j = \langle 1\rangle$ for $i \neq j$. We've assumed that $p_i(x) \bmod p, p_j(x) \bmod p \in \mathbb{F}_p[x]$ are distinct monic irreducibles in the PID $\mathbb{F}_p[x]$, so we can find a linear combination equal to 1. So write $p_i(x)X(x)+p_j(x)Y(x) = 1 + pQ(x)$ for some polynomials $X, Y \in \mathbb{F}_p[x]$ and $Q \in \mathbb{Z}[x]$. Plug in α and mod out by $I \coloneqq \langle p, p_i(\alpha), p_j(\alpha)\rangle$ to get $o \equiv 1 \bmod I$. But then $1 \in I$ forces $I = \langle 1\rangle$ Thus

$$\begin{aligned}
\langle 1\rangle &= \langle p, p_i(\alpha), p_j(\alpha)\rangle \\
&= \langle p, p_i(\alpha)\rangle + \langle p, p_j(\alpha)\rangle \\
&= P_i + P_j.
\end{aligned}$$

It remains to show that $\langle p\rangle = \prod P_i^{e_i}$. Consider taking powers of P_i:

$$\begin{aligned}
P_i^2 &= \left\langle p^2, p_i(\alpha), p_i(\alpha)^2\right\rangle \subseteq \left\langle p, p_i(\alpha)^2\right\rangle \\
P_i^3 &\subseteq P_i \left\langle p_i, p_i(\alpha)^2\right\rangle \subseteq \left\langle p_i, p_I(\alpha)^3\right\rangle .
\end{aligned}$$

Repeating this will show that $P_i^{e_i} \subseteq \langle p, p_i(\alpha)^{e_i}\rangle$. A similar argument will show

$$\begin{aligned}
\prod P_i^{e_i} &\subseteq \prod \langle p, p_i(\alpha)^{e_i}\rangle \\
&\subseteq \left\langle p, \prod p_i(\alpha)^{e_i}\right\rangle .
\end{aligned}$$

Recall that we can write $m(x) = \prod p_i(x)^{e_i} + pR(x)$ where $R \in \mathbb{Z}[x]$. Plugging in α yields $0 \equiv \prod p_i(\alpha)^{e_i} \bmod p$, so the right-hand side is a multiple of p, making the ideal above redundant. Thus $\prod P_i^{e_i} \subseteq \langle p\rangle$, and since to contain is to divide, we can write

$$\prod P_i^{e_i} = \langle p\rangle\, J,$$

and we want to show $J = \langle 1 \rangle$.
Strategy: take norms. We know $N(p_i)^{e_i} = p^{e_i \deg p_i}$, and so

$$\begin{aligned} N\left(\prod P_i^{e_i}\right) &= \prod N(P_i)^{e_i} \\ &= p^{\sum e_i \deg p_i} \\ &= p^{\deg m(x)} \\ &= p^{[K:\mathbb{Q}]}. \end{aligned}$$

We also have $N(\langle p \rangle) = \#\mathbb{Z}_k / \langle p \rangle = p^{[K:\mathbb{Q}]}$, which forces $N(J) = 1$

■

Remark 21.0.2: An recurring example in this class, due to Dedekind: let $K = \mathbb{Q}(\alpha)$ where α is a root of the irreducible polynomial $x^3 + x^2 - 2x + 8 \in \mathbb{Q}[x]$. We saw that $\mathbb{Z}_K \neq \mathbb{Z}[\alpha]$ but their index divides 2, forcing it to be exactly 2. So the hypothesis of the Dedkind-Kummer theorem are not satisfied, but is the conclusion still true? It turns out that the answer is no, and 2 splits completely as $\langle 2 \rangle = P_1 P_2 P_3$. The proof can be done bare-hands, we won't do it here. This is incompatible with the conclusion of the theorem: we would need the polynomial to factor into three monic linear polynomials mod 2. But there are only 2 different linear polynomials mod 2!

Remark 21.0.3: Every ideal in $\mathbb{Z}_K$ can be generated by at most 2 elements. Or really, "3/2" elements – look it up!

22 | Ch. 18: Units of $\mathbb{Z}_K$

Remark 22.0.1: Setting up some notation: let K be a number field of degree n, and let

- r_1 be the number of real embeddings, i.e. their images are contained in $\mathbb{R}$,
- r_2 be *half* the number of non-real embeddings, since they come in pairs by composing with complex conjugation.

Note that $n = r_1 + 2r_2$. Label the real embeddings $\sigma_1, \cdots, \sigma_{r_1}$, and $\sigma_{r_1+1}, \cdots, \sigma_{r_1+r_2}$ a set of non-real embeddings, where we take one such nonreal embedding from each pair.

Question 22.0.2
What is the structure of $\mathbb{Z}_K^\times$?

Remark 22.0.3: For imaginary quadratic fields, the units were norm 1 in the ring of integers. Usually there were just 2, ± 1, and in $\mathbb{Z}[i]$ there were 4, and $\mathbb{Q}(\sqrt{-3})$ there were 6. All of these formed cyclic groups.

For real quadratic fields, there was a fundamental unit u of infinite order, and all units were $\pm u$, so

the group is abstractly $\mathbb{Z} \times \mathbb{Z}/2$. So everything was a root of unity times a power of the fundamental unit.

Define

$$\mu_K = \left\{ \zeta \in K \;\middle|\; \zeta^n = 1 \text{ for some } n \in \mathbb{Z}^{>0} \right\}.$$

Clearly $\mu_K \subseteq K^\times$, and in fact $\mu_k \subseteq \overline{\mathbb{Z}}$. In fact, it forms a subgroup $\mu_K \leq \mathbb{Z}_k^\times$. The big theorem on the structure of units is the following, which says the same thing as the real quadratic field case happens in general, just with more fundamental units.

Theorem 22.0.4 ***(Dirichlet's Units Theorem).***

There are elements $\varepsilon_1, \cdots, \varepsilon_{r_1+r_2-1} \in \mathbb{Z}_K^\times$ of infinite order such that $\mathbb{Z}_K^\times = \mu_K \prod_{i=1}^{r_1+r_2-1} \langle \varepsilon_i \rangle$ as an internal direct product. So every unit has a unique decomposition of this form. Moreover, $\#\mu_K < \infty$.

Example 22.0.5 ***(?):*** When is $\mathbb{Z}_K^\times$ finite? This happens iff $r_1 + r_2 = 1$, and there are a few cases:

- $r_1 = 1, r_2 = 0$, and since $n = r_1 + 2r_2 = 1$, this forces $K = \mathbb{Q}$.
- $r_1 = 0, r_2 = 1 \iff n = 2$, so this is a quadratic field with no real embeddings, so K is an imaginary quadratic field.

Remark 22.0.6: Our goal will be to prove the units theorem with *some* number g, and we'll show in the next chapter that $g = r_1 + r_2 - 1$ is the right g to choose.

An outline of the proof:

- Define a homomorphism

$$\begin{aligned} \text{Log} : K^\times &\to \mathbb{R}^{r_1+r_2} \\ \alpha &\mapsto [\log|\sigma_1(\alpha)|, \cdots, \log|\sigma_{r_1}(\alpha)|, 2\log|\sigma_{r_1+1}(\alpha)|, \cdots 2\log|\sigma_{r_1+r_2}(\alpha)|,]. \end{aligned}$$

  We'll mostly consider its restriction to $\mathbb{Z}_K^\times$.

- Prove $\ker \text{Log}|_{\mathbb{Z}_K^\times} = \mu_K$ and is finite.
- Prove $\text{Log}(\mathbb{Z}_K)$ is a discrete subgroup of $\mathbb{R}^{r_1+r_2}$.
- Use the fact that such discrete subgroups are lattices.
- Prove the units theorem with g defined as the rank of this lattice.
- Finally prove the rank g is equal to $r_1 + r_2 - 1$.

Lemma 22.0.7 *(?).*
Let $M \in \mathbb{R}^{>0}$ and let $\alpha \in \mathbb{Z}_K$. If for all embeddings $\sigma : K \hookrightarrow \mathbb{C}$ we have bounds $|\sigma(\alpha)| \leq M$, then α is a root of a polynomial in

$$P_{n,m} \coloneqq \left\{ x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x] \;\middle|\; |a_i| \leq \binom{n}{i} M^{n-i} \right\}.$$

Note that this is a finite set.

Proof (?).
Note that α is a root of its **field polynomial**

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

Since $\alpha \in \mathbb{Z}_K$, this polynomial $f \in \mathbb{Z}[x]$. So it suffices to show that $f \in P_{n,m}$. It's degree n, the coefficients are integers, but why do they satisfying the bound? Expanding the multiplication, there are $\binom{n}{i}$ prducts each of which involves $n - i$ of the $\sigma_i(\alpha)$, which is bounded.

■

Remark 22.0.8: We'll first show the kernel of Log is finite, then it'll be easy to see it's μ_K.

Proposition 22.0.9 *(?).*

$$\# \ker \operatorname{Log}|_{\mathbb{Z}_K^\times} < \infty.$$

Proof (?).
Suppose $\alpha \in \mathbb{Z}_K^\times$ and $\operatorname{Log}(\alpha) = \mathbf{0}$. This says that $|\sigma_i(\alpha)| = 1$ for all embeddings $\sigma_i : K \hookrightarrow \mathbb{C}$. Applying the lemma above with $M = 1$, α is a root of a polynomials in $P_{n,1}$, each of which has at most n roots. So there are only finitely many possibilities for α.

■

Proposition 22.0.10 *(?).*

$$\ker \operatorname{Log}|_{\mathbb{Z}_K^\times} = \mu_K.$$

Proof (?).
Start with $\zeta \in \mu_K$, then under any σ, $\sigma(\zeta)$ is a complex root of unity. So $|\sigma(\zeta)| = 1$, and by the previous result, $\operatorname{Log}(\zeta) = \mathbf{0}$. So $\mu_K \subseteq \ker \operatorname{Log}$.
Conversely suppose $\zeta \in \ker \operatorname{Log}$, which in particular is a group. Suppose $\# \ker \operatorname{Log} = n$, since we know it's finite. Then $\xi^n = e = 1$ in this group, making it an nth root of unity.

■

Remark 22.0.11: Note that μ_K is always cyclic This follows because for K a field, it's an exercise

that any finite subgroup $H \leq \mathbb{G}_m(K)$, it is always cyclic. So we've written $\mathbb{Z}_K = C_q \times \mathbb{Z}^{r_1+r_2-1}$ as an abstract group.

23 Ch. 18: Dirichlet's Units Theorem Part I (Friday, May 21)

Remark 23.0.1: Some notation introduced last time: for K a number field, $[K : \mathbb{Q}] = n$ the degree, set $\sigma_1, \cdots, \sigma_{r_1}$ to be the real embeddings, and $\sigma_{r_1+1}, \cdots, \sigma_{r_1+r_2}$ (along with their complex conjugates) to be the nonreal embeddings into $\mathbb{C}$. Let $\mu_K \coloneqq \left\{ z \in K \;\middle|\; z^n = 1, n \in \mathbb{N} \right\}$ be the nth roots of unity Recall Dirichlet's unit theorem: there are $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{r_1+r_2-1} \in \mathbb{Z}_K^\times$ of infinite order such that

$$\mathbb{Z}_K^\times = \mu_K \times \prod_{i \leq r_1+r_2-1} \langle \mu_i \rangle .$$

Moreover, $\#\mu_K < \infty$.

Remark 23.0.2 ***(An outline of the proof):*** Set $d = r_1 + r_2$. We define a homomorphism

$$\begin{aligned} \mathrm{Log} : K^\times &\to \mathbb{R}^d \\ \alpha &\mapsto [\log|\sigma_i(\alpha)|, \cdots, \log|\sigma_{r_1}(\alpha)|, 2\log|\sigma_{r_1+1}(\alpha)|, \cdots, 2\log|\sigma_{r_1+r_2}(\alpha)|,]. \end{aligned}$$

Note that we only used half of the non-real embeddings, but made up for it by including a 2! We'll mostly be concerned with its restriction to $\mathbb{Z}_K^\times$.

1. Show that the restriction has finite kernel μ_k – we've completed this.
2. Show $\mathrm{Log}(\mathbb{Z}_K^\times)$ is discrete as a subgroup of $\mathbb{R}^d$
3. Use the fact that every discrete subgroup of $\mathbb{R}^d$ is a lattice, the $\mathbb{Z}$-span of linearly independent vectors.
4. Prove the units theorem with $d-1$ replaced by $g = \operatorname{rank} \mathrm{Log}(\mathbb{Z}_K^\times)$.
5. Deferred to next chapter: show $g = r_1 + r_2 - 1$.

23.1 Step 2: Discreteness

Definition 23.1.1 (Discrete lattices)
Let $d \in \mathbb{Z}^{\geq 0}$ and let $\Lambda \leq \mathbb{R}^d$ be a subgroup. Then Λ is **discrete** iff for every $R > 0$, $\Lambda \cap B_R(0)$ is a finite set, where $B_R(0)$ is a ball of radius R about 0.

Proposition 23.1.2 *(?).*
$\mathrm{Log}(\mathbb{Z}_K^\times)$ is discrete in $\mathbb{R}^d$ for $d = r_1 + r_2$.

Proof (?).
Let $R > 0$, we'll show that there are only finitely many $\alpha \in \mathbb{Z}_K^\times$ for which $\mathrm{Log}(\alpha) \in B_R(0)$. This forces $\log|\sigma(\alpha)| \leq R$ for all $\sigma : K \hookrightarrow \mathbb{C}$. Thus $|\sigma(\alpha)| \leq e^R$ for all such embeddings. By a previous lemma, this makes α a root of a polynomial in some finite set P_{n,e^R} – what this set is isn't important, just recall that once you have a bound on the embeddings, this gives a bound on the coefficients of the field polynomial.

■

23.2 Step 3

Theorem 23.2.1 *(?).*
Every discrete subgroup of $\mathbb{R}^d$ is a lattice.

Proof (?).
See the book!

■

23.3 Step 3

Theorem 23.3.1 ***(Weak units theorem).***
Let g be the rank of $\mathrm{Log}\,\mathbb{Z}_K^\times \subseteq \mathbb{R}^{r_1+r_2}$. Then there are fundamental units $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_g \in \mathbb{Z}_K^\times$ of infinite order such that

$$\mathbb{Z}_K^\times = \mu_K \times \prod_{i \leq g} \langle \varepsilon_i \rangle .$$

Note that this is the same theorem from before, just with d replaced by g.

Proof (?).
Using that g is by definition the rank of the lattice $\mathrm{Log}\,\mathbb{Z}$, choose $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_g \in \mathbb{Z}_K^\times$ such that the $\mathrm{Log}(\varepsilon_i)$ are $\mathbb{R}$-linearly independent and their $\mathbb{Z}$-span is the lattice. Let $\varepsilon \in \mathbb{Z}_K^\times$ be any unit, then $\mathrm{Log}(\varepsilon) \in \mathrm{Log}\,\mathbb{Z}_K^\times$, so there are integers $n_1, n_2, \cdots, n_g \in \mathbb{Z}$ such that

$$\mathrm{Log}(\varepsilon) = \sum n_i \,\mathrm{Log}(\varepsilon_i).$$

Hence

$$\operatorname{Log}\left(\varepsilon / \prod_{i\leq g} \varepsilon_i^{n_i}\right) = \mathbf{0}.$$

So it's in the kernel and equal to some $\zeta \in \mu_K$, so we can write $\varepsilon = \zeta \prod_{i\leq g} \varepsilon_i^{n_i}$. This representation of ε is unique, in the sense that ζ and the n_i are uniquely determined. Why? For any other representation, applying Log would kill the ζ part and write $\operatorname{Log}(\varepsilon) = \sum n_j \varepsilon_j$ in the basis ε_j. So the n_i are unique, and ζ is just obtained by dividing, so it can be recovered uniquely as well.

■

Remark 23.3.2: Our goal is to now show $g = r_1 + r_2 - 1$, which is hard. It's easier to obtain a bound instead.

Proposition 23.3.3 ***(Lattice rank bound).***
Let $g = \operatorname{rank} \operatorname{Log}(\mathbb{Z}_K^\times)$, then

$$g \leq r_1 + r_2 - 1.$$

Lemma 23.3.4 ***(?).***
Let $\Lambda \subseteq \mathbb{R}^d$ be a lattice, then $\operatorname{rank} \Lambda = \dim_{\mathbb{R}} V$ where V is the smallest subspace of $\mathbb{R}^d$ containing Λ.

Proof (?).
Let $g \coloneqq \operatorname{rank} \Lambda$, and write $\Lambda = \sum_{i\leq g} \mathbb{Z}\mathbf{v}_i$ where the $\mathbf{v}_i$ are $\mathbb{R}$-linearly independent. Then $V = \sum_{i\leq g} \mathbb{R}\mathbf{v}_i$, and $\dim_{\mathbb{R}} V = g = \operatorname{rank} \Lambda$.

■

Proof (of proposition, lattice rank bound).
Let $\mathbf{w} = [1, 1, \cdots, 1] \in \mathbb{R}^{r_1+r_2}$. If $\alpha \in \mathbb{Z}_K^\times$, then dotting sums the components, so

$$\mathbf{w} \cdot \operatorname{Log} \alpha = \sum_{i\leq r_1} \log|\sigma_i(\alpha)| + 2 \sum_{r_1+1\leq i\leq r_1+r_2} \log|\sigma_i(\alpha)|.$$

Note that $|\sigma_i(\alpha)| = \left|\overline{\sigma(\alpha)}\right|$, so because we have a 2 here, we could have written this as

$$\begin{aligned}
\mathbf{w} \cdot \operatorname{Log} \alpha &= \sum_{\sigma: K\hookrightarrow\mathbb{C}} \log|\sigma(\alpha)| \\
&= \log \prod_{\sigma: K\hookrightarrow\mathbb{C}} |\sigma(\alpha)| \\
&= \log|N(\alpha)| \\
&= 0,
\end{aligned}$$

since $\alpha \in \mathbb{Z}_K^\times \implies N(\alpha) = \pm 1$. This says that $\mathrm{Log}(\mathbb{Z}_K^\times) \subseteq \mathbf{w}^\perp$, which has codimension 1 and thus dimension $r_1 + r_2 - 1$. Now $V \subseteq \mathbf{w}^\perp$. so its rank is bounded by this dimension. So $g \leq r_1 + r_2 - 1$.

■

24 | Ch. 20: Unit Theorem, Part II

Remark 24.0.1: We still need to prove that this is an equality. We'll start with some geometric preliminaries.

Definition 24.0.2 (The Minkowski Embedding)
The **Minkowski embedding** of K is the map

$$\begin{aligned}\iota : K &\to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \\ \alpha &\mapsto [\sigma_1(\alpha), \cdots, \sigma_{r_1}(\alpha), \sigma_{r_1+1}(\alpha), \cdots, \sigma_{r_1+r_2}(\alpha)].\end{aligned}$$

Identify $\mathbb{C} \cong \mathbb{R}^2$ using $a+bi \mapsto [a,b]$, which identifies the codomain above with $\mathbb{R}^{r_1} \times \mathbb{R}^{2r_2} = \mathbb{R}^n$. So we view $\iota : K \to \mathbb{R}^n$.

Remark 24.0.3: Note ι is injective and $\mathbb{Q}$-linear.

Proposition 24.0.4 ***(Extremely important).***
$\iota(\mathbb{Z}_K)$ is a lattice of full rank in $\mathbb{R}^n$.

Proof (?).
Why is this a lattice? We'll show it's a discrete subgroup.
Let $R > 0$, then if $\alpha \in \mathbb{Z}_K$ and $\iota(\alpha) \in B_R(0)$, then $|\sigma(\alpha)| \leq R$ for all $\sigma : K \hookrightarrow \mathbb{C}$. This forces α to be a root of one of finitely many polynomials in $P_{n,R}$.
Now let $g \coloneqq \operatorname{rank} \iota(\mathbb{Z}_K)$ as a lattice. This is a free abelian group of rank g, so isomorphic to $\mathbb{Z}^g$ since it's the $\mathbb{Z}$-span of g linearly independent elements. On the other hand, by the integral basis theorem, $\mathbb{Z}_K$ is a free abelian group of rank n. Since ι is injective, $\iota(\mathbb{Z}_K)$ is free of rank n, and a fact from algebra implies $n = g$.

■

Remark 24.0.5: Since $\iota(\mathbb{Z}_K$ is a full rank lattice, $\operatorname{covol} \iota(\mathbb{Z}_K)$ is well-defined, where the covolume is the volume of the fundamental parallelepiped spanned by any generating set, and is measured by the absolute value of the determinant of the matrix of basis elements. It turns out that the covolume is the discriminant from before, but we don't need the exact value at the moment.

Remark 24.0.6: We'll now make some further reductions. Recall that $g \coloneqq \operatorname{rank} \mathrm{Log}(\mathbb{Z}_K^\times) = \dim_{\mathbb{R}} V$, where V is the smallest subspace of $\mathbb{R}^{r_1+r_2}$ containing $\mathrm{Log}(\mathbb{Z}_K^\times)$. Recall the rank-nullity

theorem:

$$\dim_{\mathbb{R}} V + \dim_{\mathbb{R}} V^\perp = r_1 + r_2 \implies g = \dim_{\mathbb{R}} V = r_1 + r_2 - \dim_{\mathbb{R}} V^\perp.$$

the goal is to show $\dim_{\mathbb{R}} V^\perp = 1$. We know $\mathbf{w} := [1, 1, \cdots, 1] \in V^\perp$, so it suffices to show every element of $V^\perp$ is a multiple of $\mathbf{w}$. Suppose not, then there's an element of $V^\perp$ of the form $[c_1, c_2 \cdots, c_j, 0]$ by subtracting a suitable multiple of $\mathbf{w}$. Not all of the c_i are zero, since this would mean the original was a multiple of $\mathbf{w}$. Define a map

$$\begin{aligned} F : K^\times &\to \mathbb{R} \\ \alpha &\mapsto [c_1, c_2, \cdots c_{r_1+r_2-1}, 0] \cdot \operatorname{Log}(\alpha). \end{aligned}$$

Now note that $F(\mathbb{Z}_K^\times) = 0$, since $V \supseteq \operatorname{Log}(\mathbb{Z}_K)$.

Proposition 24.0.7 ***(?).***
Let $c_1, c_2, \cdots, c_{r_1+r_2-1} \in \mathbb{R}$ not all 0. Then if F is defined as above, $F(\mathbb{Z}_K^\times) \neq 0$.

Remark 24.0.8: This requires some delicate inequalities, and an application of Minkowski's convex body theorem.

Lemma 24.0.9 ***(Key lemma).***
There is a sequence of nonzero $\alpha \in K$ such that

- $|F(\alpha)| \to \infty$, but
- $|N(\alpha)| < C_1 = C_1(K, c_1, \cdots, c_{r_1+r_2-1})$ not depending on α.

Proof (of proposition, assuming the key lemma).
Note that there are only finitely many ideals of $\mathbb{Z}_K$ of norm bounded by any constant C_1. We saw this for quadratic fields: if $N(J) = m$, which by Lagrange's theorem yields $1 + 1 + \cdots 1 = m \equiv 0 \bmod J$. So $m \in J$ and thus $J \mid m$. But by unique factorization, any ideal only has finitely many divisors, so there are only finitely many possible values of m.
Note also that $|N(\alpha)| = N(\langle\alpha\rangle) < C_1$, so there are only finitely many such ideals. So given an infinite sequence of αs, there are only finitely many different principal ideals they generate. So by the pigeonhole principle, we can pass to a subsequence such that $\langle a \rangle$ is constant. Note that F can't be constant on this sequence, since $F(\alpha) \to \infty$, so we can choose α_1, α_2 such that

$$\langle\alpha_1\rangle = \langle\alpha_2\rangle \quad \text{but} \quad F(\alpha_1) \neq F(\alpha_2).$$

If this happens, then $\alpha_1/\alpha_2 \in \mathbb{Z}_K^\times$, and

$$F(\alpha_1/\alpha_2) = F(\alpha_1) - F(\alpha_2) \neq 0.$$

So we have $F(\mathbb{Z}_K^\times) \neq 0$, since we've found a unit that maps to a nonzero element.

■

25 | Ch. 20 Continued (Friday, May 21)

Remark 25.0.1: Goal of Ch.18: prove that units theorem where the rank is left unspecified, and we proved it for g the rank of a certain lattice. For Ch.20, we want to show g is the right number! Recall the log function:

$$\mathrm{Log} : K^\times \to \mathbb{R}^{r_1+r_2}$$

where we take the $\log|-|$ of the real embeddings and $2\log|-|$ of one of each pair of complex embeddings. We know $\mathrm{Log}\,\mathbb{Z}_K^\times \subseteq \mathbb{R}^{r_1+r_2}$ is a lattice of rank $g \leq r_1 + r_2 - 1$, and we want to show equality. We showed that everything follows if we establish the key lemma: if $c_1, \cdots, c_{r_1+r_2-1} \in \mathbb{R}$ are not all zero, defin

$$F(\alpha) \coloneqq [c_1, \cdots, c_{r_1+r_2-1}, 0] \cdot \mathrm{Log}(\alpha).$$

We want to show there is a sequence of $\alpha \in \mathbb{Z}_K$ such that $|F(\alpha)| \to \infty$ with $|N(\alpha)| \leq C_1$ bounded, where C_1 doesn't depend on α. We want to make the dot product above large while keeping the norms small while making linear combinations of $\log|\sigma_i(\alpha)|$ large. The only embeddings that show up are the ones labeled up to $r_1 + r_2 - 1$, since the last component is zero, and we'll show that we can essentially control the image of α under these embeddings while keeping its norm bounded.

Recall the Minkowski embedding realizes K as a subspace of Euclidean space:

$$\iota : K \to \mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2},$$

where the first components are the first r_1 real embeddings and the latter are the complex embeddings. Identifying the target with $\mathbb{R}^n$, we said last time that $\iota(\mathbb{Z}_K) \subseteq \mathbb{R}^n$ is a full rank lattice, so of rank n, which thus has a finite nonzero covolume.

We'll use this with Minkowski's convex body theorem: suppose R is a region in $\mathbb{R}^d$ which is centrally symmetric and convex, and Λ is a full rank lattice in $\mathbb{R}^d$. Then if $\mathrm{vol}(R) > w^d \,\mathrm{covol}(\Lambda)$, R contains a nonzero point $x \in \Lambda$. How we'll use these: apply s the convex body theorem on $\Lambda = \iota(\mathbb{Z}_K)$, and use this to locate the types of α we want.

Remark 25.0.2: Given $\lambda_1, \cdots, \lambda_{r_1+r_2} \in \mathbb{R}^{\geq 0}$, denote this by the vector λ. Define

$$R_\lambda \coloneqq \left\{ [x_1, \cdots, x_{r_1+r_2}] \in \mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2} \;\middle|\; |x_i| \leq \lambda_i \ \forall i \right\} \subseteq \mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2} \cong \mathbb{R}^n.$$

This is clearly centrally symmetric: negating anything lands in the region since we're taking absolute values. It's less clearly convex, but this follows from the triangle inequality. More intuitively, it's a product of discs and boxes, each of which are convex. One can compute its volume as

$$\mathrm{vol}\, R_\lambda = \prod_{i \leq r_1} 2\lambda_i \prod_{j \leq r_2} \pi \lambda_{r_1+j}^2 = 2^{r_1}\pi^{r_2} \prod_{i \leq r_1} \lambda_i \prod_{j \leq r_2} \lambda_{r_1+j}^2,$$

since the first r_1 components form boxes and the last form discs.

As a convention, we'll fill out $r_1 + r_2$ tuples to $r_1 + 2r_2$ tuples in the following way: for $1 \leq i \leq r_2$, set

- $\sigma_{r_1+r_2+i} = \overline{\sigma_{r_1+i}}$, and
- $\lambda_{r_1+r_2+i} = \lambda_{r_1+i}$.

This introduces the remaining embeddings from each conjugate pair and assigns it the same λ_i. We can now write

$$\operatorname{vol} R_\lambda = 2^{r_1}\pi^{r_2}\prod_{i\le n}\lambda_i,$$

since each λ now appears twice in the product.

Proof (of key lemma).
Rather than working with arbitrary tuples, we'll only consider $\lambda_1, \lambda_2, \cdots, \lambda_{r_1+r_2} \in \mathbb{R}^{\ge 0}$ contained such that

$$\operatorname{vol} R_\lambda = 2\left(2^n \operatorname{covol} \iota(\mathbb{Z}_K)\right),$$

noting that the parenthesized quantity is exactly twice what's needed in Minkowski's theorem. This allows one to choose the first $r_1 + r_2 - 1$ freely, and the last will be determined uniquely. By Minkowski's theorem, there is an $\alpha \in \mathbb{Z}_K$ nonzero with $\iota(\alpha) \in R_\alpha$. Hence

$$|\sigma_i(\alpha)| \le \lambda_i \qquad\qquad \forall i = 1, 2, \cdots, n.$$

Consequently,

$$\begin{aligned} |N\alpha| &= \prod_i |\sigma_i(\alpha)| \le \prod \lambda_i \\ &= \frac{\operatorname{vol} R_\lambda}{2^{r_1}\pi^{r_2}} \\ &= C_1. \end{aligned}$$

Notice that

$$\begin{aligned} 1 \le |N\alpha| &= \prod_i |\sigma_i(\alpha)| \\ &= |\sigma_j(\alpha)| \prod_{i\ne j} |\sigma_i(\alpha)| \\ &\le |\sigma_j(\alpha)| \prod_{i\ne g} \lambda_i \\ &\le \frac{|\sigma_j|}{\lambda_j} \prod_i \lambda_i \\ &\le \frac{|\sigma_j|}{\lambda_j} C_1. \end{aligned}$$

Rearranging yields

$$|\sigma_j(\alpha)| \ge C_1^{-1}\lambda_j.$$

Thus for every $1 \le j \le n$, we have an inequality

$$C_1 \int \lambda_j \le |\sigma_j(\alpha)| \le \lambda_j.$$

Taking logarithms yields

$$\log C_1^{-1} \le \log|\sigma_j(\alpha)| - \log \lambda_j \le 0.$$

Recalling the definition of $\mathrm{Log}(\alpha)$, and the above inequality says we know $\log|\sigma_j(\alpha)|$ up to a constant – it's about $\log\lambda_j$. So setting

$$\mathbf{L} \coloneqq [\log\lambda_1, \cdots, \lambda_{r_1}, 2\log\lambda_{r_1+1}, 2\log\lambda_{r_1+r_2}],$$

we have $\mathbf{L} \approx \mathrm{Log}\,\alpha$, where $\approx$ means each component is off by at most a constant. So $|\mathrm{Log}\,\alpha - \mathbf{L}| \leq C_2$, some other constant. We want to understand

$$F(\alpha) \coloneqq [c_1, \cdots, c_{r_1+r_2-1}, 0] \cdot \mathrm{Log}(\alpha) \approx F(\alpha) \coloneqq [c_1, \cdots, c_{r_1+r_2-1}, 0] \cdot \mathbf{L}.$$

How can we estimate the error? By Cauchy-Schwarz, the difference is bounded by

$$\|[c_1, \cdots, c_{r_1+r_2-1}, 0]\| \cdot \|\mathrm{Log}\,\alpha - \mathbf{L}\| \leq \|[c_1, \cdots, c_{r_1+r_2-1}, 0]\| C_2 \coloneqq C_3.$$

We've show that for any choice of $\lambda_1, \cdots, \lambda_{r_1+r_2}$ satisfying the volume condition, one can find α where $|N\alpha|$ is bounded and all of the above inequalities hold. In particular, $F(\alpha) \approx \mathbf{c} \cdot \mathbf{L}$. We claim we can now choose αs to make $|F(\alpha)| \to \infty$. Every choice of λ_is yield an α, and the c_i in $\mathbf{c}$ are fixed, so $\mathbf{c} \cdot \mathbf{L}$ is just a function of the λ_i. So to finish the prove, we need to show we can pick λ_i satisfying the volume condition but making $\mathbf{c} \cdot \mathbf{L}$ as large as we want. This correspondingly makes $F(\alpha)$ large, since they differ by at most a constant.
Here's why we can do this: we assumed not all c_i were zero, so fix an i where $c_i \neq 0$. Choose λ_j with λ_i very large, and $\lambda_{j'} = 1$ for $j = 1, \cdots, r_1 + r_2 - 1$ not including i. Then choose $\lambda_{r_1+r_2}$ as determined by the volume condition. The claim is that we're done. The dot product has a zeroth $r_1 + r_2$ component, so the dot product doesn't see $\sigma_{r_1+r_2}$. Recall $\mathbf{L}$ is a function of the λ_i, since the whole point was that we removed the dependence on α, and is given by

$$\mathbf{L} = [\log\lambda_1, \cdots, \lambda_{r_1}, 2\log\lambda_{r_1+1}, \cdots, 2\log\lambda_{r_1+r_2}].$$

What survives the dot product? We're taking $\log(1) = 0$ in the $j \neq i$ components, and in the ith component we have at most $2\log\lambda_i \cdot c_i$, where the λ_i is a large number. So we can make $\mathbf{c} \cdot \mathbf{L}$ as large as we want.

■

26 Ch. 21: Applications of Minkowski's Theorem

Proposition 26.0.1 *(?).*
Recall the Minkowski embedding, $\iota : K \to \mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2}$, where we concatenate all of the real embeddings followed by the complex embeddings. View the target as $\mathbb{R}^n$, then there is a formula:

$$\mathrm{covol}\,\iota(\mathbb{Z}_K) = 2^{-r_2}\sqrt{|\Delta_K|}.$$

Proof (?).
Pick an integral basis $\omega_1, \omega_2, \cdots, \omega_n$ for K, then $\iota(\omega_1), \cdots, \iota(\omega_n)$ span $\iota(\mathbb{Z}_K)$ over $\mathbb{Z}$. It suffices to show that if A is the $n \times n$ matrix with ith column $\iota(\omega_i)$, then $|\det A|$ is the right-hand side in the formula. If this is true, the $\iota(w_i)$ are linearly independent over $\mathbb{R}$, otherwise the determinant would be $\mathbb{R}$, so they're a basis for the lattice $\iota(\mathbb{Z}_K)$, and this determinant is precisely the formula for the covolume of a lattice. We claim the matrix looks like the following.

$$\begin{bmatrix} \sigma_1(\omega_1) & \cdots & \sigma_1(\omega_1) \\ \vdots & \cdots & \vdots \\ \sigma_{r_1}(\omega_1) & \cdots & \sigma_{r_1}(\omega_1) \\ \Re\sigma_{r_1+1}(\omega_1) & \cdots & \Re\sigma_{r_1+1}(\omega_1) \\ \Im\sigma_{r_1+1}(\omega_1) & \cdots & \Im\sigma_{r_1+1}(\omega_1) \\ \vdots & \cdots & \vdots \\ \Re\sigma_{r_1+r_2}(\omega_1) & \cdots & \Re\sigma_{r_1+r_2}(\omega_1) \\ \Im\sigma_{r_1+r_2}(\omega_1) & \cdots & \Im\sigma_{r_1+r_2}(\omega_1) \end{bmatrix}.$$

Let $D_{ij} \coloneqq [\sigma_i(\omega_j)]$, then by tracking row operations that transform D to A, $\det(A) = (-i/2)^{r_2} \det(D)$. So

$$|\det A| = 2^{-r_2} |\det D|.$$

Since $\det(D)^2 = \Delta_K$, then taking square roots yields $|\det D| = \sqrt{|\Delta_K|}$.

■

Remark 26.0.2: We now now the covolume of this lattice, we'd like to do this not just for $\mathbb{Z}_K$ but also its ideals.

Lemma 26.0.3 ***(?).***
If $I \trianglelefteq \mathbb{Z}_K$, then I is a free abelian group of rank n.

Proof (?).
Take any nonzero $\alpha \in I$, then $\alpha\mathbb{Z}_K \subseteq I \subseteq \mathbb{Z}_K$. The outer terms are free abelian of rank n, so I must be as well.

■

Proposition 26.0.4 ***(?).***
If $I \trianglelefteq \mathbb{Z}_K$ is nonzero, then $\iota(I)$ is a full rank lattice in $\mathbb{R}^n$ and

$$\operatorname{covol} \iota(I) = 2^{r_2} \sqrt{|\Delta_K|} N(I).$$

27 Ch. 21: Applications of Minkowski's Theorem (Friday, May 21)

Remark 27.0.1: Recall that we're considering the Minkowski embedding $\iota : K \to \mathbb{R}^n$. We saw that $\iota(\mathbb{Z}_K) \subseteq \mathbb{R}^n$ is a full rank lattice whose covolume is the following:

$$\operatorname{covol} \iota\mathbb{Z}_K = 2^{r_2}\sqrt{|\Delta_K|}.$$

We wanted to make this work for arbitrary ideals $I \trianglelefteq \mathbb{Z}_K$, and the proposition was that

$$\operatorname{covol} \iota I = 2^{r_2}\sqrt{|\Delta_K|}N(I).$$

Proof (?).
We know I is free abelian of rank n, so choose a $\mathbb{Z}$-basis $\omega_1, \omega_2, \cdots, \omega_n$ for $\mathbb{Z}_K$ and $\theta_1, \theta_2, \cdots, \theta_n$ for I. There is some $A \in \operatorname{Mat}(n \times n; \mathbb{Z})$ such that

$$[\theta_1, \theta_2, \cdots, \theta_n] = [\omega_1, \omega_2, \cdots, \omega_n]A.$$

The index-determinant theorem tells us that $\#\mathbb{Z}_K/I = |\det A|$, and this is equal to $N(I)$. Now apply ι to both sides above to obtain $n \times n$ matrix with the $\iota(\theta_i)$ and $\iota(\omega_i)$ as column vectors:

$$\left[\iota{\theta^t}_1, \iota{\theta^t}_2, \cdots, \iota{\theta^t}_n\right] = [\iota{\omega^r}_1, \iota{\omega^r}_2, \cdots, \iota{\omega^r}_n]A.$$

Taking $|\det -|$ on both sides, we get

$$\operatorname{covol} \iota(I) = \operatorname{covol} \iota(\mathbb{Z}_K)|\det A| = \operatorname{covol} \iota(\mathbb{Z}_K)N(I).$$

■

27.1 Minkowski's Class Group Bound

Remark 27.1.1: We've proved that $\#\mathrm{Cl}(\mathbb{Z}_K) < \infty$ for a general number field, which is in the book and uses Dirichlet's approximation theorem and goes similarly to how it did for quadratic fields. That proof isn't so good if you want to concretely compute the class group: what you'd like would be an upper bound on the smallest ideal in any ideal class. This would allow computing all ideals up to that bound and discerning the structure based on these finitely many ideals.

Proposition 27.1.2 ***(Minkowski's Bound).***
Every ideal class contains a representative I with $N(I) \leq M_K$, where

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

Remark 27.1.3: The precise form of this bound isn't important yet. We can prove using this bound that some specific number fields have class number 1. How do we prove this?

Lemma 27.1.4*(?).*
Let $B > 0$, then the following are equivalent:

1. Every ideal class contains a representative of norm at most B,
2. Every nonzero ideal $I \trianglelefteq \mathbb{Z}_K$ contains a nonzero α with $|N\alpha| \leq NN(I)$.

Proof (?).
2 $\implies$ 1: done for quadratic fields.
1 $\implies$ 2: Start with $I \trianglelefteq \mathbb{Z}_K$ nonzero. Pick $J \in [I]^{-1}$ with $N(J) \leq B$ using (1). Then IJ is principal, so write $IJ = \langle\alpha\rangle$. This shows that $I \mid \langle\alpha\rangle$, so $\alpha \in I$ since to divide is to contain. Moreover

$$\begin{aligned} |N(\alpha)| &= N(\langle\alpha\rangle) \\ &= N(I)N(J) \\ &\leq BN(I). \end{aligned}$$

■

Remark 27.1.5: So we've reduced the problem, and it suffices to prove (2) in the above lemma taking $B = M_K$ from above. Idea: we'll introduce a region $R \subseteq \mathbb{R}^n$ which is centrally symmetric, convex, and $\text{vol}(R) > 2^n \operatorname{covol} \iota(I)$ big enough. Then we'll be guaranteed an $\alpha \in I$ nonzero with $\iota(\alpha) \in R$, coming from Minkowski's theorem.

What does this tell us? The components of $\iota(\alpha)$ are the images of α under embeddings σ_i. If we know these images, we can recover the norm as the product, so one ought to be to rig the region R in order to control the size of α. So we'll choose R such that

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

Question 27.1.6
What kinds of regions R correspond to $|N(\alpha)| \leq X$ for an arbitrary X?

Answer 27.1.7
It's precisely the following region:

$$\left\{ [x]r_1 + r_2 \in \mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2} \;\middle|\; \prod_{i \leq r_1} |x_i| \prod_{j \leq r_2} |x_{r_1+j}|^2 \leq X \right\}.$$

Note that this is centrally symmetric, but the convexity may be a problem.

Example 27.1.8 *(?):* Let K be a real quadratic field, so $r_1 = 2, r_2 = 0$. Then the region above is $R_0 = \left\{(x_1, x_2) \;\middle|\; |x_1 x_2| \leq X\right\}$, which looks like the following:

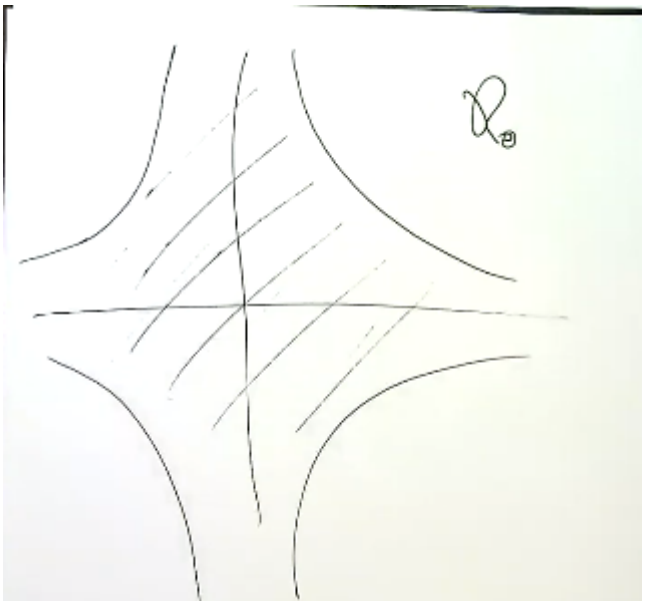


Figure 1: image_2021-05-22-17-53-50

The solution: choose a convex region inside R_0 and apply Minkowski's theorem, noting that this maintains the bound. For example, one can take

$$R = \left\{(x_1, x_2) \;\middle|\; |x|_1 + |x|_2 \leq 2x^{1/2}\right\},$$

which is a diamond lying inside R_0 due to the AM-GM inequality.

Proposition 27.1.9 ***(AM-GM Inequality).***
Let $t_1, t_2, \cdots, t_m \geq 0$, then

$$\frac{1}{m}\sum_{i\leq m} t_i \geq \left(\prod_{i\leq m} t_i\right)^{1/m}.$$

Remark 27.1.10: So we'll take the region

$$R \coloneqq \left\{[x_1, x_2, \cdots, x_{r_1+r_2}] \in \mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2} \;\middle|\; \frac{1}{n}\left(\sum_{i\leq r} |x_i| + 2\sum_{r_1+1\leq j\leq r_1+r_2} |x_j|\right) \leq X^{1/n}\right\}.$$

Then by AM-GM, $R \subseteq R_0$ and $n = r_1 + r_2$. This is still centrally symmetric, and now convex using the triangle inequality. When is $\operatorname{vol} R > 2^n \operatorname{covol} \iota(I)$? We'll need to compute the volume of R, which is an involved exercises in multivariable calculus. This is done in the book, and it turns out that

$$\operatorname{vol}(R) = 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\frac{n^n}{n!}X.$$

Recall that

$$2^n \operatorname{covol} \iota(I) = 2^n 2^{-r_2} \sqrt{|\Delta_K|},$$

and solving this linear equality for X yields $X > M_K N(I)$ as defined before.

Now apply Minkowski's theorem: for any $X > M_K N(I)$ there is a nonzero $\alpha \in I$, there is a nonzero $\alpha \in I$ with $\iota(\alpha) \in R$, and hence $|N(\alpha)| \leq X$. Note that the inequalities don't quite match up as-is, since we can't take $X = M_K N(I)$. Does this imply that we can find an α with $|N(\alpha)| \leq X$? The answer is yes, because we can choose X with $\lfloor X \rfloor = \lfloor M_K M(I) \rfloor$. Then $|N(\alpha)| \leq X \implies |N(\alpha)| \leq \lfloor X \rfloor = \lfloor M_K N(I) \rfloor$, since the left-hand side is an integer.

27.2 Example: Showing Number Fields are PIDs using Dedekind-Kummer and the Minkowski Bound

Example 27.2.1 *(?):* Let $K = \mathbb{Q}(\sqrt[3]{3})$. Then $n = 3$, and $r_1 = 1, r_2 = 1$ since embeddings permute the roots of $x^3 - 3$, which has exactly one real root. We need the discriminant, so we need an integral basis, in which case it helps to know $\mathbb{Z}_K$. By a homework problem, if $K = \mathbb{Q}(\sqrt[3]{d})$ with d squarefree and $d \not\equiv \pm 1 \bmod 9$, then $\mathbb{Z}_K$ is what you guess it'd be! So here $\mathbb{Z}_K = \mathbb{Z}[\sqrt[3]{3}]$, and thus

$$\Delta_K = \Delta(1, 3^{1/3}, 3^{2/3}) = \Delta(x^2 - 3) = -3^5.$$

Thus

$$M_K = \left(\frac{4}{\pi}\right) \frac{3!}{3^3} \sqrt{3^5} \approx 4.42,$$

and thus we know every ideal class contains a representative of norm at most 4, using that $N(I)$ is an integer. Any such I is a product of ideals of norms $2, 3, 4$. Prime ideals of norm 2 or 4 lie above the prime 2, and of norm 3 lie above 3. If we can show that every prime ideal with $N(I) = 2, 3, 4$ is principal, then I will be a product of principal ideals and thus principal. Then since every class contains such an I, $\mathrm{Cl}(\mathbb{Z}_K)$ is trivial. We look at all of the primes above 2 and 3 using Dedekind-Kummer, which says the factorization of $\langle p \rangle$ mirrors the factorization of $x^2 - 3 \bmod p$.

Note that if $\mathbb{Z}(\sqrt[3]{3}) \neq \mathbb{Z}_K$, there'd be some exceptional primes p to worry about, but since these are equal here this is literally true for all p.

So we factor polynomials. First mod 2:

$$x^2 - 3 = x^3 - 1 = (x - 1)(x^2 + x + 1),$$

where the second term is an irreducible quadratic with no roots in $\mathbb{F}_2$. This yields

$$\langle 2 \rangle = \left\langle 2, \sqrt[3]{3} - 1 \right\rangle \left\langle 2, \left(\sqrt[3]{3}\right)^2 + \sqrt[3]{3} + 1 \right\rangle.$$

Next mod 2:

$$x^3 - 3 = x^3,$$

which yields

$$\langle 3 \rangle = \left\langle 3, \sqrt[3]{3} \right\rangle^3.$$

Although we have explicit factorizations, but it may not obvious whether or not they're principal. It's easy to see that $\left\langle 3, 3^{1/3} \right\rangle$ is principal since $3^{1/3} \mid 3$ and the first generator is redundant For $\langle 2 \rangle$, it's less clear, but

$$(3^{1/3} - 1)(3^{2/3} + 3^{1/3} + 1) = 2,$$

and so the 2s are redundant generators in both terms. So every ideal above 2 and 3 is principal, so I is principal. Every ideal class contains such an I, so $\mathrm{Cl}(\mathbb{Z}_K) = 0$ and $\mathbb{Z}_K$ is a PID.

Remark 27.2.2: Asking whether or not this ring is a PID is an undergraduate-level question, but it's not clear how one would determine this without the theory developed in this class.

Example 27.2.3*(?):* Let $K = \mathbb{Q}(\theta)$ where θ is a root of $f(x) = x^5 - x^3 + 1$. This is irreducible over $\mathbb{Q}$ and has one real root. Then $n = 5, r_1 = 1, r_2 = 2$, but we need the discriminant to apply the Minkowski bound. If we could prove $\mathbb{Z}_K = \mathbb{Z}(\theta)$, $\Delta_K = \Delta(f)$. If it were squarefree, it'd correspond to an integral basis, so we compute

$$\Delta(f) = \Delta(1, \theta, \theta^2, \theta^3, \theta^4) = 3017,$$

using determinant formulas in the book. This is squarefree, so the power basis is an integral basis, so $\mathbb{Z}_K = \mathbb{Z}[\theta]$ and $\Delta_K = 3017$. Then

$$M_k = \left(\frac{4}{\pi}\right)^2 \frac{5!}{5^5} \sqrt{3017} \approx 3.41.$$

So every ideal class is represented by an ideal of norm at most 3.

- Norm 1: Unit ideal and thus principal,
- Norm 2: Primes above 2
- Norm 3: Primes above 3

We'll apply Dedekind-Kummer. First mod 2: $f(x)$ is irreducible mod 2, so $\langle 2 \rangle$ is inert and prime. So there are no ideals of norm 2, since it would have to factor as a product of primes above 2, but the only possible factor is 2 which has norm $2^5 = 32$.

Mod 3: f is no longer irreducible, but factors as $f = pq$ with $\deg p = 2, \deg q = 3$. So there are no ideals of norm 3, since all prime ideals above 3 would have to have norms of 3^2 corresponding to p or 3^3 corresponding to q. Thus $\mathrm{Cl}(\mathbb{Z}_K) = 0$, since every I is represented by an ideal of norm 1 and hence is principal.

Remark 27.2.4: Next up we'll talk about a lower bound for $|\Delta_K|$ Obviously $M_K \geq 1$, since the theorem states that every ideal class has a representative of norm at most M_K, and $M_K < 1$ wouldn't make sense. Using the formula, rearranging yields a bound

$$|\Delta_K| \geq \left(\frac{n^n}{n!}\right)^2 \left(\frac{\pi}{4}\right)^{2r_2}.$$

28 Ch. 21: Consequences of Minkowski's Bound (Saturday, May 22)

Remark 28.0.1: We were discussing a lower bound on $|\Delta_K|$. We have Minkowski's class number bound: every ideal class has a representative of norm at most M_K, where

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

A consequence of the theorem is $M_K \geq 1$, and rearranging yields a bound

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

What is this bound really telling us? Let's bound the right-hand side from below. Note that $\pi/4 < 1$, and since this is raised to a power, this might make things smaller. The worst case, i.e. the smallest it could be, is when $2r_2$ is as large as possible, so using that $r_1 + r_2 = n$ we have

$$|\Delta_K| \geq \left(\frac{n^n}{n!}\right)^2 (\pi/4)^n \coloneqq B_n.$$

How does B_n grow? We could use Stirling's formula, but we'll take a crude bound by looking at ratios:

$$\begin{aligned}
\frac{B_{n+1}}{B_n} &= (1 + \frac{1}{n})^{2n}(\pi/4) \\
&= \left(1 + \binom{2n}{1}\frac{1}{n} + \cdots\right)(\pi/4) \\
&\geq 3\pi/4.
\end{aligned}$$

Noting that $B_2 = \pi^2/4$, so by induction

$$B_n \geq (3\pi/4)^{n-2}(\pi^2/4).$$

Remark 28.0.2: Some consequences:

a. $|\Delta_K| > 1$ for all number fields $K \neq \mathbb{Q}$.
b. $|\Delta_K| \to \infty$ as $[K : \mathbb{Q}] \to \infty$.

The following says why (a) is important:

Theorem 28.0.3 ***(Dedekind).***
p ramifies in $\mathbb{Z}_K \iff p \mid \Delta_K$.

Proof (?).
Omitted, see book.
■

Remark 28.0.4: So by (a), every number field $K \geq \mathbb{Q}$ there is at least one ramified prime p.

Remark 28.0.5: Note that if $|\Delta_K| = 1$, then $K = \mathbb{Q}$, i.e. there is only one such number field. What about for any fixed number n? The next theorem says that there are only finitely many number fields occurring below a prescribed bound:

Theorem 28.0.6 ***(Hermite's theorem).***
For every $X > 0$, there are finitely many number fields K with $|\Delta_K| \leq X$.

Remark 28.0.7: Since $|\Delta_K| \to \infty$ as $[K : \mathbb{Q}] \to \infty$, it suffices to prove this theorem with a fixed $n \coloneqq [K : \mathbb{Q}]$. We'll make a simplifying assumption that $r_1 = n$ – this doesn't simplify the proof so much, but rather simplifies the notation. The full proof in the book is not so different.

Remark 28.0.8: Define a region

$$R \coloneqq \left\{ [x_1, x_2, \cdots, x_n] \in \mathbb{R}^n \;\middle|\; |x_{i \leq n-1}| \leq \frac{1}{2},\ |x_n| \leq T \right\} \subseteq \mathbb{R}^n,$$

where we'll specify T in a moment.

Note that

- R is centrally symmetric
- R is convex, by the triangle inequality,
- The volume is easily computable: $\operatorname{vol} R = 1 \cdot 1 \cdot \ldots \cdot 1 \cdot 2T = 2T$.

Choose $T = 2^n \sqrt{X}$. Suppose K is totally real with $|\Delta_K| \leq X$. Recall that

$$\operatorname{covol} \iota\mathbb{Z}_K = 2^{r_2} \sqrt{|\Delta_K|} \leq \sqrt{X}.$$

Then

$$\operatorname{vol} R = 2^{n+1} \sqrt{X} > 2^n \operatorname{covol} \iota\mathbb{Z}_K,$$

so Minkowski's theorem can be applied: there is a nonzero $\alpha \in \mathbb{Z}_K$ with $\iota(\alpha) \in R$. Then $|\sigma_i(\alpha)| \leq 1/2$ for $i \leq n-1$ and $|\sigma_n(\alpha)| \leq T$. The claim is that there are only finitely many such α, since it was a root of a polynomial in a finite set $P_{n,T}$. The claim is now that $K = \mathbb{Q}(\alpha)$, so this α uniquely determines K. Since there were finitely many α, there can only be finitely many such K.

The claim is that the size of $\sigma_n(\alpha)$ has to be big, say at least 1. We have control over the product, since

$$1 \leq |N\alpha| = \prod |\sigma_i(\alpha)| \leq \frac{1}{2^{n-1}}|\sigma_n(\alpha)|,$$

since the first $n-1$ terms contribute at most $1/2$ each. So $|\sigma_n(\alpha)| \geq 2^{n-1} \geq 1$. Suppose now that $\mathbb{Q}(\alpha) < K$ is a proper subfield, so $[K : \mathbb{Q}(\alpha)] = d > 1$. Then every embedding $\mathbb{Q}(\alpha) \hookrightarrow \mathbb{C}$ extends to d embeddings $K \hookrightarrow \mathbb{C}$, but this means that for any element $x \in \mathbb{Q}(\alpha)$, the images $\sigma_1(x), \cdots, \sigma_n(x)$ would have the same element repeated d times. But we know that $\sigma_n(\alpha)$ is different from all of the other $\sigma_i(\alpha)$, so this is a contradiction.

Remark 28.0.9: Idea of proof: making sure some image of α under one embedding is different than all of the other images.

Remark 28.0.10: Some remarks on modern research! Let $N_n(X)$ be the set of number fields of degree n where $|\Delta_K| \leq X$.

Conjecture 28.0.11.
For each fixed n,

$$\lim_{X\to\infty} \frac{N_n(X)}{X} = \delta_n > 0,$$

where δ_n is some particular constant.
Some known results:

- $n = 2$: known to Gauss, since this is more or less equivalent to counting squarefree numbers.
- $n = 3$: much harder, Davenport-Heilbronn.
- $n = 4, 5$: Bhargava, part of what resulted in his 2014 Fields medal.

Remark 28.0.12: One could restrict this problem, e.g. by prescribing a particular Galois group. See Mahler's conjecture.

29 Chapter XYZ: Relative Extensions, Galois Theory, Prime Splitting

Remark 29.0.1: Up until now: we've compared extensions over $\mathbb{Q}$:

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

Link to Diagram

We'll next talk about extensions between number fields:

$$\begin{array}{ccc} L & & \mathbb{Z}_L \\ | & & | \\ K & & \mathbb{Z}_K \end{array}$$

Link to Diagram

We can ask the same sorts of questions about prime ideals factoring. Note that if $I = \prod P_i^{e_i}$ with each $P_i \in \operatorname{Spec} \mathbb{Z}_K$, then extending to $\mathbb{Z}_L$ yields

$$I\mathbb{Z}_L = \prod (P_i \mathbb{Z}_L)^{e_i}.$$

So we want to understand the following: given a prime ideal P of $\mathbb{Z}_K$, how does $P\mathbb{Z}_L$ factor?

Definition 29.0.2 (lies above)
Let $K \leq L$ be number fields, and suppose $Q \in \operatorname{Spec} \mathbb{Z}_L, P \in \operatorname{Spec} \mathbb{Z}_K$. Then we say Q **lies above** P if $Q \supseteq P$, or equivalently $Q \mid P\mathbb{Z}_L$.

Proposition 29.0.3 *(?).*
Every nonzero $Q \in \operatorname{Spec} \mathbb{Z}_L$ lies above a unique nonzero $P \in \operatorname{Spec} \mathbb{Z}_K$.

Proof (?).
Consider $P \coloneqq Q \cap \mathbb{Z}_K \in \operatorname{Spec} \mathbb{Z}_K$. This is nonzero because taking the norm of any element of Q yields a nonzero integer still in the ideal. Then Q lies above P by definition. Why is this unique? Suppose Q lies about P', we'll show $P = P'$. Since Q lies above P', $Q \supseteq P'$. But $P' \trianglelefteq \mathbb{Z}_K$, so $Q \cap \mathbb{Z}_K \supseteq P'$, so $P \supseteq P'$. We know P' is maximal, since $\mathbb{Z}_K / P'$ is a finite domain and thus a field, so $P = P'$.

■

Definition 29.0.4 (Ramification and residue degrees)
Let $P \in \operatorname{Spec} \mathbb{Z}_K$, then write

$$P\mathbb{Z}_L = \prod Q_i^{e_i}$$

with $Q_i \in \operatorname{Spec} \mathbb{Z}_L$. Then the Q_i are the prime ideals of $\mathbb{Z}_L$ above P. The exponent e_i is called the **ramification degree**, usually denoted $e(Q_i/P)$. We have the following picture:

$$\begin{array}{ccccc} L & & \mathbb{Z}_L & & Q \\ | & & | & & | \\ K & & \mathbb{Z}_K & & P \end{array}$$

Link to Diagram

The inclusion $\mathbb{Z}_K \hookrightarrow \mathbb{Z}_L$ induces a ring morphism $\mathbb{Z}_K \to \mathbb{Z}_L/Q$, where the kernel is $\mathbb{Z}_K \cap Q = P$. Thus there is an injection $\mathbb{Z}_K/P \hookrightarrow \mathbb{Z}_L/Q$, which is an inclusion of finite fields. So we'll define

$$f(Q/P) \coloneqq [\mathbb{Z}_L/Q : \mathbb{Z}_K/P]$$

to be the **residue degree** of Q/P. Note that

$$\#\mathbb{Z}_L/\mathbb{Q} = (\#\mathbb{Z}_K/P)^{f(Q/P)} \quad \text{i.e.} \quad N_L(Q) = N_K(P)^{f(Q/P)}.$$

Theorem 29.0.5 ***(efg theorem).***
If $P \in \operatorname{Spec} \mathbb{Z}_K$ is nonzero with $P\mathbb{Z}_L = \prod Q_i^{e_i}$, then

$$\sum_i e(Q_i/P) f(Q_i/P) = [L : K].$$

Lemma 29.0.6 ***(?).***
If $I \in \operatorname{Spec} \mathbb{Z}_K$ is nonzero, then extend to L to get $I\mathbb{Z}_L$. Then

$$N_L(I\mathbb{Z}_L) = (N_K(I))^{[L:K]}.$$

Proof (?).
Omitted. Idea of why it's true: the norm of an ideal is supposed to be a "product of conjugates", although naive conjugates of an ideal might not remain an ideal in the field one starts with. So interpret norms as products of images under all embeddings into $\mathbb{C}$. But then just interpret $[L : K]$ is the number of lifts of embeddings $K \hookrightarrow \mathbb{C}$ to $L \hookrightarrow \mathbb{C}$.

■

Proof (of efg theorem).
Take norms in L, then

$$\begin{aligned} N(P\mathbb{Z}_L) &= \prod N(Q_i)^{e_i} \\ &= N_K(P)^{e_1 \sum f(Q_i/P)}. \end{aligned}$$

On the other hand, the left-hand side is $N_K(P)^{[L:K]}$, so the exponents must be equal.

■

Remark 29.0.7: What are the specific prime ideals involved in the factorization, i.e. is there a generalization of Dedekind-Kummer here?

Proposition 29.0.8 ***(Generalized Dedekind-Kummer theorem).***
Write $L = K(\theta)$ for some $\theta \in L \cap \overline{\mathbb{Z}} = \mathbb{Z}_L$. Let $m(x)$ be the minimal polynomial of θ over K, so $m \in \mathbb{Z}_K[x]$. Let $P \in \operatorname{Spec} \mathbb{Z}_K$ lying above $p \in \operatorname{Spec} \mathbb{Z}$. Then as long as $p \nmid [\mathbb{Z}_L : \mathbb{Z}_K[\theta]]$, then the factorization of $P\mathbb{Z}_L$ mirrors the factorization of m over the residue field $\mathbb{Z}_K/P$.

Proof (?).
Omitted, see "Number Rings" by Marcus. Paul strongly recommends!
■

30 | Ch. XYZ: April 6

30.1 Multiplicativity in Towers

Remark 30.1.1: An important topic not in the book: relative extensions of number fields, vs absolute extensions over $\mathbb{Q}$.

$$\begin{array}{ccc} L & \mathbb{Z}_? & Q \\ | & | & | \\ K & \mathbb{Z}_K & P = Q \cap \mathbb{Z}_K \end{array}$$

Link to Diagram

Note that if $Q \supseteq P$, then Q will divide the extension of P to $\mathbb{Z}_L$, if Q will show up in the prime factorization of $P\mathbb{Z}_L$. We defined $e(Q/P)$ to be the exponent of Q in the factorization of $P\mathbb{Z}_L$, and $f(Q/P)$ to be the degree of the field extension $\mathbb{Z}_L/Q$ over $\mathbb{Z}_K/P$.

Remark 30.1.2: Note that "lying above" is transitive, and the following situation makes sense:

$$\begin{array}{cc} M & P'' \\ | & | \\ L & P' \\ | & | \\ K & P \end{array}$$

Link to Diagram

How are the various e and f related? It turns out they work similarly to degrees of field extensions:

Theorem 30.1.3 ***(Multiplicativity in towers).***

$$e(P''/P) = e(P''/P') \cdot e(P'/P)$$
$$f(P''/P) = f(P''/P') \cdot f(P'/P).$$

Proof (?).
Note that f is the degree of a field extension where we take $\mathbb{Z}_K/P \hookrightarrow \mathbb{Z}_L$ and consider the induced quotient map to $\mathbb{Z}_L/Q$. By composing inclusions we have a commutative diagram:

$$\mathbb{Z}_K/P \hookrightarrow \mathbb{Z}_L/P' \hookrightarrow \mathbb{Z}_M/P''$$

Link to Diagram

So for f, this reduces to the multiplicativity of degrees in towers of field extensions.
For e, write $P\mathbb{Z}_L = P'^{e(P'/P)}I$ where $I \in \mathrm{Id}(\mathbb{Z}_L)$ is nonzero and $P' \nmid I$. Similarly we can write $P'\mathbb{Z}_< = P''^{e(P'/P')}J$ where $J \in \mathrm{Id}(\mathbb{Z}_L)$ and $P'' \nmid J$. Using general facts about ideal extensions and substituting yields

$$\begin{aligned} P\mathbb{Z}_M &= (P\mathbb{Z}_L)\mathbb{Z}_M \\ &= (P'\mathbb{Z}_M)^{e(P'/P)} I\mathbb{Z}_M \\ &= P''^{e(P'/P)e(P'/P')} J^{e(P'/P)}(I\mathbb{Z}_M) \end{aligned}$$

.

We know that $P'' \nmid J$, so it doesn't divide any power of J either. We can check that $P'' \nmid I\mathbb{Z}_M$: otherwise, if it did then $P'' \supseteq I\mathbb{Z}_M$ and

$$P'' \cap \mathbb{Z}_L \supseteq (I\mathbb{Z}_M) \cap \mathbb{Z}_L \supset I$$

by intersecting both sides with $\mathbb{Z}_L$. But we know $P'' \cap \mathbb{Z}_L = P'$ since P'' was above P', and $P' \nmid I$ and thus $P' \not\supseteq I$.

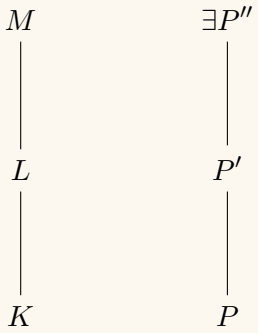
■

Definition 30.1.4 (Splitting completely)
Suppose L/K is an extension of number fields and say $P \supseteq \mathbb{Z}_K$ is a nonzero prime ideal. Then P **splits completely** in L (or $\mathbb{Z}_L$) if $e(G/P) = f(G/P) = 1$ for all G above P in $\mathbb{Z}_L$. Equivalently, there is a factorization $P\mathbb{Z}_L = \prod_{i \le n} Q_i$ with the Q_i distinct and $n \coloneqq [L : K]$.

Proposition 30.1.5 ***(?).***
Let $M/L/K$ be a tower of number fields and $P \in \operatorname{Spec} \mathbb{Z}_K$. Then if P splits completely in M, it splits completely in L.

Slogan 30.1.6
Splitting completely in an extension implies splitting completely in every intermediate extension.

Proof (?).
Suppose P splits completely in M, we then want to show that for any P' in $\mathbb{Z}_L$ above P, then $e = f = 1$. We know P' has some prime factor, so choose any P'' in $\mathbb{Z}_M$ above P':



Link to Diagram

Since P'' is above P and $e(P''/P) = f(P''/P) = 1$, we can use multiplicativity in towers:

$$e(P'/P) \mid e(P''/P) = 1 \implies e(P'/P) = 1$$
$$f(P'/P) \mid f(P''/P) = 1 \implies f(P'/P) = 1$$

.

■

Definition 30.1.7 (?)
If L/K is an extension of number fields and $P \in \operatorname{Spec} \mathbb{Z}_K$ is nonzero, then P **ramifies** in L (or $\mathbb{Z}_L$) if $e(Q/P) > 1$ for some $Q \in \operatorname{Spec} \mathbb{Z}_L$ above P.

Proposition 30.1.8 ***(?).***
For $M/L/K$ a tower of number fields and $P \in \operatorname{Spec} \mathbb{Z}_K$ is nonzero and unramified in M, then P is unramified in L.

Proof (?).
Same as the last proof.

■

30.2 Galois Theory and Prime Decomposition

Remark 30.2.1: This will lead into defining the Frobenius element and the fundamental theorem of algebraic number theory: Chebotarev Density. Some setup/notation:

- L/K will be a Galois extension of number of fields
- $P \in \operatorname{Spec} \mathbb{Z}_K, Q \in \operatorname{Spec} \mathbb{Z}_L$ will be nonzero prime ideals. We may or may not require Q to lie above P.

Remark 30.2.2:

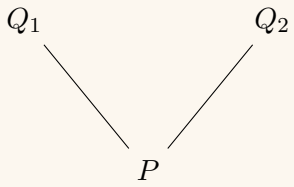
- Any $\sigma \in G(L/K)$ is an automorphism of L fixing K, which restricts to an automorphism of $\mathbb{Z}_L$ since it preserves algebraic integers.
  - It also preserves prime ideals.
- Suppose Q lies above P, then $P\mathbb{Z}_L = Q^{e(Q/p)} \cdots$. σ fixes K pointwise, so applying it to both sides yields $P\mathbb{Z}_L = \sigma(Q)^{e(Q/P)} \cdots$ where $\sigma(Q)$ shows up with the exact same power since it preserves distinctness of ideals.
  - In particular, $\sigma(G)$ lies above P, so $G(L/K)$ acts on the set of primes above P, and it turns out (very importantly) to be transitive.

Theorem 30.2.3 *(?).*
The action of $G(L/K)$ on primes above P is transitive.

Proof (?).
Let Q_1, Q_2 be primes above P and suppose toward a contradiction that $\mathrm{Orb}(Q_1)$ does not contain Q_2. We may choose $\alpha \in \mathbb{Z}_L$ such that

- $\alpha \equiv 0 \bmod Q_2$
- $\alpha \equiv 1 \bmod Q$ for all Q of the form $Q = \sigma(Q_1)$, noting that none are Q_2

This system can be solved by the CRT, since the Q_i are pairwise comaximal, since nonzero primes of a number ring are maximal. These congruences say $\alpha \in Q_2$ but not any other Q, since $0 \equiv 1$ only in the unit ideal. Define $\beta = \prod_{\sigma \in G(L/K)} \sigma(\alpha) \in \mathbb{Z}_K$, and observe that $\beta \notin Q_1$. If it were in Q_1, one $\sigma(\alpha) \in Q_1$ for some $\sigma \in G(L/K)$ which would force $\alpha = \sigma\sigma^{-1}(\alpha) \in \sigma^{-1}(Q_1)$, which contradicts the choice of α since $\sigma^{-1}(Q_1)$ is one of the Qs appearing in the second congruence. On the other hand we have $\beta \in Q_2$ since the identity is an element of $G(L/K)$ and $\alpha \in Q_2$ and β is a multiple of α. We know $\beta \in \mathbb{Z}_K$, so $\beta \in Q_2 \cap \mathbb{Z}_K = P$. But this is fishy because Q_1, Q_2 both lie above P and both must contain P:



Link to Diagram

Since β is in every ideal above P, in particular $\beta \in Q_1$ since $Q_1 \supseteq P$, and this is a contradiction. ■

Proposition 30.2.4 *(?).*
If Q, Q' both lie above P, then $e(Q/P) = e(Q'/P)$ and $f(Q/P) = f(Q'/P)$.

Proof (?).
Pick $\sigma \in G(L/K)$ with $\sigma(Q) = Q'$. Factor $P\mathbb{Z}_L = Q^{e(Q/P)}J$ where J is a product of primes

not equal to Q. Applying σ yields $P\mathbb{Z}_L = Q'^{e(Q/P)}J'$ where J' is a product of primes not equal to Q'. This factors $P\mathbb{Z}_L$ into primes, and by uniqueness of prime factorization this exponent has to be $e(Q'/P)$ by definition.
For the fs, note that σ induces a ring morphism between the residue fields:

$$\begin{aligned}\bar{\sigma} : \mathbb{Z}_K/Q &\to \mathbb{Z}_L/Q' \\ \alpha \bmod Q &\mapsto \sigma(\alpha) \bmod Q'.\end{aligned}$$

This is well-defined since $\sigma(Q) = Q'$, and is an isomorphism since the inverse comes from σ^{-1}. This will imply that the fs are the same: we're looking at the degree of these extensions over $\mathbb{Z}_K/P$. An element of $\mathbb{Z}_L/Q$ also belonging to $\mathbb{Z}_K/P$ (as a subfield) has the form $\alpha \bmod Q$ where $\alpha \in \mathbb{Z}_K$, and under σ this is sent to $\sigma(\alpha) \bmod Q' = \alpha \bmod Q'$, which is an element of the copy of $\mathbb{Z}_K/P \hookrightarrow \mathbb{Z}_L/Q'$. So σ identifies the copies of $\mathbb{Z}_K/P$ in either side, and

$$[\mathbb{Z}_L/Q : \mathbb{Z}_K/P] = [\mathbb{Z}_L/Q : \mathbb{Z}_K/P].$$

■

Theorem 30.2.5 ***(efg theorem for Galois extensions).***
Let L/K be a Galois extension of number fields and $P \in \operatorname{Spec} \mathbb{Z}_K$ be nonzero. Let e, f be the common e, f for all Q above P, and let g be the number of distinct Q above P. Then

$$efg = n \coloneqq [L : K].$$

Proof (?).
Using the previous efg theorem, $\sum_{i=1}^{g} e_i f_i = n$, but by the previous proposition, all of the e_i are the same and all of the f_i are the same.

■

Example 30.2.6 ***(?):*** Let $L = \mathbb{Q}(\zeta_5)$ over $K = \mathbb{Q}$, which is Galois with $G(L/K) \cong (\mathbb{Z}/5)^\times \cong \mathbb{Z}_4$. We know $\mathbb{Z}_L = \mathbb{Z}[\zeta_5]$, which actually happens for any n, and $\min_{\zeta_5}(x) = x^4 + x^3 + x^2 + x + 1$. Since $\mathbb{Z}_L$ is a monogenic, we can apply Dedekind-Kummer.

- Factoring $2\mathbb{Z}_L = P$ yields a single factor, so $g = 1$. Since e is the common exponent, $e = 1$, so $f = 4$. If you factor $\min_{\zeta_5} \bmod 2$, in order to get a single prime D-K says this must be irreducible and f_i are the degrees of the irreducible factors.
- $19\mathbb{Z}_L = P_1P_2$, so $g = 2, e = 1$, and so $f = 2$.
- $11\mathbb{Z}_L = P_1P_2P_3P_4$ yields $g = 4, e = 1, f = 1$.
- $5\mathbb{Z}_L = P_1^4$ so $g = 1, e = 4, f = 1$.

Can the combination $(e, f, g) = (2, 2, 1)$ occur? This would require a prime factoring as P^2, but the answer is know. In fact $e > 1$ only happens for 5 since this corresponds (for all applicable primes p,

which is all primes since $\mathbb{Z}_L$ is monogenic here) to the polynomial having a repeated factor mod p. This would require $\Delta(\min_{\zeta_5}(x)) \equiv 0 \bmod p$, but you can show that 5 is the only prime that divides this discriminant. So 5 is the only prime that could ramify, so $e = 2$ never happens.

In general, for cyclotomic extensions, p is always totally ramified and $e = p - 1$.

30.3 Decomposition, Inertia, Frobenius

Definition 30.3.1 (Decomposition)
Let L/K be a Galois extension of number fields and let $Q \in \operatorname{Spec} \mathbb{Z}_L$ be nonzero. Then Q lies above a unique prime $P \in \operatorname{Spec} \mathbb{Z}_K$, where $P = Q \cap \mathbb{Z}_K$. Define the **decomposition group of** Q is defined as

$$D(Q) = D(Q/P) = \left\{ \sigma \in G(L/K) \;\middle|\; \sigma(Q) = Q \right\}.$$

Definition 30.3.2 (?)
Better notation: define $\mathbb{F}_Q \coloneqq \mathbb{Z}_L/Q$ and $\mathbb{F}_P = \mathbb{Z}_K/P$, so $\mathbb{F}_P \subseteq \mathbb{F}_Q$.

Remark 30.3.3: We know that the Galois group will take Q to some prime above P, these are the ones that take Q to itself. These are the automorphisms that make sense "modulo Q": there is a group morphism

$$\begin{aligned} \operatorname{red}_{Q/P} : D(G/P) &\to G(\mathbb{F}_Q/\mathbb{F}_P) \\ \sigma &\mapsto \bar{\sigma}. \end{aligned}$$

where we reduce σ mod Q, so $\bar{\sigma}(\alpha \bmod Q) \coloneqq \sigma(\alpha) \bmod Q$. One can check

- For $\sigma \in D(Q/P)$, $\bar{\sigma}$ is a well-defined automorphism of $\mathbb{F}_Q$ fixing $\mathbb{F}_P$, since the elements in $\mathbb{F}_P$ are of the form $\alpha \bmod Q$ where $\alpha \in \mathbb{Z}_K$ and σ fixes K. This crucially uses that σ fixes Q, otherwise it won't be well-defined.
- $\operatorname{red}_{Q/P}$ defines a group morphism.

We'll see later that this is in fact a surjective morphism. So all automorphisms in the Galois group $G(\mathbb{F}_Q/\mathbb{F}_P)$ are reductions mod Q of automorphisms in the decomposition group, which are the only ones that make sense to reduce mod Q anyway!

31 Ch. XYZ: Galois Theory and Prime Decomposition (April 13)

Remark 31.0.1: Two recommended resources:

- Samuel, Algebraic Theory of Numbers (Dover)
- Matt Baker's online notes on Algebraic number theory.

Remark 31.0.2: Setup:

- L/K a Galois extension of number fields.
- $P \in \operatorname{mSpec} K$
- $Q \in \operatorname{mSpec} L$

We saw that $G(L/K)$ acts on the prime ideals above P, making all of the e, f values the same, and thus the decomposition into prime ideals in this type of extension is simpler than in a general extension. We'll look at decomposition and inertia groups today.

Recall that if Q lies above P, then the **decomposition group** $D(Q/P)$ is the set of $\sigma \in G(L/K)$ such that $\sigma(Q) = Q$. Note that P is redundant in this notation, since $Q \cap \mathbb{Z}_K = P$. Also recall that $\mathbb{F}_Q \coloneqq \mathbb{Z}_L/Q$ is the residue field associated to Q and $\mathbb{Z}_P \coloneqq \mathbb{Z}_L/P$ and we view $\mathbb{F}_P \subseteq \mathbb{F}_Q$. Such an extension of finite fields is always Galois, and the Galois groups turn out to be related to the decomposition groups. For $\sigma \in D(Q/P)$ we defined $\bar{\sigma} : \mathbb{F}_Q \to \mathbb{F}_Q$ where $\alpha \bmod Q \mapsto \sigma(\alpha) \bmod Q$. It's easy to check this is

- Well-defined, precisely by the definition of $D(Q/P)$,
- An automorphism of $\mathbb{F}_Q$: it must be surjective since everything in $\mathbb{Z}_L$ is in the image of σ since σ was an automorphism of $\mathbb{Z}_L$ to begin with. But then it's a surjective morphism from a finite field to itself, hence an automorphism.
- σ fixed $\mathbb{F}_P$ pointwise Now consider applying σ to an element of $\mathbb{F}_P$, which are of the form $\alpha \bmod Q$ where α comes from $\mathbb{Z}_K$. But σ fixed $\mathbb{Z}_K$ pointwise, so σ fixed $\mathbb{F}_P$ pointwise.

So each $\sigma \in D(Q/P)$ yields a $\bar{\sigma} \in G(\mathbb{F}_Q/\mathbb{F}_P)$ and we get a group morphism

$$\begin{aligned} \operatorname{red}_{Q/P} : D(Q/P) &\to G(\mathbb{F}_Q/\mathbb{F}_P) \\ \sigma &\mapsto \bar{\sigma}. \end{aligned}$$

The following is the deeper and more important fact about this morphism, which requires a technical proof:

Theorem 31.0.3 *(?).*
$\operatorname{red}_{Q/P}$ is surjective.

Proof (?).
We can assume $\mathbb{F}_P$ is a proper subfield of $\mathbb{F}_Q$, since the result follows immediately otherwise. By the primitive element theorem, since $|FF_Q/\mathbb{F}_P$ is separable we can write $\mathbb{F}_Q = \mathbb{F}_P(\bar{\alpha})$ where $\alpha \in \mathbb{Z}_L$ and $\bar{-}$ denotes reducing mod Q. Note $\alpha \notin Q$, since this would mean $\bar{\alpha} = 0$ and thus $\mathbb{F}_Q = \mathbb{F}_P$. On the other hand, we can assume $\alpha \in Q'$ for all other $Q' \neq Q$ above P. Why? Sketch: the equation $\mathbb{F}_Q = \mathbb{F}_P(\bar{\alpha})$ only depends on $\alpha \bmod Q$, so if α is not in some Q', just

adjust α modulo Q' without affecting its class mod Q to get a new α in Q'. So if not, replace α with α' satisfying

$$\begin{aligned} &\alpha' \cong \alpha \bmod Q \\ &\alpha' \cong 0 \bmod Q' \qquad\qquad \forall Q' \neq Q \text{ above } P. \end{aligned}$$

Look at the minimal polynomial $\overline{m}(x)$ of $\bar{\alpha}$ over $\mathbb{F}_P$, some monic polynomial in $\mathbb{F}_P[x]$, where $\mathbb{F}_P$ is the reduction mod P of elements in $\mathbb{Z}_K$. So we can think of $\overline{m}(x)$ as some $m(x) \in \mathbb{Z}_K[x]$ whose coefficients have been reduced mod Q. We'll show that for each root r of $\overline{m}(x)$ in $\mathbb{F}_Q$, there is some $\sigma \in D(Q/P)$ such that $\bar{\sigma}(\bar{\alpha}) = r$ This is enough, since any automorphism of $\mathbb{F}_Q$ fixing $\mathbb{F}_P$ is determined by the image of $\bar{\alpha}$, which has to go to some other root of $\overline{m}(x)$. If we can show this statement, this means that $\bar{\sigma}$ has to hit every automorphism in $G(\mathbb{F}_Q/\mathbb{F}_P)$.
Define $g(x) = \prod_{\sigma \in G(L/K)} (x - \sigma(\alpha))$. Where does g live? α came from L, so $\sigma(\alpha) \in L$, and multiplying over all σ puts the coefficients in K. Even better, since $\alpha \in \mathbb{Z}_L$ is algebraic, this will have $\mathbb{Z}_K$ coefficients, so $g \in \mathbb{Z}_K[x]$. Now reduce mod Q to get $\bar{g}(x) \in \mathbb{F}_P[X]$, and moreover $\bar{g}(\bar{\alpha}) = \overline{g(\alpha)} = 0$ in $\mathbb{F}_Q$, since $g(\alpha) = 0$ by definition since one σ in the product is the identity. Thus we know $\overline{m}(x) \mid \bar{g}(x)$ in $\mathbb{F}_P[x]$. Notice that in $\mathbb{F}_Q[x]$, if we take g and reduce mod Q we get

$$\bar{g}(x) = \prod_{\sigma \in G(L/K)} (x - \overline{\sigma(\alpha)}).$$

Since $\overline{m}(x)$ divides $\bar{g}(x)$, every root of $\overline{m}$ has the form $\overline{\sigma(\alpha)}$ for some $\sigma \in G(L/K)$. We want this to be $\bar{\sigma}(\bar{\alpha})$ instead to conclude the proof, so take a root of $\overline{m}$ in $\mathbb{F}_Q$ and write it as $\overline{\sigma(\alpha)}$ with $\sigma \in G(L/K)$

Claim: $\sigma \in D(G/P)$ has to be in the decomposition group.
If this is true, we're done since $\overline{\sigma(\alpha)} = \bar{\sigma}(\bar{\alpha})$.
Suppose toward a contradiction that $\sigma \notin D(G/P)$, so neither σ nor σ^{-1} fixes Q, so $\sigma^{-1}(Q) \neq Q$. By choice of α, we have $\alpha \in Q' \coloneqq \sigma^{-1}(Q)$, so $\sigma(\alpha) \in Q$. Then $\overline{\sigma(\alpha)} = 0$, but 0 is not a root of $\overline{m}(x)$ since it is irreducible where $\overline{m}(x) \neq x$ since $[\mathbb{F}_Q : \mathbb{F}_P] \geq 2$ and thus $\deg \overline{m}(x) \geq 2$.
■

Remark 31.0.4: By the first isomorphism theorem, we have

$$G(\mathbb{F}_Q/\mathbb{F}_P) \cong D(Q/P)/\ker \mathrm{red}_{Q/P}.$$

, where we call the kernel the **inertia group**:

$$\ker \mathrm{red}_{Q/P} = I(Q/P) \coloneqq \left\{ \sigma \in D(Q/P) \;\middle|\; \bar{\sigma} = \mathrm{id}_{\mathbb{F}_Q} \right\}.$$

These are the elements σ in the decomposition group such that $\sigma(\alpha) \equiv \alpha \bmod Q$ for every α.

Since we have a group action of the Galois group on primes above P, we can apply Orbit-Stabilizer: we have $\mathrm{Stab}(Q) = D(Q/P)$ and the orbit is all primes above P, so

$$G(L/K)/D(Q/P) \cong \{\text{Primes above } P\}.$$

Taking cardinalities,

$$[L:K]/\#D(Q/P) = g \implies \#D(Q/P) = \frac{[L:K]}{g} = \frac{efg}{g} = ef.$$

We also have

$$\frac{ef}{\#I(Q/P)} = \#G(\mathbb{F}_Q/\mathbb{F}_P) = [\mathbb{F}_Q : \mathbb{F}_P] = f.$$

In summary,

- $\#D(Q/P) = f$,
- $\#I(Q/P) = e$,
- If P is unramified, $e = 1$ and $I(Q/P)$ is trivial and $\text{red}_{Q/P}$ is an isomorphism.

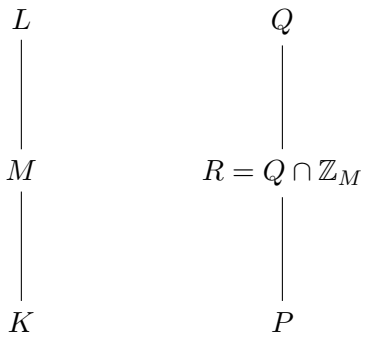
This map is usually an isomorphism, since there are only finitely many P ion $\mathbb{Z}_K$ that ramify in $\mathbb{Z}_L$.

31.1 Inertia and Decomposition Fields

Remark 31.1.1: It will turn out that the fixed fields appearing here have number-theoretic interpretations.

Definition 31.1.2 (?)
If Q lies above P, then define the **inertia field** corresponding to Q/P, written $L^{I(Q/P)}$, and the **decomposition field** $L^{D(Q/P)}$.

Remark 31.1.3: Suppose L/K is Galois, and consider an intermediate field $L/M/K$. We can find intermediate primes:



Link to Diagram

We can consider e, f of R/P in this picture. Going to bigger extensions then M makes R bigger, so e increases as M gets bigger.

Theorem 31.1.4 *(?).*
The inertia field $L^{I(Q/P)}$ is the largest field extension M for which $e(R/P) = 1$. More precisely,

$$e(R/P) = 1 \iff M \subseteq L^{I(Q/P)}.$$

Remark 31.1.5: From Galois theory, L/M is also Galois, so the key to proving this theorem involves understanding D, I of Q/R. Noting that $G(L/M) \subseteq G(L/K)$, We have

$$\begin{aligned} D(Q/R) &\coloneqq \left\{\sigma \in G(L/M) \;\middle|\; \sigma(Q) = Q\right\} \\ &= \left\{\sigma \in G(L/K) \;\middle|\; \sigma(Q) = Q\right\} \cap G(L/M) \\ &= D(Q/P) \cap G(L/M), \end{aligned}$$

so the decomposition groups are related by restriction. Suppose $\sigma \in D(Q/R)$, then $\mathrm{red}_{Q/R}(\alpha)$ is an automorphism of $\mathbb{F}_Q$. We can also get an automorphism of $\mathbb{F}_Q$ by taking $\mathrm{red}_{Q/P}(\sigma)$ – it turns out these are the same automorphism. Why? Both map $\alpha \bmod Q$ to $\sigma(\alpha) \bmod Q$, which doesn't involve R or P. We can thus write

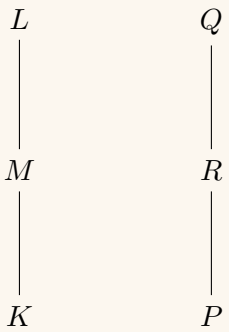
$$\begin{aligned} I(Q/R) &= \left\{\sigma \in D(Q/R) \;\middle|\; \bar{\sigma} = \mathrm{id}_{\mathbb{F}_Q}\right\} \\ &= \left\{\sigma \in D(Q/P) \cap G(L/M) \;\middle|\; \bar{\sigma} = \mathrm{id}_{\mathbb{F}_Q}\right\} \\ &= \left\{\sigma \in D(Q/P) \;\middle|\; \bar{\sigma} = \mathrm{id}_{\mathbb{F}_Q}\right\} \cap G(L/M) \\ &= I(G/P) \cap G(L/M). \end{aligned}$$

Remark 31.1.6 ***(Upshot):***

$$\begin{aligned} D(Q/R) &= D)Q/P) \cap G(L/M) \\ I(Q/R) &= I)Q/P) \cap G(L/M) \end{aligned}$$

.

Proof (of theorem).
Let $L/M/K$ with $Q/R/P$, we want to show $e(R/P) = 1 \iff M \subset L^{I(Q/P)}$:



Link to Diagram

We'll use multiplicativity of e in towers. Recall that $e(R/P) = e(Q/R)e(R/P)$, so $e(R/P) = 1$ iff $e(Q/P) = e(Q/R)$. Interpreting this as the size of inertia, this happens iff $\#I(Q/P) = \#I(Q/R)$, iff $\#I(Q/P) = \#(I(Q/P) \cap G(L/M))$. This happens iff $I(Q/P) \subseteq G(L/M)$, iff $M \subseteq L^{I(Q/P)}$.

■

Theorem 31.1.7 *(?).*
The decomposition field $L^{D(Q/P)}$ is the largest M for which *both* $e(R/P) = f(R/P) = 1$.

Proof (?).
Replace e in the previous proof with the product ef and I replaced by D, using $\#D = ef$.

■

Remark 31.1.8: Next time: why these theorems are interesting! How ramification and splitting completely behaves in fields vs their Galois closures.

32 Decomposition and Inertia Fields (April 15)

32.1 Ramification in Composite Fields

Remark 32.1.1: Recall the setup:

- L/K is a Galois extension of number fields.
- $P \in \operatorname{Spec} K$ nonzero, and in fact we'll usually mean $P \in \operatorname{mSpec} \mathbb{Z}_K$.
- $Q \in \operatorname{Spec} L$.
- $\mathbb{F}_Q \coloneqq \mathbb{Z}_L/Q, \mathbb{F}_P \coloneqq \mathbb{Z}_K/P$

When Q lies above P, we defined $D(Q/P)$ as all $\sigma \in G(L/K)$ preserving Q. We have a reduction map

$$\begin{aligned} \operatorname{red}_{Q/P} : D(Q/P) &\to G(\mathbb{F}_Q/\mathbb{F}_P) \\ \sigma &\mapsto \bar{\sigma}, \end{aligned}$$

which we saw was a surjective group morphism with kernel $I(Q/P) \coloneqq \ker(\operatorname{red}_{Q/P})$. Since D, I are subgroups of $G(\mathbb{F}_Q/\mathbb{F}_P)$, we can consider the corresponding intermediate fixed fields, the *inertia field* and *decomposition field*. Using that the Galois correspondence is inclusion-reversing, we get the following:

Link to Diagram

Remark 32.1.2: Suppose we have a tower $L/M/K$ with prime ideals $Q/R/P$ with $R \coloneqq Q \cap \mathbb{Z}_M$. We showed that with respect to containment,

a. $L^{I(Q/P)}$ is the largest intermediate field in which $e(R/P) = 1$.
b. $L^{D(Q/P)}$ is the largest intermediate field in which $e(R/P) = f(R/P) = 1$.

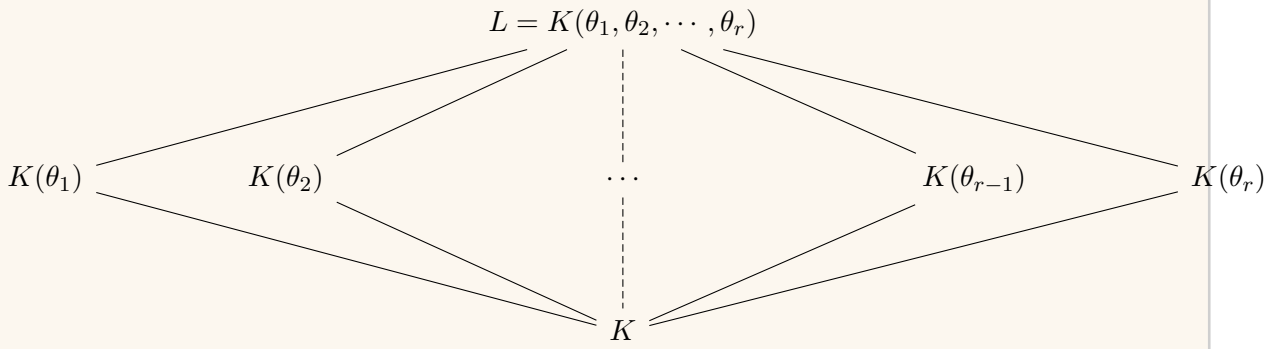
Note that (b) is a stronger condition, so this matches the containment in the previous diagram.

Theorem 32.1.3 *(?).*
Let M/K be an extension of number fields, not necessarily Galois. Let L be the **Galois closure** of M/K, the smallest field extension containing M which is Galois over K. Then

a. $P \in \operatorname{Spec} K$ is unramified in $M \iff P$ is unramified in L.

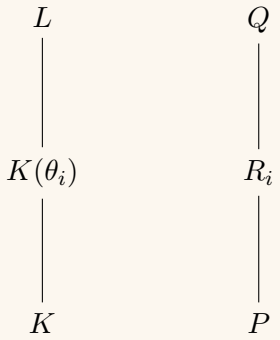
b. $P \in \operatorname{Spec} K$ splits completely in $M \iff P$ splits completely in L.

Proof (?).
We'll just prove (a), and a very similar argument will yield (b).
$\impliedby$: This is clear: if $L/M/K$ is a tower and P is unramified in L, why is it unramified in M? This is multiplicativity of e in towers. If we have R in M with R/P, we can choose Q in L with $Q/R/P$. If $e(R/P) > 1$, we have $e(Q/P) = e(Q/R)e(R/P) > 1$, forcing P to ramify in L. Note that we haven't used that L is the Galois closure.
$\implies$: By the primitive element theorem, write $M = K(\theta)$, how can we describe the Galois closure L? Listing $\theta_1, \theta_2, \cdots, \theta_r$ the roots of $\min_{\theta}(x)$ over K, then $L = K(\theta_1, \theta_2, \cdots, \theta_r)$:



Link to Diagram

By assumption, P is unramified in M, which is one $K(\theta_i)$. There is always an isomorphism between any of the two $K(\theta_i)$ which preserves K, so abstractly they're all equivalent. So P is unramified in $K(\theta_i)$ for all i. Take any $Q \in \operatorname{Spec} L$ over P. We can consider the tower involving $K(\theta_i)$ for any i and produce a corresponding prime R_i:



Link to Diagram

Since P is unramified in all $K(\theta_i)$, we have $e(R_i/P) = 1$. Now use the characterization of the inertia field: $K(\theta_i) \subset L^{I(Q/P)}$, which is true for every i. So their composite is also contained in the inertia field, so we have

$$L = K(\theta_1, \theta_2, \cdots, \theta_r) \subseteq L^{I(Q/P)} \subseteq L,$$

yielding equality. Now note that the inertia field was the largest intermediate field for which $e = 1$, and we've just conclude $L = L^{I(Q/P)}$, so $e(Q/P) = 1$. Since Q/P was arbitrary, P is unramified.

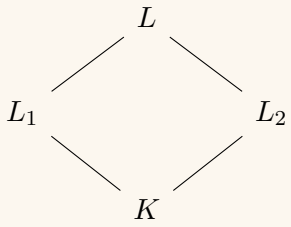
■

Theorem 32.1.4 *(?).*
Let $M_1/K, M_2/K$ be any two extensions of K. Then

a. P is unramified in M_1 and $M_2 \iff P$ is unramified in the composite field M_1M_2.

b. P splits completely in M_1 and $M_2 \iff P$ splits completely in the composite field M_1M_2.

Proof (?).
As before, we'll only prove (a).
$\Longleftarrow$: Again clear by multiplicativity in towers.
$\Longrightarrow$: Note that everything involving inertia only makes sense for Galois extensions, and we haven't assumed that here. So let L be the Galois closure of M_1M_2/K, and let L_1, L_2 be the Galois closures of $M_1/K, M_2/K$ respectively. By the previous theorem, P is unramified in L_1, L_2. How is L related to L_1 and L_2? You can convince yourself that $L = L_1L_2$, since the right-hand side is a Galois extension of K, and it contains M_1M_2. We'll forget the M_i and work with the following diagram:



Link to Diagram

We have a prime in K which is unramified in the L_i, and we want to show it's also unramified in L, which is equivalent to being unramified in M_1M_2 (which was our goal). Strat: let $Q \in \operatorname{Spec} L$ with Q/P and let R_1, R_2 be the corresponding primes in $\operatorname{Spec} L_1, \operatorname{Spec} L_2$ between Q and P. Since P is unramified in the L_i, we have $e(R_1/P) = e(R_2/P) = 1$. Thus $L_i \subseteq L^{I(Q/P)}$, and so is their composite $L_1L_2 \subseteq L^{I(Q/P)}$. But $L = L_1L_2$, and so $e(Q/P) = 1$.

■

32.2 Frobenius

Remark 32.2.1: Let E/F be an extension of *finite* fields, so E/F is automatically Galois. Taking $F \coloneqq \mathbb{F}_q$, then E is of the form $E = \mathbb{F}_{q^m}$ for some m. Then $G(E/F)$ is cyclic of order m, and is generated by $x \mapsto x^q$, the **Frobenius map** on the finite field E/F. For number fields, we'll want a slightly different notion of Frobenius.

Remark 32.2.2: Let L/K be a Galois extension of number fields, P a prime of K unramified in L, and Q a prime of L above P. Then $\mathbb{F}_Q/\mathbb{F}_P$ is an extension of finite fields, so we know $\operatorname{red}_{Q/P}$ is a surjective group morphism, and the inertia group has size $e(Q/P)$, which is 1 in this situation. So this is an isomorphism between the "global" object $D(Q/P)$ and the "local" object $G(\mathbb{F}_Q/\mathbb{F}_P)$ on residue fields. We can pull back the generator on the right-hand side to define the **Frobenius element**

$$\operatorname*{Frob}_{Q/P} \coloneqq \operatorname{red}_{Q/P}^{-1}(x \mapsto x^q) \in D(Q/P) \qquad q \coloneqq \#\mathbb{Z}_K/P \coloneqq N(P).$$

Observation 32.2.3
Note that $\underset{Q/P}{\text{Frob}}$ is an element of $G(L/K)$ where for every $\alpha \in \mathbb{Z}_L, \underset{Q/P}{\text{Frob}}(\alpha) \equiv \alpha^q \bmod Q$ where $q \coloneqq N(P)$. So $\underset{Q/P}{\text{Frob}}$ acts by the qth power map in $\mathbb{Z}_L/Q$, and in fact this is a characterization of the Frobenius element.

Lemma 32.2.4 *(?).*
Suppose $\sigma \in \mathsf{Gal}(L/K)$ satisfies $\sigma(\alpha) \equiv \alpha^q \bmod Q$ for all $\alpha \in \mathbb{Z}_L$ where $q \coloneqq N(P)$. Then $\sigma = \underset{Q/P}{\text{Frob}}$.

Remark 32.2.5: Why this is useful: you can check if something is the Frobenius element by just checking this congruence.

Proof (?).
Take any $\alpha \in Q$, then $\sigma(\alpha) \equiv \alpha^q \bmod Q \equiv 0^q \bmod Q$ and so $\sigma(\alpha) \in Q$. So $\sigma(Q) \subseteq Q$, but these are maximal ideals, forcing equality. Then $\sigma(Q) = Q$ implies $\sigma \in D(Q/P)$ by definition, and now applying $\text{red}_{Q/P}(\sigma) = (x \mapsto x^q)$ is the qth power map and $\sigma = \text{red}^{-1}_{Q/P}(x \mapsto x^q) \coloneqq \underset{Q/P}{\text{Frob}}$. ■

Proposition 32.2.6 *(?).*
Suppose L/K is a Galois extension of number fields with $L/M/K$ where we additionally assume that M/K is Galois. For the tower $L/M/K$, take primes $Q/R/P$ where P is unramified in L. Then

$$\underset{R/P}{\text{Frob}} = \underset{Q/P}{\text{Frob}}\Big|_M.$$

Remark 32.2.7: Note that the right-hand side is an automorphism of L restricted to M, which is only an automorphism of M when M/K is Galois.

Proof (?).
Definition chasing and using characterization of Frobenius. It's enough to show that for all $\alpha \in \mathbb{Z}_M$, we have

$$\underset{Q/P}{\text{Frob}}\Big|_M (\alpha) \equiv \alpha^q \bmod R \qquad\qquad q = N(P).$$

Since $\alpha \in \mathbb{Z}_M$ and $M \subseteq L$ so we can think of $\alpha \in L$ and it makes sense to compute $\underset{Q/P}{\text{Frob}}(\alpha) \equiv \alpha^q \bmod Q$ since this is how Frobenius acts upstairs. So we just need to show that this congruence that holds for Q also holds for R. Consider the difference: it's in Q by the modular condition, and using that M/K is Galois, the Frobenius restricts to an automorphism of M and thus $\underset{Q/P}{\text{Frob}}(\alpha) \in M$ (and is in fact still in $\mathbb{Z}_M$). Thus we have a difference of two

things in $\mathbb{Z}_M$ and in Q, so

$$\operatorname*{Frob}_{Q/P}(\alpha) - \alpha^q \in Q \cap \mathbb{Z}_M = R.$$

■

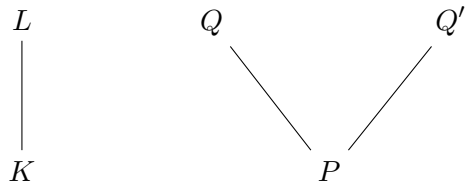
Remark 32.2.8: We'll see a nice example later of how to get the law of quadratic reciprocity from this!

33 Frobenius (April 20)

Remark 33.0.1: Setup and reminders:

- L/K a Galois extension of number fields,
- $P \in \operatorname{Spec} K$ unramified in L
- $Q \in \operatorname{Spec} L$ above P, so $e(Q/P) = 1$.
- The Frobenius was defined as $\operatorname{red}^{-1}_{Q/P}(x \mapsto x^q)$ for $q := N(P)$.
- The characterization theorem for Frobenius: $\sigma = \operatorname*{Frob}_{Q/P}$ iff $\sigma(\alpha) \equiv \alpha^q \bmod Q$, so Frobenius acts like that qth power map mod Q.
- When $L/M/K$ with M/K Galois with $Q/R/P$, $\operatorname*{Frob}_{R/P} = \operatorname*{Frob}_{Q/P}\Big|_M$

Proposition 33.0.2 *(?).*
Let L/K be Galois and let Q, Q' be two primes lying above P:



Link to Diagram

Since Galois acts transitively, we can write $Q' = \sigma(Q)$ for some $\sigma \in G(L/K)$. Then

$$\operatorname*{Frob}_{Q'/P} = \sigma \circ \operatorname*{Frob}_{Q/P} \circ \sigma^{-1}.$$

Proof (Sketch).
An exercise, use the characterization theorem. Set τ to be the right-hand side, and check that $\tau(\alpha) \equiv \alpha^p \bmod Q'$ for all $\alpha \in \mathbb{Z}_L$ and $q := N(P)$.

■

Remark 33.0.3: What can we do when we are given a P but not a Q? There are many choices of Q, all related by conjugation.

Definition 33.0.4 (Frobenius Conjugacy Class)
Define the **Frobenius conjugacy class** as

$$\left(\frac{L/K}{P}\right) = \left\{ \operatorname*{Frob}_{Q/P} \;\middle|\; Q \text{ lies above } P \right\} \subseteq G(L/K).$$

This is a conjugacy class of $G(L/K)$.

Remark 33.0.5: Note that this collapses to a single element when $G(L/K) \in \mathsf{Ab}$! By abuse of notation, we'll identify $\left(\frac{L/K}{P}\right)$ with that common element (despite it being a singleton set).

Proposition 33.0.6 ***(Order of Frobenius).***
Every element of $\left(\frac{L/K}{P}\right)$ has order f, where $f = f(Q/P)$ for any Q/P.

Proof (?).
Let Q/P be a prime over P, then $\operatorname*{Frob}_{Q/P} \coloneqq \operatorname{red}_{Q/P}^{-1}(x \mapsto x^q)$, where the qth power map is the generator of $G(\mathbb{F}_Q/\mathbb{F}_P)$, which has size $[\mathbb{F}_Q : \mathbb{F}_P] = f$. Since red was an isomorphism, we're done.

■

33.1 Cyclotomic Fields

Remark 33.1.1: Fix m. Recall that the mth cyclotomic field K is defined by

$$K \coloneqq \mathbb{Q}(\zeta_m) \qquad\qquad \zeta_m = e^{2\pi i/m}.$$

This is the splitting field of $x^m - 1$, and in characteristic zero this implies $K/\mathbb{Q}$ is Galois.

Proposition 33.1.2 ***(?).***

$$[K : \mathbb{Q}] = \varphi(m).$$

Definition 33.1.3 (Cyclotomic Polynomials)
Define the m**th cyclotomic polynomial** as

$$\Phi_m(x) \coloneqq \prod_{\substack{a \bmod m \\ (a,m)=1}} (x - \zeta_m^a).$$

Remark 33.1.4: Note that $\deg \Phi_m(x) = \varphi(m)$, since this is precisely how many terms show up in the indexing set. We'll show that this is the minimal polynomial of ζ_m

- The coefficients are algebraic integers, since the roots are all roots of $x^m - 1$, which is monic in $\mathbb{Z}[x]$. Since $\overline{\mathbb{Z}}$ is a ring, we have $\Phi_m(x) \in \overline{\mathbb{Z}}[x]$.

- If $\sigma \in G(K/\mathbb{Q})$, then $\sigma(\zeta_m) = \zeta_m^b$ for some b coprime to m. Then
$$\sigma(\Phi_m(x)) = \prod_{\substack{a \bmod m \\ (a,m)=1}} (x - \zeta_m^{ab}) = \Phi_m(x),$$
since as a runs through the number coprime to m, so does ab. Thus $\Phi_m(x) \in \mathbb{Q}[x]$, since its coefficients are fixed by every element of the Galois group.

- Combining these, the coefficients are in $\overline{\mathbb{Z}}[x] \cap \mathbb{Q}[x] = \mathbb{Z}[x]$.

Proposition 33.1.5 *(?).*
$\Phi_m(x) = m(x) \coloneqq \min_{\zeta_m}(x)$ is the minimal polynomial of ζ_m over $\mathbb{Q}$.

Proof (?).
Clearly $m(x) \mid \Phi_m(x)$ in $\mathbb{Q}[x]$ since $\Phi_m(x)$ vanishes at ζ_m. So every root of $m(x)$ is a primitive mth root of unity, so we just need to show that every primitive mth root of unity is a root of m, i.e. we get all of them. Observe that if ζ is *any* mth root of unity, then $\zeta \in \mathbb{Z}_K$: ζ is an algebraic integer, as a root of $x^m - 1$, and is in K since it's a power of ζ_m. Also note that $m(x) \in \mathbb{Z}[x]$ since the minimal polynomial of *any* algebraic integer has rational integer coefficients. So $m(\zeta) \in \mathbb{Z}_K$ since $\mathbb{Z}_K$ is a ring and $\zeta \in \mathbb{Z}_K$, and $N(m(\zeta)) \in \mathbb{Z}$.

Claim: There is an $M \in \mathbb{Z}^{\geq 0}$ such that if q is any prime with $q > M$ and ζ is any root of $m(x)$, then ζ^q is still a root of $m(x)$.
I.e. the roots of $m(x)$ are closed under taking qth powers for large enough q. Moreover, it's enough to pick any $M > \max_{\zeta} |N(m(\zeta))|$, taking ζ over all mth roots of 1.

Proof (of claim).
Let $q > M$ be chosen as above and let ζ be a root of $m(x)$. We know ζ is a primitive mth root of unity and in $\mathbb{Z}_K$. Work modulo Q: since $0 = m(\zeta)$ we have
$$0 \equiv m(\zeta)^q \equiv m(\zeta^q).$$
Hence
$$q \mid N(q) \mid N(m(\zeta^q)),$$
using that $N(q) = q^d$ since it's a rational integer where d is the degree of the number field. But we have $q > |N(m(\zeta^q))|$, which can only happen if the right-hand side is zero. The only element of norm zero in a number field is zero, so $m(\zeta^q) = 0$.
■

So if $q > M$ and ζ is a root of $m(x)$, so is ζ^q. ζ_m is a root of $m(x)$, thus so us $\zeta_m^{q_1}, \zeta_m^{q_1 q_2}, \cdots, \zeta_m^A$

for any $A \in \mathbb{Z}^{\geq 0}$ which can be written as a product of primes bigger than M.

Exercise *(?)*
Show that we can choose any $a \in \mathbb{Z}$ with $\gcd(a, m) = 1$, and choose A as above with $A \cong a \bmod m$.

With this, $\zeta_m^a = \zeta_m^A$ will be a root of $m(x)$ and we're done.

■

Remark 33.1.7: Note that the exercise does follow from Dirichlet's theorem for arithmetic progressions, but there are easier proofs.

33.2 Galois Theory of $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ and The Frobenius

Remark 33.2.1: Let $\sigma \in G(K/\mathbb{Q})$, then we saw that $\sigma(\zeta_m) = \zeta_m^a$ for some a coprime to m. So we know $\#G(K/\mathbb{Q}) < \varphi(m)$, since there are only that many possibilities for the right-hand side. Since $[K : \mathbb{Q}] = \varphi(m)$, for each a coprime to m there is a σ_a with $\sigma_a(\zeta_m) = \zeta_m^a$, so we can write

$$G(K/\mathbb{Q}) = \left\{ \sigma_a \;\middle|\; a \in (\mathbb{Z}/m)^\times \right\}.$$

Noting that $\sigma_a \sigma_b(\zeta_m) = \zeta_m^{ab} = \sigma_{ab}$, so we get an isomorphism

$$\begin{aligned} G(K/\mathbb{Q}) &\xrightarrow{\sim} (\mathbb{Z}/m)^\times \\ \sigma_a &\rightleftharpoons a \bmod m, \end{aligned}$$

so $K/\mathbb{Q}$ is an abelian extension.

Remark 33.2.2: Consider $K \coloneqq \mathbb{Q}(\zeta_m)$, then for every rational prime P unramified in K, there is a well-defined element in $\left(\frac{K/\mathbb{Q}}{P}\right) \in G(K/\mathbb{Q}) = (\mathbb{Z}/m)^\times$. For a given P, which element in $(\mathbb{Z}/m)^\times$ do you get?

Proposition 33.2.3 *(?).*
If $p \nmid m$, then p is unramified in $\mathbb{Q}(\zeta_m)$.

Remark 33.2.4: The converse is more or less true: $\mathbb{Q}(\zeta_2) = \mathbb{Q}$ since $\zeta_2 = -1$, but 2 is not ramified in $\mathbb{Q}$ since nothing is ramified in itself. So if you avoid $m \equiv 2 \bmod 4$, the converse becomes true. We'll just prove the mentioned direction.

Lemma 33.2.5 *(?).*

$$\mathbb{Z}_K = \mathbb{Z}[\zeta_m].$$

Exercise 33.2.6 (?)
Show that p ramifies in K iff $\mathbb{Z}_K/p\mathbb{Z}_K$ has a nonzero nilpotent element.

Proof (of proposition, cute!).
Suppose $p \nmid m$, then it suffices to show that $\mathbb{Z}[\zeta_m]/p\mathbb{Z}[\zeta_m]$ has no nonzero nilpotents. Let $\alpha \in \mathbb{Z}[\zeta_m]$ with $\alpha \bmod p$ nilpotent in the quotient, we'll show it must be zero in the quotient. By the lemma, we can write $\alpha = \sum_{i=0}^{d-1} a_i \zeta^i$, using that $\mathbb{Z}_K = \mathbb{Z}[\zeta]$ where all of the a_i are in $\mathbb{Z}$, we've set $\zeta \coloneqq \zeta_m$ and $d = \varphi(m) = [K : \mathbb{Q}]$.
Look mod p, then

$$\alpha^p \equiv \sum_{i=0}^{d-1} a_i \zeta^{ip} \bmod p \implies \alpha^{p^f} \equiv \sum_{i=0}^{d-1} a_i \zeta^{ip^f} \bmod p \qquad \forall f.$$

If f is large enough, $\alpha^{p^f} \equiv 0 \bmod p$, since some power of α is zero. On the other hand, $p \nmid m$, so there are powers of p that are $1 \bmod m$ that show up regularly, and we can choose f so that $p^f \cong 1 \bmod m$, e.g. by choosing f to be any multiple of the order of p mod m. But then the second line above reduces to $\sum a_i \zeta^{ip^f} \equiv \sum a_i \zeta^i = \alpha$ since $p^f \equiv 1 \bmod m$, so $\alpha^{p^f} \equiv \alpha$, but we know $\alpha^{p^f} \equiv 0$.

■

Theorem 33.2.7 ***(?).***
Suppose $p \nmid m$, which guarantees p does not ramify in K. Then

$$\left(\frac{K/\mathbb{Q}}{P}\right) = \sigma_p \qquad \sigma_p(\zeta_m) \coloneqq \zeta_m^p.$$

Proof (?).
Choose any Q lying above p. We'll show that for all $\alpha \in \mathbb{Z}_K$, $\sigma_p(\alpha) = \alpha^p \bmod Q$, which by the characterization theorem will show $\sigma_p = \operatorname{Frob}_{Q/P}$, and in the abelian case $\left(\frac{K/\mathbb{Q}}{p}\right)$ reduces to this single element. We know that $Q \supseteq p\mathbb{Z}_K$ since Q is above p, so it's enough to show $\sigma_p(\alpha) \equiv \alpha^p \bmod p$ for all $\alpha \in \mathbb{Z}_K$ – this is because the difference is a multiple of p in $\mathbb{Z}_K$, which is a subset of Q. Using $\mathbb{Z}_K = \mathbb{Z}[\zeta_m]$ to write $\alpha = \sum_{i=0}^{d-1} a_i \zeta_m^i$ where d is the degree of the extension. Now reducing $\bmod p$ and applying the Freshman's dream yields

$$\begin{aligned}
\sigma_p(\alpha) &= \sum_{i=0}^{d-1} a_i \zeta_m^{ip} \\
&\equiv \left(\sum_{i=0}^{d-1} a_i \zeta_m^i\right)^p \bmod p \\
&\equiv \alpha^p.
\end{aligned}$$

■

Remark 33.2.8: This can be used to determine how all of the primes $p \nmid m$ factor in $\mathbb{Q}(\zeta_m)$, i.e. easily determining the relevant values of f and g.

34 Chebotarev Density (April 26)

34.1 Setup

Remark 34.1.1: Today: the Frobenius element, cyclotomic extensions of $\mathbb{Q}$, Chebotarev density theorem, and some applications. We'll then look at applying Frobenius to understanding squares modulo a prime and get a proof of quadratic reciprocity.

Setup: let L/K be a Galois extension of number fields, $P \in \operatorname{Spec} K$ unramified in L, and $Q \in \operatorname{Spec} L$ lying above p.

- There is a unique element $\operatorname*{Frob}_{Q/P} \in \mathsf{Gal}(L/K)$ satisfying

$$\operatorname*{Frob}_{Q/P}(\alpha) = \alpha^p \bmod q \qquad\qquad p \coloneqq \#\mathbb{Z}_K/p.$$

- As Q ranges over the primes of L over P, then $\operatorname*{Frob}_{Q/P}$ ranges over an entire conjugacy class, which we denoted $\left(\frac{L/K}{P}\right)$. For abelian Galois groups, we'll identify this class with its single representative.

Remark 34.1.2: How does this theory play out for cyclotomic extensions? We've seen that for $K \coloneqq \mathbb{Q}(\zeta_n)$, the extension $K/\mathbb{Q}$ is Galois of degree $\varphi(m) = \#(\mathbb{Z}/m)^\times$, and moreover these are isomorphic via

$$\begin{aligned}(\mathbb{Z}/m)^\times &\to \mathsf{Gal}(K/\mathbb{Q}) \\ a \bmod m &\mapsto \sigma_a : \zeta_a \mapsto \zeta_m^a.\end{aligned}$$

Proposition 34.1.3 *(?).*
If p is prime and $p \nmid m$, then p is unramified in K. We proved this last time, and it follows that $\left(\frac{K/Q}{P}\right) \in \mathsf{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/m)^\times$. Moreover, we saw that

$$\left(\frac{K/Q}{P}\right) \equiv p \bmod m.$$

Remark 34.1.4: Thus for any two primes not dividing m which become equal modulo m, then they split in the same way in the cyclotomic field. So the way a rational prime splits in $\mathbb{Q}(\zeta_m)$ is entirely determined by its residue class $\bmod m$.

Corollary 34.1.5 ***(?).***
If p is a prime not dividing m, then e, f, g depend only on $p \bmod m$.

Proof (?).
If p doesn't divide m, p is unramified and $e = 1$. Recall that f is the order of any Frobenius element above p in the Galois group, $\left(\frac{K/Q}{P}\right) = p \bmod m$ in $(\mathbb{Z}/m)^\times$. Note that $efg = \varphi(m)$ is the degree of the field, and solving yields $g = \varphi(m)/f$.
■

Remark 34.1.6: In class field theory, there are analogs of this, foreshadowing something that happens in general for abelian extensions of number fields. In fact, every such extension is a subfield of the cyclotomic field.

34.2 Chebotarev's Theorem

Question 34.2.1
A classical question: let $a \bmod m$ be a coprime residue class, are there infinitely many (positive) rational primes p with $p \equiv a \bmod m$? For instance, are there infinitely many primes p satisfying $p \equiv 5 \bmod 11$?

Remark 34.2.2: Note that only coprime residue classes are interesting here. Considering, say, $p \equiv 5 \bmod 10$ would only yield multiples of 5 and thus $p = 5$ is the only solution. In general, for $a \bmod m$ with a, m not coprime, there is at most one solution.

Answer 34.2.3
For a, m coprime, it is a theorem of Dirichlet that there are infinitely many. This proof uses L-functions and their analytic behavior.

Theorem 34.2.4 ***(Chebotarev's Density Theorem: The Fundamental Theorem of Algebroanalytic Number Theory).***
Let L/K be a Galois extension of number fields and C a conjugacy class of $\mathsf{Gal}(L/K)$. Note that for every prime P of K that is unramified in L, we can associate the Frobenius conjugacy class. There are only finitely many primes of K that ramify in L, so all but finitely many primes yield a conjugacy class – is it this fixed conjugacy class C?
The theorem is that there are infinitely many primes P of K for which P is unramified in L and the Frobenius conjugacy class satisfies $\left(\frac{L/K}{P}\right) = C$.

Remark 34.2.5: This is qualitatively stated, but one can make this quantitative – there is a well-defined proportion of primes for which this is true. Letting P range over the primes of K, the

proportion with $\left(\frac{L/K}{P}\right) = C$ will be $\#C/[L:K]$. Here *proportion* is defined in the following way:

$$\lim_{x\to\infty}\left(\frac{\#\left\{P \in \operatorname{Spec} K \;\middle|\; N(P) \le x, \left(\frac{L/K}{P}\right) = C\right\}}{\#\left\{P \in \operatorname{Spec} K \;\middle|\; N(P) \le x\right\}}\right),$$

which is sometimes called the *natural density* of these primes. What Chebotarev proved is slightly weaker and involved the *Dirichlet density* instead.

Corollary 34.2.6 ***(?).***
We recover Dirichlet's theorem on primes $p \equiv a \bmod m$ by taking $L := \mathbb{Q}(\zeta_m)$, $K = \mathbb{Q}$, and $C := \{a \bmod m\}$. The density theorem yields infinitely many primes P with Frobenius equal to C, but then $\left(\frac{L/K}{p}\right) = \{p \bmod m\}$, yielding $p \equiv a \bmod m$. Moreover the proportion of such primes is $1/\varphi(m)$, the degree of $[L:K]$, so the coprime residue classes are essentially distributed uniformly.

Remark 34.2.7: This is useful when one needs infinitely many primes of a certain form, for which one can apply the density theorem to a well-chosen extension of number fields.

Question 34.2.8
Consider primes p and consider the multiplicative order of $2 \bmod p$, which is a divisor of $p-1$. How often is this order even or odd? One might expect this to happen half of the time, but this is not true. Instead:

Corollary 34.2.9 ***(of a strong Chebotarev theorem, due to Hasse).***
The proportion of p for which 2 has even order $\bmod p$ is $17/24$.

Remark 34.2.10: Note that 2 is special, and this proportion changes for $3 \bmod p$ to something around $2/3$. Interesting algebraic number theory governs why this is *not* $17/24$, and involves how different number fields intersect.

34.3 Residues $\bmod p$ and Quadratic Reciprocity

Remark 34.3.1: If G is a cyclic group of even order, there is a unique morphism

$$\varphi_G : G \to \{\pm 1\}$$
$$g \mapsto \begin{cases} 1 & g \in G^2 \\ -1 & \text{else.} \end{cases}$$

Definition 34.3.2 (Legendre Symbol)
Let p be an odd prime, and let $G \coloneqq (\mathbb{Z}/p)^\times$ which is cyclic of order $p-1$. For each $a \in \mathbb{Z}$ coprime to p, define the **Legendre symbol**

$$\left(\frac{a}{p}\right) \coloneqq \varphi_G(a \bmod p) = \begin{cases} 1 & a = a_0^2 \bmod p \text{ for some } a_0 \in G \\ -1 & \text{else]}. \end{cases}$$

Note that this is a group morphism, and thus multiplicative and we get

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \qquad a, b \in \mathbb{Z} \text{coprime to} p.$$

One can also extend the symbol by defining $\left(\frac{n}{p}\right) = 0$ when n is not coprime to p.

Question 34.3.3
Given a, can we characterize the primes p (not dividing a) for which $\left(\frac{a}{p}\right) = 1$.

Remark 34.3.4: Let $K = \mathbb{Q}(\sqrt{d})$ where d is squarefree, then $K/\mathbb{Q}$ is abelian and the Galois group can be thought of as $G \coloneqq \mathsf{Gal}(K/\mathbb{Q}) = \{\pm 1\}$. Each rational prime P unramified in K will yields a well-defined Frobenius conjugacy class in K, and since G is a abelian this is a single element – which element is it?

If p is an odd prime not dividing d, we know from our study of quadratic fields that p is unramified in K.

Proposition 34.3.5 ***(?).***
Let p be an odd prime not dividing d, then

$$\left(\frac{K/\mathbb{Q}}{p}\right) = \left(\frac{d}{p}\right),$$

where we've identified the Galois group as $\{\pm 1\}$. Thus is d is a square mod p, the Frobenius is trivial, and conversely if d is not a square then the Frobenius is nontrivial.

Proof (?).
Since p is odd not dividing d, p doesn't ramify and thus $e = 1$. Since we're in a quadratic field, the only other things that can happen are being split (completely) or inert. So when does p split? This is precisely when $g = 2$, so there are two primes above p, and we know $efg = 2$ is the degree of the extension, so $f = 1$. But f is the order of any Frobenius element, so the order of $\left(\frac{K/\mathbb{Q}}{p}\right) = 1$, making it the identity. So p splits $\iff \left(\frac{K/\mathbb{Q}}{p}\right) = 1$.
On the other hand, when we worked out how primes factor in quadratic fields, we used Dedekind-Kummer, and if p is odd not dividing d then $\left(\frac{d}{p}\right) = 1$. Equivalently, p splitting

involves looking at how $x^2 - d$ factors in K, and that's what yields this condition. So p splits $\iff \left(\frac{d}{p}\right) = 1$.

Note that looking at how arbitrary primes factor involves looking at the minimal polynomial of $\tau = \sqrt{d}, \frac{1+\sqrt{d}}{2}$, but we can throw out the second case here if we're willing to throw out primes dividing the index $[\mathbb{Z}_K : \mathbb{Z}[\sqrt{d}]] \in \{1, 2\}$. So for odd primes, the way p factors is exactly the way $x^2 - d$ factors.

Thus p splits iff both of these quantities are $+1$ and doesn't split iff they're both -1, so they must be equal.

■

Proposition 34.3.6 *(?).*
If p is an odd prime,

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & p \equiv 1 \bmod 4 \\ -1 & \text{else.} \end{cases}$$

Proof (?).
Consider $K \coloneqq \mathbb{Q}(\sqrt{-1})$. If p is an odd prime, we can identify $\mathsf{Gal}(K/\mathbb{Q}) = \{\pm 1\}$ to obtain

$$\left(\frac{K/\mathbb{Q}}{p}\right) = \left(\frac{-1}{p}\right).$$

Note that K is also the cyclotomic extension $K = \mathbb{Q}(\zeta_4)$, and for cyclotomic extensions we can compute the Frobenius elements as $\left(\frac{K/\mathbb{Q}}{p}\right) \equiv p \bmod 4$, viewing $\mathsf{Gal}(K/\mathbb{Q}) = (\mathbb{Z}/4)^\times$.

From the first perspective, we have $\left(\frac{K/\mathbb{Q}}{p}\right) = \text{id} \iff \left(\frac{-1}{p}\right) = 1$, and from the second perspective this happens $\iff p \equiv 1 \bmod 4$.

■

Remark 34.3.7: This is perhaps overkill, but it's nice that it follows easily from the general theory! What about 2 instead of -1?

Proposition 34.3.8 *(?).*
If p is an odd prime,

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv \pm 1 \bmod 8 \\ -1 & \text{else.} \end{cases}$$

Remark 34.3.9: The usual elementary proof uses Gauss' lemma, and there are other proofs that use clever counting.

Proof (?).
We have a tower of extensions $K/L/\mathbb{Q} \coloneqq \mathbb{Q}(\zeta_8)/\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, and consider corresponding primes $Q/R/P$. Since the overall extension is Galois, by the Galois correspondence we can write $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\zeta_8)^H$ as the fixed field of some $H \leq G \coloneqq \mathsf{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q})$ of index 2.
We know that $G = (\mathbb{Z}/8)^\times$ which has size 4, so H has 2 elements: the identity and an order 2 element. All of the $g \in G$ are order 2, so which is it? We look for an automorphism of $K/\mathbb{Q}$ fixing L, and taking σ to be complex conjugation works since $\sigma(\zeta_8) = \zeta_8^{-1} \neq \zeta_8$, so $\sigma \neq \mathrm{id}$ is nontrivial. So $\sigma = -1 \bmod 8$ and we can write $H = \{\pm 1 \bmod 8\}$.
Now note that

$$\left(\frac{2}{p}\right) = 1 \iff \left(\frac{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}{p}\right) = \mathrm{id},$$

since the Legendre and Frobenius symbols are equal here. This happens $\iff \underset{R/P}{\mathrm{Frob}} = \mathrm{id} \iff$

$\left.\underset{Q/P}{\mathrm{Frob}}\right|_{\mathbb{Q}(\sqrt{2})} = \mathrm{id}$, using what we've previously proved about how Frobenius behaves in towers of extensions. This happens $\iff \left(\frac{\mathbb{Q}(\zeta_8)/\mathbb{Q}}{P}\right) \in H \iff p \bmod 8 \in \{\pm 1 \bmod 8\}$.

■

Remark 34.3.10: For a general $a \in \mathbb{Z}_{\neq 0}$, we can factor $a = (\pm 1)(2^k)\prod p_i$ where the p_i are odd primes. Using multiplicativity of the Legendre symbol, since we understand the first two terms, it only remains to understand $\left(\frac{q}{p}\right)$ for q an odd prime – this is precisely what quadratic reciprocity gives us.

35 Quadratic Reciprocity (April 29)

Remark 35.0.1: Last time: quadratic residues mod p, and how all of the usual content from a first course in number theory follows immediately from the high-powered machinery of the Frobenius and cyclotomic fields. The problem we were looking at was the following: given $a \in \mathbb{Z}_{\neq 0}$, classify all odd primes p where $\left(\frac{a}{p}\right) = 1$.

For $a = -1$, we saw that this happens iff $p \equiv 1 \bmod 4$, and for $a = 2$, $p \equiv \pm 1 \bmod 8$. The key facts for the latter were that $\mathbb{Q}(i) = \mathbb{Q}(\zeta_4)$ and $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\zeta_8)$. Then because the Legendre symbol is multiplicative, we can reduce to the case $a = q$ is an odd prime.

This was solved by Gauss in the early 19th century, which he called the "golden theorem", but is more commonly known now as the law of quadratic reciprocity.

35.1 Quadratic Reciprocity

Definition 35.1.1 (?)
For an odd prime p, define $p^* := \pm p$ with the sign chosen such that $p^* \equiv 1 \bmod 3$. Explicitly, one can check that $p^* = (-1)^{\frac{p-1}{2}} p$. The law of **quadratic reciprocity** states the following: if p, q are distinct odd primes, then

$$\left(\frac{q^*}{p}\right) = \left(\frac{p}{q}\right).$$

Remark 35.1.2: This is not the usual formulation, but it can be recovered easily: note that

$$\begin{aligned}
\left(\frac{q^*}{p}\right) &= \left(\frac{(-1)^{\frac{q-1}{2}} q}{p}\right) \\
&= \left(\frac{-1}{p}\right)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) \\
&= \left((-1)^{\frac{p-1}{2}}\right)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) \\
\implies (-1)^{\frac{p-1}{2}\frac{q-1}{2}} &= \left(\frac{p}{q}\right)\left(\frac{q}{p}\right),
\end{aligned}$$

where the last step follows from multiplying through by $\left(\frac{q}{p}\right)$ and noting that $\left(\frac{q}{p}\right)^2 = 1$

Proof (of quadratic reciprocity).
Let $p \neq q$ be distinct odd primes. Then $\mathsf{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) \cong (\mathbb{Z}/q)^\times$. Since this is a cyclic group of even order, there is a unique index 2 subgroup, which we can take to be the subgroup of square $U(\mathbb{Z}/q)^2$. By Galois theory, the fixed field $\mathbb{Q}(\zeta_q)^H$ corresponds to a unique quadratic subfield.

Claim: This subfield is exactly $\mathbb{Q}(\sqrt{q^*})$.

Proof (?).
Let $K := \mathbb{Q}(\zeta_q)^H$, so we have a tower $\mathbb{Q}(\zeta_q)/K/\mathbb{Q}$. Suppose r is a prime that ramifies in K, then it ramifies in any larger field by multiplicativity of the e values. So r ramifies in $\mathbb{Q}(\zeta_q)$, but the only primes that can possibly ramify in any $\mathbb{Q}(\zeta_m)$ are those that divide m. So $r \mid q$, forcing $r = q$, so the only prime that ramifies is q.
Write $K = \mathbb{Q}(\sqrt{d})$ for d squarefree, then every prime dividing d is ramified in K. So d is not divisible by any primes other than q. Thus d could be $\pm q$ or -1, noting that the $d = 1$ case doesn't yield a quadratic extension, and we'd like to show that q^* is the only viable option. We can rule out $d = -1$, since 2 ramifies in $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i)$ – but the only prime that can ramify is q, which was an *odd* prime.
We can also rule out which ever value of q yields $q \equiv 3 \bmod 4$, since again 2 ramifies in this case. This was a general fact: for $K = \mathbb{Q}(\sqrt{d})$ with $d \equiv 3 \bmod 4$, then 2 automatically ramifies. So $q \equiv 1 \bmod 4$, and $d = q^*$.
■

Remark 35.1.3: This can also be proved with Gauss sums, but we don't necessarily need that here.

Continuing the proof, consider $\mathbb{Q}(\zeta_q)/\mathbb{Q}(\sqrt{q^*})/\mathbb{Q}$ with primes $Q/R/p$ lying over p. We'll show that $\left(\frac{p}{q}\right) = 1 \iff \left(\frac{q^*}{p}\right) = 1$, making them equal. Note that $\left(\frac{p}{q}\right) = 1 \iff p$ is a square in $U(\mathbb{Z}/q) \iff \operatorname{Frob}_{Q/p} \in H$. This happens $\iff \operatorname{Frob}_{Q/p}\Big|_{\mathbb{Q}\sqrt{q^*}} = \mathrm{id}$, which we can write as $\operatorname{Frob}_{R/P} = \mathrm{id}$, or equivalently the symbol $\left(\frac{\mathbb{Q}(\sqrt{q^*}/\mathbb{Q})}{p}\right) = \mathrm{id}$. Since we can write this as the Legendre symbol $\left(\frac{q^*}{p}\right) = 1$ when we identify $\mathsf{Gal}(\mathbb{Q}(\sqrt{d^*})/\mathbb{Q}) \cong \{\pm 1\}$, which is precisely what we wanted.

■

35.2 Applying Quadratic Reciprocity: Recovering Classical Results

Example 35.2.1 ***(of applying quadratic reciprocity):*** Let $a = 6$, then for odd primes p not dividing 6,

$$\left(\frac{6}{p}\right) = 1 \iff p = 1, 5, 19, 23 \bmod 24.$$

Note that $6 \mid 24$, and importantly $\varphi(24) = 8$ and this allowed list is 4 elements, so exactly half are squares.

Theorem 35.2.2 ***(?).***
Let $a \in \mathbb{Z}_{\neq 0}$ with a not a square, then

1. If p, p' are distinct odd primes not dividing a with $p \equiv p' \bmod 4|a|$, then $\left(\frac{a}{p}\right) = \left(\frac{a}{p'}\right)$. So $\left(\frac{a}{p}\right) = 1$ is entirely a function of the equivalence class of $p \bmod 4|a|$.
2. The number of allowable residue class modulo $4|a|$ is precisely $\frac{1}{2}\varphi(4|a|)$.

Remark 35.2.3: For odd p not dividing a, we have $\left(\frac{a}{p}\right) = \left(\frac{\mathbb{Q}(\sqrt{a})/\mathbb{Q}}{p}\right)$ where we identify $\mathsf{Gal}(\mathbb{Q}(\sqrt{a})/\mathbb{Q}) = \{\pm 1\}$. We did this for a squarefree, but we can generally write $a = a_0 a_1^2$ with a_0 squarefree, and the claim is that replacing a with a_0 doesn't change either side of this equality. The right-hand side doesn't change since $\mathbb{Q}(\sqrt{a}) \cong \mathbb{Q}(\sqrt{a_0})$, and the left-hand side doesn't change because

$$\left(\frac{a}{p}\right) = \left(\frac{a_0}{p}\right)\left(\frac{a_1}{p}\right)^2 = \left(\frac{a_0}{p}\right) \cdot 1 = \left(\frac{a_0}{p}\right).$$

Lemma 35.2.4 *(?).*
The proportion of primes p with $\left(\frac{a}{p}\right) = 1$ is exactly $1/2$.

Proof (of lemma).
If p is odd and doesn't divide a, so p doesn't divide $2a$, then $\left(\frac{a}{p}\right) = \left(\frac{\mathbb{Q}(\sqrt{a})/\mathbb{Q}}{p}\right)$. Applying Chebotarev's density to this Frobenius yields that the proportion of p for which the right-hand side equals 1 is $\#\{\text{id}\}/2 = 1/2$, noting that the denominator is just the degree of the extension, which is quadratic.

■

Exercise 35.2.5 (A fun one)
For what proportion of p is 2 a cube mod p?

Proof (of theorem, part 1).
Suppose $p \equiv p' \bmod 4|a|$ with $p \nmid 2a$. From a homework problem, $\mathbb{Q}(\sqrt{a}) \subseteq \mathbb{Q}(\zeta_{4|a|})$. So we have a tower $\mathbb{Q}(\zeta_{4|a|})/\mathbb{Q}(\sqrt{a})/\mathbb{Q}$, and corresponding towers of primes $Q/R/p$ and $Q'/R'/p'$. Since we're assuming $p \equiv p' \bmod 4|a|$, we have $\underset{Q/p}{\text{Frob}} = \underset{Q'/p'}{\text{Frob}}$. Restricting both to $\mathbb{Q}(\sqrt{a})$ we get

- $\underset{R/p}{\text{Frob}} = \left(\frac{\mathbb{Q}(\sqrt{a})/\mathbb{Q}}{p}\right) = \left(\frac{a}{p}\right)$,
- $\underset{R'/p'}{\text{Frob}} = \left(\frac{\mathbb{Q}(\sqrt{a})/\mathbb{Q}}{p'}\right) = \left(\frac{a}{p'}\right)$,

so the two Legendre symbols are equal.

■

Proof (of theorem, part 2).
List the coprime residue classes mod $4|a|$ corresponding to $\left(\frac{a}{p}\right) = 1$, say $a_1, \cdots, a_k \bmod 4|a|$. By Dirichlet's theorem on prime progressions (or Chebotarev density on $\mathbb{Q}(\zeta_{4|a|})$), we know that the proportion of p with $p \equiv a_i \bmod 4|a|$ is $1/\varphi(4|a|)$. Adding these up yields $k/\varphi(4|a|)$. But we just computed this proportion alternatively and found it to be $1/2$, so this forces $k = (1/2)\varphi(4|a|)$.

■

Exercise 35.2.6 (?)
Think about the theorem of Hasse which stated that the primes p for which 2 has an even order mod p has density $17/24$. A way to start: divide up the primes according to the largest power of 2 that divides $p-1$. For $2^1 \mid p-1$ but 2^2 does not, these are primes $p \equiv 3 \bmod 4$, a has even order precisely when a is not a square mod p, since otherwise if a is a square then the order will divide $\frac{p-1}{2}$, which is odd, and the order will be odd. So one should think about which primes $p \equiv 3 \bmod 4$ for which (for example) 2 is not a square mod p, and these ideas will apply.

For $2^2 \mid p-1$ but 2^3 does not, such primes are of the form $p \equiv 5 \bmod 8$. When does 2 have even order? Now one needs 2 not to be a *fourth* power, and one can find the density of primes for which 2 is not a 4th power mod p and $p \equiv 5 \bmod 8$ using these ideas, but it's harder.
For 2^3, one gets $p \equiv 9 \bmod 16$ and needs 2 to not be an eighth power.
Doing this for every k and summing all of the densities will yield 17/24.

ToDos

List of Todos

Definitions

Theorems

Exercises

Figures

List of Figures