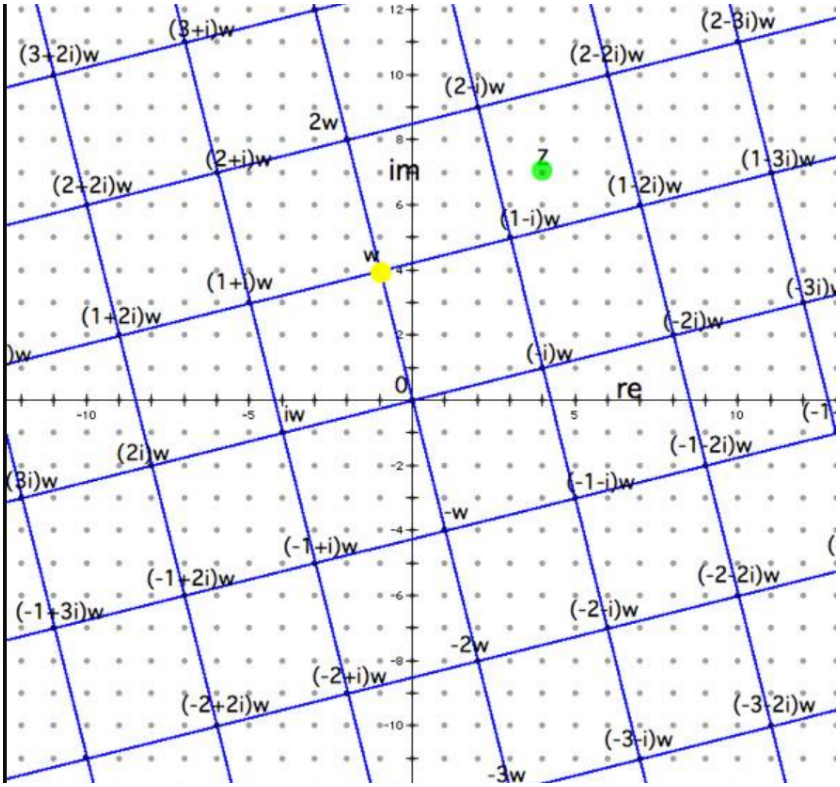


Notes: These are notes live-tex'd from a graduate course in Algebraic Number Theory taught by Paul Pollack at the University of Georgia in Spring 2021. As such, any errors or inaccuracies are almost certainly my own.

Algebraic Number Theory

Lectures by Paul Pollack. University of Georgia, Spring 2021

D. Zack Garza

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

Last updated: 2021-01-28

Table of Contents

Contents

1 | Thursday, January 14

See website for notes on books, intro to class.

- Youtube Playlist: https://www.youtube.com/playlist?list=PLAOxtXqOUji8fjQysx4k8a6h-hOZ7x5ue
- Free copies of textbook: https://www.dropbox.com/sh/rv5j222kn74bjhm/AABZ1qcR1rOnpaBsa5CL3P_Ea?dl=0&lst=
- Course website: ?

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."

1.1 Motivation

Solving Diophantine equations, i.e. polynomial equations over $\mathbb{Z}$.

Example 1.1.1 ***(?):*** 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 1.1.2 ***(Fermat):*** Consider $y^2 = x^3 - 2$.

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

Rewrite

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

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 1.1.3 ***(Norm Map)***
For $\alpha \in \mathbb{Z}[\sqrt{-2}]$ define $N\alpha = \alpha\overline{\alpha}$.

Lemma 1.1.4 ***(?).***
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 $1 = \alpha\overline{\alpha}$ if $N(\alpha) = 1 \in R^\times$. Conversely if $\alpha \in R^\times$ write $\alpha\beta = 1$, then

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

which forces both to be 1.

■

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

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

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

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

■

We can identify the units in this ring:

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

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.

Example 1.1.5 ***(?):*** 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 1.1.6
When does a ring admit unique factorization? Do you even *need* it?

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!

2 | Lecture 2 (Tuesday, January 19)

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

Remark 2.0.2: 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 2.0.3 *(?):* $\mathbb{Q}[\sqrt[3]{2}, \mathbb{Q}[\sqrt{2}, \sqrt[5]{7}]$ or $\mathbb{Q}(\theta)$ where θ is a root of $x^5 - x - 1$ (which you can check is irreducible. Now that the round vs. square brackets here won't make a difference, since we're adjoining algebraic numbers.

Proposition 2.0.4 *(?).*
Let $K_{/\mathbb{Q}}$ be a finite extension, say of degree $n \coloneqq [K : \mathbb{Q}]$. Then there are n distinct embeddings [a] of K into $\mathbb{C}$

[a] An injective ring morphism.

Proof (?).
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 $f = \prod_{i=1}^{n}(x - \theta_i$ which each $\theta_i \in CC$ 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 inject 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 2.0.5 (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 2.0.6: If σ is a nonreal, then $\overline{\sigma}$ is a nonreal embedding, so this 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 2.0.7 *(?):* 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 $3 = 1 + 2(1)$ and this is consistent.

Remark 2.0.8: We've only been talking about fields, since unique factorization is trivial since there are no primes. There are thus "too many" units, compared to the rings we were considering before, so we'll restrict to subrings. 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 2.0.9 (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 2.0.10: 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 2.0.11 ***(?).***
$\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ is a subfield and every number field is a subfield of $\overline{\mathbb{Q}}$.

These are still fields, so lets define some interesting subrings.

Definition 2.0.12 ($\overline{\mathbb{Z}}$)
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 2.0.13 ***($\overline{\mathbb{Z}}$ is a ring).***
$\overline{\mathbb{Z}}$ is a ring, and in fact a domain since it's a subring of $\mathbb{C}$.

We'll use an intermediate criterion to prove this:

Proposition 2.0.14 ***(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

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

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

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

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 $\det(x \operatorname{id} - A) \in \mathbb{Z}[x]$ 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 $+, \cdot$.

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: $\left\{\alpha^i \beta^j\right\}_{\substack{0 \le i < n \\ 0 \le j < m}}$, 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 $0 \le I, J \in \mathbb{Z}$, the term $\alpha^I \beta^J$ is a $\mathbb{Z}$-linear combination of the restricted elements above. Divide by f and g to obtain $x^I = f(x)q(x) + r(x)$ and $x^J = g(x)\tilde{q}(x)\tilde{r}(x)$ 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 2.0.15: We've just filled in another part of the previous picture:

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

Definition 2.0.16 (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 2.0.17: 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 (noting that $\sqrt{2}$ is not a unit) as $\sqrt{\sqrt{2}} \cdot \sqrt{\sqrt{2}}$, 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 is thus not Noetherian.

The following is a reality check, and certainly a property we would want:

Proposition 2.0.18 ***(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 $a \mid a_0, b \mid 1$, so $b = \pm 1, \alpha = a/\pm 1 = \pm a \in \mathbb{Z}$ and thus $\alpha \in \mathbb{Z}$.

■

We'll want to study $\mathbb{Z}_K$ for various number fields K, but we'll need more groundwork.

Proposition 2.0.19 ***(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 2.0.20 ***(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 2.0.21 *(*$\mathrm{ff}(\mathbb{Z}_K) = K$ *).*

a. $\overline{\mathbb{Z}}$ has $\overline{\mathbb{Q}}$ as its fraction field, and
b. For any number field K, $\mathbb{Z}_K$ has K as its fraction field.

Moreover, both of these statements follow from:

c. If $\alpha \in \overline{\mathbb{Q}}$ then $d\alpha \in \overline{\mathbb{Z}}$ for some $d \in \mathbb{Z}^{\geq 0}$

Remark 2.0.22: 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 2.0.23 (?)
Prove the proposition!

Proposition 2.0.24 *(?).*
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 2.0.25: 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 2.0.26 (Prove the proposition.)
Prove this! Can use the integrality criterion (slightly challenging), can also use Galois theory.

3 | Lecture 3 (Thursday, January 21)

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.

3.1 Quadratic Number Fields

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

Definition 3.1.1 (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 3.1.2: 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 3.1.3 *(?).*
If K is a quadratic number field, then $K = \mathbb{Q}(\sqrt{d})$ for some squarefree [a] $d \in \mathbb{Z}$. 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 (?).
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 $\alpha = \dfrac{-B \pm \sqrt{B^2 - 4AC}}{2A}$ where $A \neq 0$ since this would imply that $\alpha \in \mathbb{Q}$. Writing $\Delta \coloneqq B^2 - 4AC$, 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 it 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.

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

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

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

Remark 3.1.5: 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 $a, b \in \mathbb{Q}$.
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 $g \in \mathrm{Gal}(K_{/\mathbb{Q}})$ with $\sigma(a + b\sqrt{d} = a - b\sqrt{d}$. We'll refer to this automorphism as **conjugation**. We can compute

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

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 $d_1 = d_2$.

■

Note that this results holds for every squarefree number not equal to 1.

Question 3.1.6
If $K = \mathbb{Q}(\sqrt{d})$, what is the ring of integers $\mathbb{Z}_K$? Some more machinery will help here.

Definition 3.1.7 (The Field Polynomial of an Element)
Assume $K_{/\mathbb{Q}}$ is a Galois number field and for $\alpha \in K$ define

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

Remark 3.1.8: 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 3.1.9 *(?).*

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

Proof (?).
$\Longleftarrow$: 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 3.1.10 *(?):* 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 $x^2 - x - 1 \in \mathbb{Z}[x]$.

Theorem 3.1.11 *(?).*
Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic number field. Then if $d = 2, 3 \pmod 4$, then $\mathbb{Z}_K = \left\{ a + b\sqrt{d} \;\middle|\; a, b \in \mathbb{Z} \right\}$. If $d = 1 \pmod 4$, then $\mathbb{Z}_K = \left\{ \dfrac{1 + b\sqrt{d}}{2} \;\middle|\; a, b \in \mathbb{Z},\ a \equiv b \pmod 2 \right\}$.

Remark 3.1.12: 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 $A, B \in \frac{1}{2}\mathbb{Z}$, so write $A = (1/2)a'$ and $B = (1/2)b'$. Writing $\alpha = (1/2)a' + (1/2)b'\sqrt{d}$, we find that $N(\alpha) = ((a')^2 - d(b')^2)/4 \in \mathbb{Z}$. So the numerator is a multiple of 4, which yields $(a')^2 \equiv d(b')^2 \pmod 4$. We proceed by cases.
Case 1: $d = 2, 3 \pmod 4$. If b' is odd then $(b')^2 = 1 \pmod 4$, which holds for any odd number. But then $(a')^2 = d(b')^2 = d \pmod 4$, which is a problem – squares modulo 4 can only be 0 or 1. This is a contradiction, so b' must be even. Then $(b')^2 \pmod 4 = 0$, which forces $a' \equiv 0 \pmod 4$ and a' must be even. But if a', b' are both even, $(1/2)a', (1/2)b' \in \mathbb{Z}$ and we obtain $\alpha \in \mathbb{Z} + \sqrt{d}\mathbb{Z}$.
Case 2: If $d \equiv 1 \pmod 4$, then $(a')^2 \equiv (b')^2 \pmod 4$. We can conclude that a', b' are either both odd or both even, otherwise we'd get $0 \equiv 1 \pmod 4$, and thus we can write $a' \equiv b' \pmod 2$. But this was exactly the condition appearing in the theorem.

■

Remark 3.1.14: Let K be a quadratic number field. Then we can reformulate the previous results as:

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

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

Remark 3.1.15: 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.

4 | Lecture 4 (Wednesday, January 27)

Today: the failure of unique factorization. Roughly corresponds to chapter 4: "Paradise Lost"!

Setup: K is a quadratic field, a degree 2 extension of $\mathbb{Q}$, which can be written as $K = \mathbb{Q}(\sqrt{d})$ with d squarefree. Last time, we completely described $\mathbb{Z}_K$ (the algebraic integers in K):

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

We saw that the second admitted a different description as $\left\{\frac{a+b\sqrt{d}}{2}\right\}$ where a, b are either both even or both odd. Note that we can do interesting arithmetic in $\mathbb{Z}_K$, but it's not necessarily well-behaved: $\mathbb{Z}_K$ is not always a UFD. 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 $\pmod 5$ 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.

4.1 Factorization Theory

[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.

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 4.1.1 (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 4.1.2 (Terminology for Cancellative Monoids)
A bunch of definitions: let M be a cancellative monoid.

- $\alpha \mid \beta$ 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.
- $\pi \in M$ 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 as a product of irreducibles (uniqueness up to order and associates).

Remark 4.1.3: 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 4.1.4
How do you show something is a UFD?

How does this proof go 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 4.1.5 (Atomic)
For M a cancellative monoid, M is **atomic** if every nonunit element of M is a product of irreducibles.

Proposition 4.1.6 *(?).*
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 (?).
Omitted – no new ideas when compared to proof of unique factorization in $\mathbb{Z}$.
■

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 4.1.7 (Reduced Monoid)
Define $M_{\text{red}} \coloneqq M/\sim$ 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 4.1.8 *(?):* This is supposed to look like $\mathbb{Z}_{\geq 0}$, where $-7 \in M \mapsto 7 \in M_{\text{red}}$.

Proposition 4.1.9 *(?).*
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.

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

Question 4.1.10
Why isn't $\mathbb{Z}[\sqrt{-5}]$ is UFD?

Answer 4.1.11
It doesn't have enough elements to make unique factorization work!

Example 4.1.12 *(?):* 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 4.1.13 *(?).*
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 (?).
Omitted, exercise in chasing definitions. The interesting part is that you can go backward!
■

Let $M_{\text{red}} \coloneqq \left(\mathbb{Z}[\sqrt{5}] \setminus \{0\}\right)_{\text{red}}$, 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 4.1.14 (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 4.1.15: 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 4.1.16 *(?).*
Let R be a commutative ring. Then

- $\cdot$ for ideals is commutative

- $\cdot$ 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, $\mathrm{Id}(R)$ is a monoid when R is a domain.

So instead of working in $\mathrm{Prin}(\mathbb{Z}[\sqrt{-5}])$, we'll work in $\mathrm{Id}(\mathbb{Z}[\sqrt{-5}])$.

Claim: 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.

5 Ch. 5: Euclidean Quadratic Fields (Thursday, January 28)

Remark 5.0.1: In a first algebra course, one process 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 5.0.2 (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 5.0.3 ***(Examples of Euclidean functions):***

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

Remark 5.0.4: 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 5.0.5
Which quadratic fields K have Z_K Euclidean?

Definition 5.0.6 (Euclidean and Norm-Euclidean Number Fields)
If K is a quadratic field, then

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

Proposition 5.0.7 ***(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 (?).
$\Longleftarrow$: 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 $\left|N(\frac{a}{b} - \gamma\right| < 1$. Multiplying both sides by $N(b)$ and using the fact that $N(\cdot), |\cdot|$ are multiplicative, we have

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

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

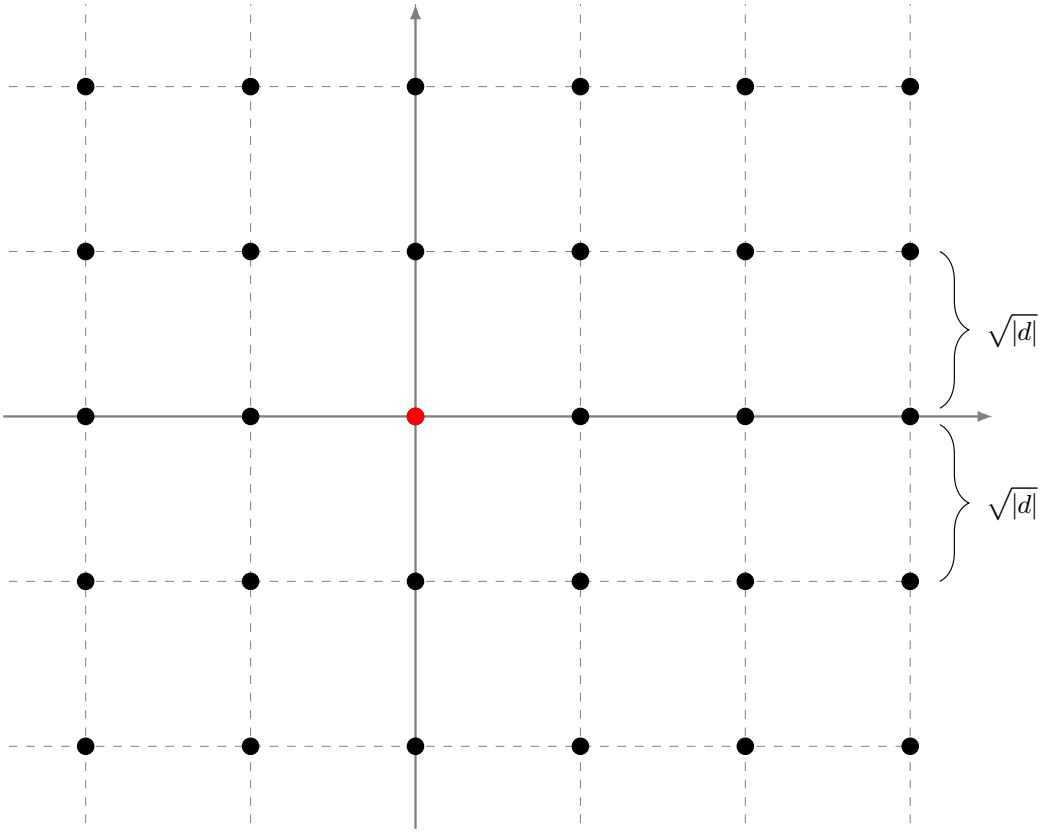
■

5.1 Norm-Euclidean Imaginary Quadratic Fields

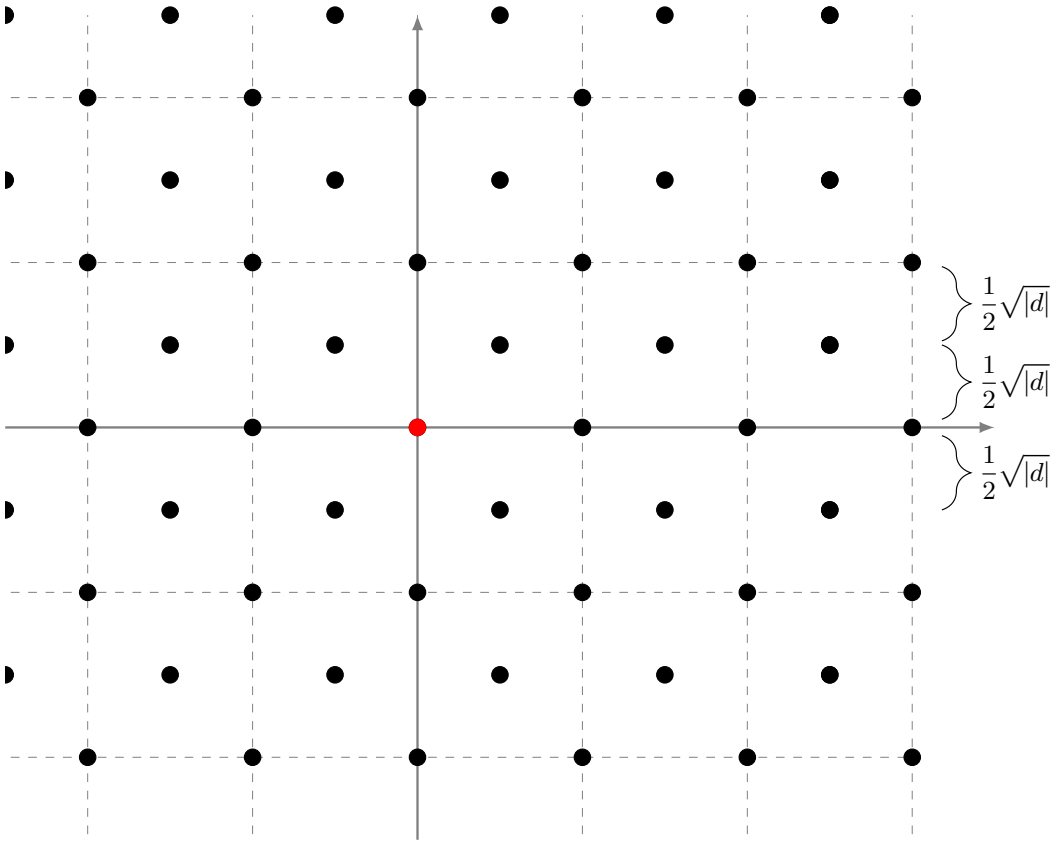
Remark 5.1.1: Suppose $K = \mathbb{Q}(\sqrt{d})$ with $d < 0$ squarefree, so we can write

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

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

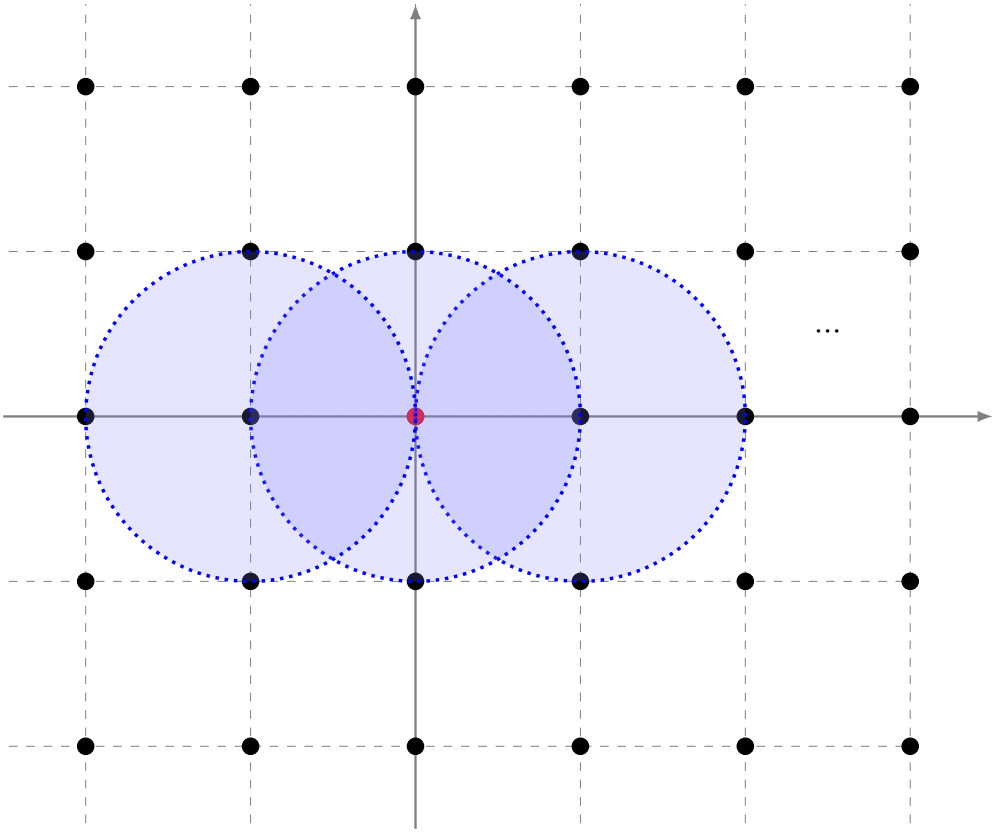


When $d \equiv 1 \pmod 4$, we have $\mathbb{Z}_k = \left\{ \frac{1}{2}(a + b\sqrt{d}) \;\middle|\; a, b, \in \mathbb{Z},\ a \equiv b \pmod 2 \right\}$. On the real axis, if $b = 0$ then a is an even integer and $\{(1/2)a\}$ is all integers. To get the remaining elements, we don't just shift up and down: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

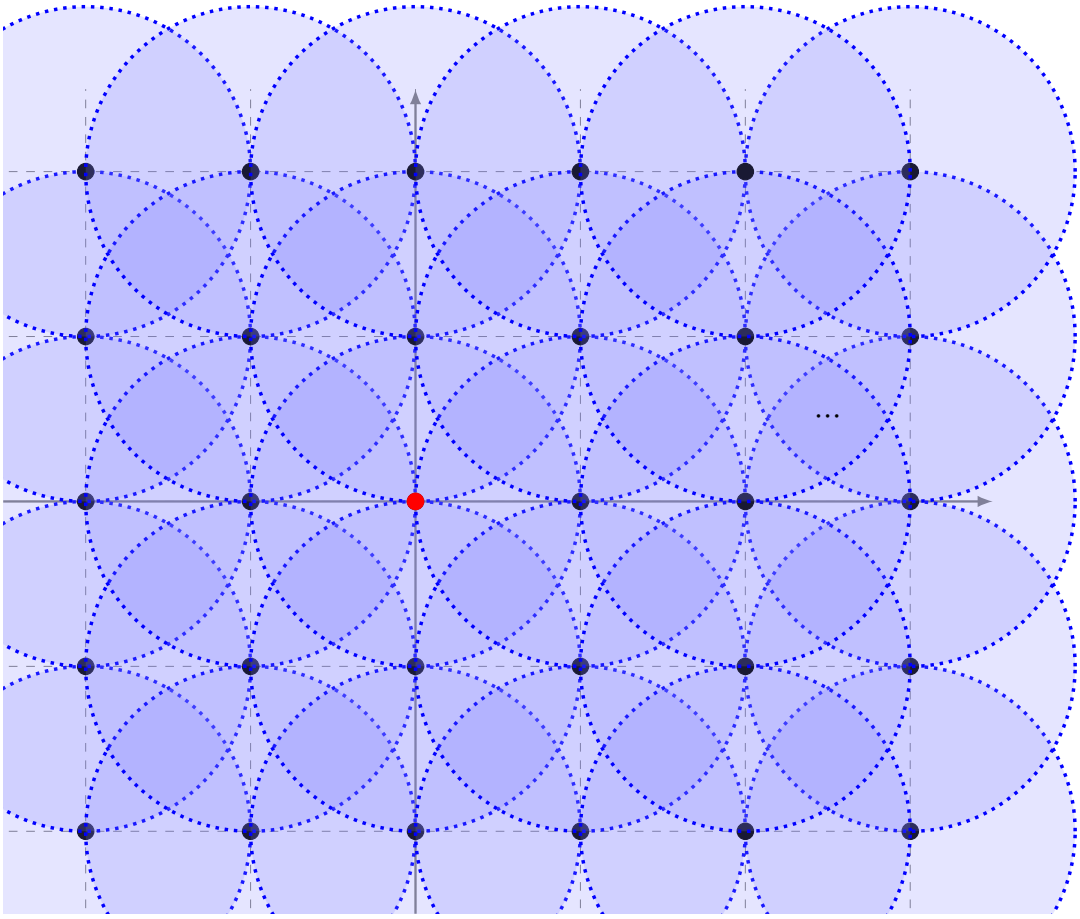


Now we can think of the criterion for an imaginary quadratic field to be norm-Euclidean: what does it mean to be within norm 1 of an element of $\mathbb{Z}_K$? If $z \in K$, we can write $N(z) = z\bar{z} = |z|^2$, and thus reformulate our criterion: K is norm-Euclidean if and only if for all $\beta \in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

Example 5.1.2 ***(?):*** $\mathbb{Q}(i)$ 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 5.1.3: 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 5.1.4 ***(?).***
K is norm-Euclidean if and only if $d \in \{-1, -2, -3, -7, -11\}$.

Corollary 5.1.5 ***(?).***
For these d, $\mathbb{Z}_K$ is a PID and thus a UFD.

Remark 5.1.6: So we've classified all norm-Euclidean imaginary quadratic fields. What about removing the word "norm"? We restricted to $|N(\cdot)|$ because there was a particularly nice geometric

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

Theorem 5.1.7 ***(Motzkin).***
For K an imaginary quadratic field, K is Euclidean if and only if $d \in \{-1, -2, -3, -7, -11\}$.

Remark 5.1.8: If $\mathbb{Z}_K$ were never a PID in these cases, we could immediately conclude it wasn't Euclidean either. But there are values of d not on this list for which $\mathbb{Z}_K$ is a PID, e.g. $d = -19$. Since $-19 \equiv 1 \pmod 4$, one can write $\mathbb{Z}_K = \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$, and by Motzkin's theorem this is a PID which is not a Euclidean domain.

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

Lemma 5.1.9 ***(?).***
Let K be an imaginary quadratic field, then $U(\mathbb{Z}_K) = \{\pm 1\}$ except if $d = -1, -3$.

Proof (of lemma (Important!)).
We know that the units u satisfy $|N(u)| = 1$, and for imaginary quadratic fields norms are non-negative, so we know $N(u) = 1$. What are the solutions this equation? Suppose $d = 2, 3 \pmod 4$, then we can write $\alpha = a + b\sqrt{d}$ with $a, b \in \mathbb{Z}$ and $1 = N\alpha = a^2 - db^2 = a^2 + |d|b^2$. If $|d| = 1$ then this will have four solutions: $(a, b) = (\pm 1, 0), (0, \pm 1)$. Otherwise if $|d| > 1$ then $b = 0$ and $a^2 = 1 \implies a = \pm 1$ and thus $\alpha = \pm 1$. So in this case, the only units are ± 1, unless $|d| = 1$. But the only negative squarefree integer of absolute value 1 is -1.
Suppose $d \equiv 1 \pmod 4$. In this case, we need

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

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

■

Remark 5.1.10: 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 5.1.11 ***(?).***
Let K be any quadratic field and $\alpha \in \mathbb{Z}_K$. Then $\#\mathbb{Z}_k / \langle \alpha \rangle = |N(\alpha)|$.

5.2 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 $\pmod{\beta}$, we obtain $\alpha = \rho \pmod{\beta}$, and hence $\#\mathbb{Z}_K / \langle \beta \rangle \leq 1 + \#U(\mathbb{Z}_K)$ where the 1 comes from the zero element and everything else in the quotient has a representative that is a unit. This is bounded above by 3 when $d \neq -1, -3$, which is one of the exclusions in the theorem.

■

Now we have $N(\beta) \leq 3$ and this can be solved – if d is large, these solutions are widely distributed. If $d = 2, 3 \pmod 4$ 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 $d \equiv 1 \pmod 4$, then $\beta = \dfrac{a + b\sqrt{d}}{2}$ where $a, b \in \mathbb{Z}$, $a \equiv b \pmod 2$. Then

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

Now considering that $-d \equiv 1 \pmod 4 \implies -d \in \{-3, -7, -11, \cdots\}$, 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 5.2.1: 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 5.2.2.
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 5.2.3.
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 5.2.4: 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.

ToDos

List of Todos

Definitions

Theorems

5

Exercises

Figures

List of Figures