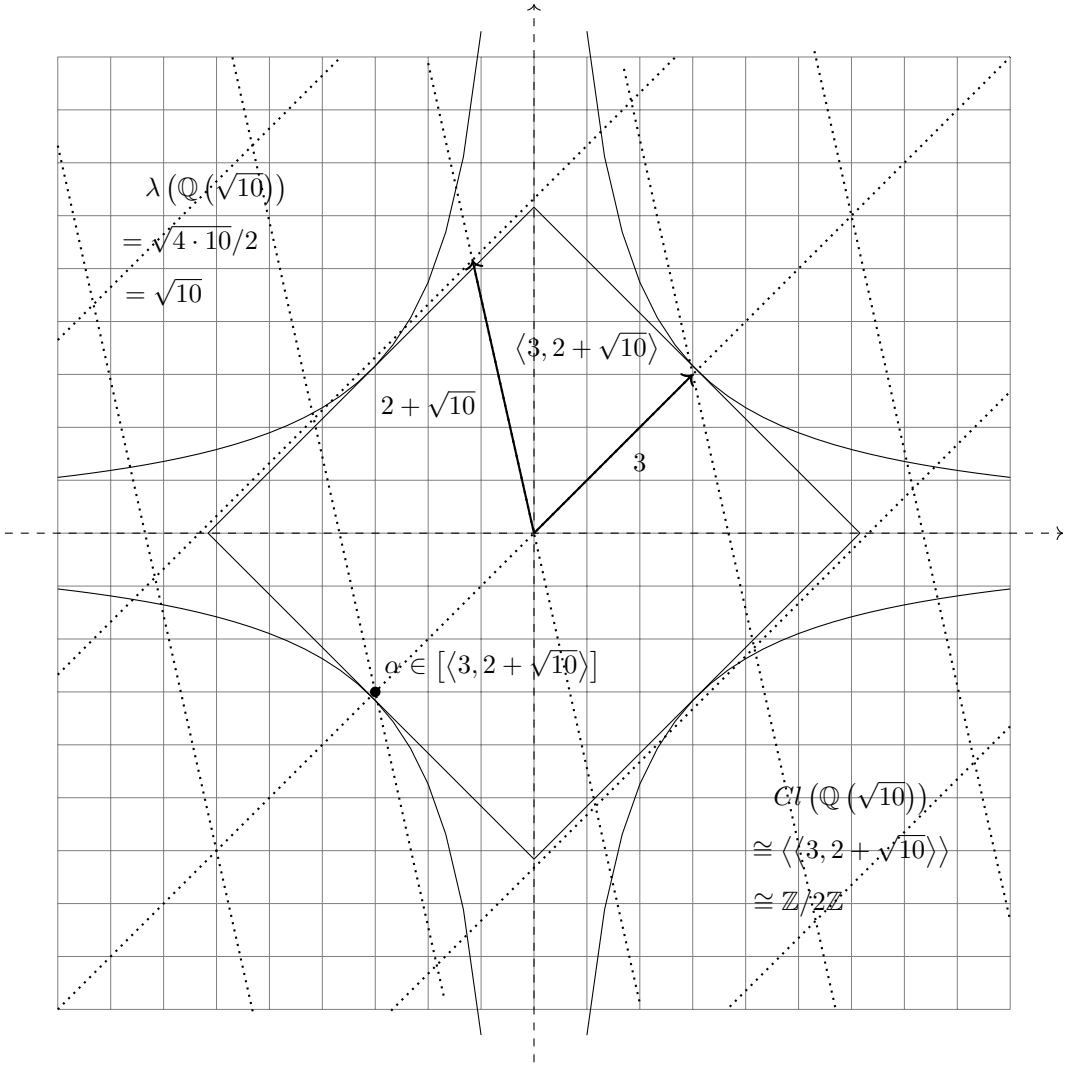
M3P15 Algebraic Number Theory

Lectured by Dr Ana Caraiani
Typed by David Kurniadi Angdinata

Spring 2019



Syllabus

Rings. Unique factorisation domains. Principal ideal domains. Euclidean domains. Gaussian integers. Eisenstein integers. Number fields. Structure theorem for finitely generated abelian groups. Integral closure. Norms. Traces. Discriminants. Ring of integers. Dedekind domains. Unique factorisation of Dedekind domains. Splitting of prime ideals in quadratic fields. Class groups. Finiteness of class groups. Groups of units.

Contents

0 Motivation and overview

Lecture 1
Friday
11/01/19

The goal of this course will be to introduce algebraic number theory, specifically the arithmetic of finite extensions of $\mathbb{Q}$, with an emphasis on quadratic extensions as a rich source of examples. We will start with some motivation and then review the necessary background from ring theory. We will then discuss unique factorisation domains, principal ideal domains and Euclidean domains. These tools will be enough to study Gaussian integers and Eisenstein integers in-depth. To understand more general number fields, we will need some more commutative algebra. We will discuss the structure theorem for finitely generated abelian groups and the notion of integral closure. We will also introduce norms, traces, and discriminants. We will show that rings of integers in number fields are Dedekind domains and we will state and prove unique factorisation for Dedekind domains. We will then study the splitting of prime ideals in quadratic fields. We will define the class group and prove that it is always finite. We will end with a discussion of the groups of units. For quadratic fields, a good reference with many examples is 2. Another reference we will use is 1.

1. P Samuel, Algebraic theory of numbers, 1970
2. M Trifkovic, Algebraic theory of quadratic numbers, 2013

Algebraic number theory developed from

- trying to generalise known properties of integers, such as unique factorisation, to finite extensions of $\mathbb{Q}$,
- trying to solve Diophantine equations in a systematic way. For example, Fermat's equation

$$x^n + y^n = z^n, \qquad n \geq 2, \qquad x, y, z \in \mathbb{Z}.$$

Let $n \in \mathbb{Z}_{\geq 0}$. A question is when can we write n as

$$n = a^2 + b^2, \qquad a, b \in \mathbb{Z}?$$

Some observations.

- If $n = a_1^2 + b_1^2$, $m = a_2^2 + b_2^2$,

$$m \cdot n = (a_1 a_2 + b_1 b_2)^2 + (a_1 b_2 - a_2 b_1)^2 .$$

- Every $n \geq 0$ can be written as a product

$$n = p_1^{k_1} \dots p_r^{k_r}, \qquad k_i \in \mathbb{Z}_{\geq 1},$$

  where p_i are prime numbers. Irreducibles are such that only divisors are 1 and p_i. Primes are such that $p_i \mid mn$ implies that $p_i \mid m$ or $p_i \mid n$. Irreducibles and primes are equivalent in $\mathbb{Z}$.

- Only care about p_i with odd exponent.

When can we write

$$p = a^2 + b^2, \qquad a, b \in \mathbb{Z},$$

where p is prime? An observation is that

$$p = 2, 5, 13, 17, 29, 37, \dots$$

is ok, and

$$p \neq 3, 7, 11, 19, 23, \dots$$

is not ok. A conjecture is if $p \equiv 3 \mod 4$, then $p \neq a^2 + b^2$, otherwise this is ok.

Theorem 0.0.1. *If $p \equiv 3 \mod 4$ then $p \neq a^2 + b^2$.*

Proof. $a^2 + b^2 \equiv 0 \mod p$ and $a, b \not\equiv 0 \mod p$ if and only if

$$\left(\frac{a}{b}\right)^2 \equiv -1 \mod p,$$

if and only if $\left(\frac{-1}{p}\right) = 1$, so $p \equiv 3 \mod 4$. □

Remark. Proof tells us that $n \neq a^2 + b^2$ whenever n has a prime factor $p_i \equiv 3 \mod 4$ with odd exponent k_i for $i = 1, \ldots, r$. If every $p \equiv 1 \mod 4$ is of the form $p = a^2 + b^2$, then we understand the general case,

$$n = a^2 + b^2 \qquad \iff \qquad \forall p_i \mid n,\ p_i \equiv 3 \mod 4,\ k_i \in 2\mathbb{Z}.$$

Theorem 0.0.2. *If $p \equiv 1 \mod 4$ then*

$$p = a^2 + b^2, \qquad a, b \in \mathbb{Z}.$$

Factorisation in $\mathbb{Z}[i]$ for $i^2 = 1$ is $p = a^2 + b^2 = (a + bi)(a - bi)$ for $a, b \in \mathbb{Z}$.

$$\mathbb{Z}[i] = \mathbb{Z} \oplus \mathbb{Z}i = \{a + bi \mid a, b \in \mathbb{Z}\}$$

is the subring of **Gaussian integers** in $\mathbb{Q}(i)/\mathbb{Q}$, an extension $\mathbb{Q}[x]/\left(x^2 + 1\right)$ of $\mathbb{Q}$ of degree two, a quadratic field. We will understand prime factorisation in $\mathbb{Z}[i]$, and in more general finite extensions of $\mathbb{Q}$.

Theorem 0.0.3 (Unique factorisation in $\mathbb{Z}$)**.** *Any $n \in \mathbb{Z} \setminus \{0, \pm 1\}$ can be written uniquely as a product of primes, up to permuting the prime factors or changing their signs.*

Proposition 0.0.4 (Division algorithm)**.** *Given $a, b \in \mathbb{Z}$, for $b \neq 0$, there exist $q, r \in \mathbb{Z}$ such that $a = qb + r$ such that $0 \leq r < |b|$.*

Proposition 0.0.5 (Euclid's algorithm)**.** *Let $a, b \in \mathbb{Z}$ and $ab \neq 0$. There exist a greatest common divisor $\gcd(a, b) \mid a$ and $\gcd(a, b) \mid b$, and $r, s \in \mathbb{Z}$ such that $ar + bs = \gcd(a, b)$.*

Proof. Consider $I = \{ma + nb \mid m, n \in \mathbb{Z}\}$. $\gcd(a, b)$ will be the smallest positive element of I. □

Let $I \subseteq \mathbb{Z}$ be the ideal of $\mathbb{Z}$ generated by a, b. Proof of Euclid's algorithm shows I is generated by $\gcd(a, b)$. In fact, every ideal of $\mathbb{Z}$ is generated by one element, that is it is **principal**.

Proposition 0.0.6 (Euclid's lemma)**.** *If $p \in \mathbb{Z}$ is prime, then $p \mid ab$ for $a, b \in \mathbb{Z}$ implies that $p \mid a$ or $p \mid b$.*

Proof of Theorem 0.0.3.

- All $n \in \mathbb{Z}$ has a prime divisor by taking $p \in \mathbb{Z}_{\geq 2}$, the smallest divisor of n.
- Prime factorisation exists. Let n be the smallest integer which does not have one.
- Uniqueness. $n = p_2 \ldots p_n = q_2 \ldots q_?$ Euclid's lemma implies that $p_1 \mid q_1$, up to reordering, so $p_1 = \pm q_1$, and continue.

□

1 Rings

Lecture 2
Monday
14/01/19

1.1 Commutative rings

Definition 1.1.1. A **ring** is commutative and with unity. A **unit** in a ring R is an element $a \in R$ such that there exists $b \in R$ with $a \cdot b = 1$.

- The set of units forms a group under multiplication, denoted by $R^\times$.
- If $b \in R$ exists such that $ab = 1$ then b is unique.

If $R \setminus \{0\} = R^\times$, then R is a **field**.

Example.

- $\mathbb{Z}^\times = \{\pm 1\}$.
- $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$.
- $\mathbb{Z}\left[\sqrt{2}\right]^\times \supseteq \{\pm 1, \epsilon^n\}$, where $\epsilon = 1 + \sqrt{2}$.

$$\mathbb{Z}\left[\sqrt{2}\right] = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\right\}.$$

$\left(1 + \sqrt{2}\right)\left(-1 + \sqrt{2}\right) = 2 - 1 = 1$. $\epsilon^n = \epsilon^m$ for $n, m \in \mathbb{Z}$ and $n \geq m$ if and only if $\epsilon^{n-m} = 1$.

Definition 1.1.2. Let R be a ring. An **ideal** $I \subseteq R$ is an additive subgroup, so $x, y \in I$ implies that $x + y \in I$, which absorbs multiplication. If $x \in I$ and $a \in R$ then $ax \in I$.

Fact. If $\phi : R \to S$ a ring homomorphism then $Ker\,(\phi) \subseteq R$ is an ideal. Conversely, if $I \subseteq R$ is an ideal, can define

$$\frac{R}{I} = \frac{R}{\sim}$$

as the set of equivalence classes modulo I, that is $a + I$ for $a \in R$, via $a \sim b$ for $a, b \in R$ if $a - b \in I$.

Proposition 1.1.3. *R/I has ring structure induced by*

$$(a + I) + (b + I) = (a + b) + I,$$
$$(a + I) \cdot (b + I) = (a \cdot b) + I,$$

and a canonical surjective ring homomorphism

$$\begin{array}{ccc} R & \longrightarrow & \dfrac{R}{I} \\ a & \longmapsto & a + I \end{array}.$$

Check that $a - a' \in I$ and $b - b' \in I$ implies that

$$(a + b) - (a' + b') = (a - a') + (b - b') \in I,$$

$$ab - a'b' = a\,(b - b') + b'\,(a - a') \in I.$$

Theorem 1.1.4 (First isomorphism theorem for rings)**.** *Let $\phi : R \to S$ be a ring homomorphism. Then we have a canonical ring isomorphism*

$$\begin{array}{ccc} \dfrac{R}{Ker\,(\phi)} & \longrightarrow & \phi\,(R) \subset S \\ r + Ker\,(\phi) & \longmapsto & \phi\,(r) \end{array}, \qquad r \in R.$$

Example. Let $R = \mathbb{Z}\left[\sqrt{5}\right] = \left\{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\right\}$.

- Let I be the ideal $11\mathbb{Z} \oplus \left(4 - \sqrt{5}\right)\mathbb{Z}$. A question is what is R/I? Claim that

$$\frac{R}{I} \cong \frac{\mathbb{Z}}{11\mathbb{Z}} = \mathbb{F}_{11},$$

the finite field with 11 elements. Write down $\phi : R \twoheadrightarrow \mathbb{Z}/11\mathbb{Z}$ such that $Ker\,(\phi) = I$, then result follows from Theorem 1.1.4. Such a ϕ would have to satisfy

$$\phi\left(4 - \sqrt{5}\right) = 0, \qquad \phi\,(11) = 0.$$

$\phi\left(\sqrt{5}\right) = \phi\,(4) = 4 \mod 11$.

$$\begin{array}{rccc} \phi & : & \mathbb{Z} \oplus \mathbb{Z}\left[\sqrt{5}\right] & \longrightarrow & \dfrac{\mathbb{Z}}{11\mathbb{Z}} \\ & & \sqrt{5} & \longmapsto & 4 \end{array}.$$

Still have to check that

$$16 = \phi\,(5)^2 = \phi\left(\sqrt{5}^2\right) = \phi\,(5) = 5 \mod 11.$$

Ok because $16 \equiv 5 \mod 11$.

- What can we say about R/J, where

$$J = \left\langle 9, 4 - \sqrt{5} \right\rangle = 9R + \left(4 - \sqrt{5}\right) R$$

is generated over R? R/J is trivial and $\left\langle 9, 4 - \sqrt{5} \right\rangle = R$.

Definition 1.1.5.

- If I, J are ideals in a ring R, we say that I **divides** J if $J \subseteq I$.
- We can form ideals

$$\begin{aligned} I \cap J &= \{r \mid r \in I,\ r \in J\}, \\ I + J &= \{r + s \mid r \in I,\ s \in J\}, \\ I \cdot J &= \left\{ \sum_{i=1}^{n} r_i s_i \;\middle|\; r_i \in I,\ s_i \in J,\ i = 1, \ldots, n \right\}. \end{aligned}$$

- I, J are said to be **relatively prime** if $I + J = R$.

Theorem 1.1.6 (Chinese remainder theorem)**.** *Let I, J be two relatively prime ideals of R. Then*

$$\frac{R}{IJ} \cong \frac{R}{I} \times \frac{R}{J}.$$

Remark. If $R = \mathbb{Z}$, all ideals are principal and Theorem 1.1.6 specialises to usual Chinese remainder theorem.

Proof. Find surjective ring homomorphism

$$\begin{array}{rcc} R & \longrightarrow & \dfrac{R}{I} \times \dfrac{R}{J} \\ r & \longmapsto & (r \mod I, r \mod J) \end{array},$$

with kernel $I \cdot J$. □

Definition 1.1.7. A ring R is **Noetherian** if it satisfies the **ascending chain condition** on ideals, that is any infinite sequence of ideals

$$I_1 \subseteq I_2 \subseteq \ldots$$

stabilises.

Example. $\mathbb{Z}$ and $\mathbb{Z}[x]$ are Noetherian. $\mathbb{Z}[x_1, x_2, \ldots]$ is not Noetherian.

1.2 Integral domains

Lecture 3
Tuesday
15/01/19

Definition 1.2.1. A ring R is an **integral domain (ID)** if $ab = 0$ for $a, b \in R$ implies that $a = 0$ or $b = 0$.

Example.

- $\mathbb{Z}$ and $\mathbb{Z}\left[\sqrt{5}\right]$ are IDs.
- $\mathbb{Z}\left[\sqrt{5}\right] / \left\langle 4 - \sqrt{5} \right\rangle = \mathbb{Z}/11\mathbb{Z} = \mathbb{F}_{11}$, since $I = 11\mathbb{Z} \oplus \left(4 - \sqrt{5}\right)\mathbb{Z} = \left(4 - \sqrt{5}\right) \cdot \mathbb{Z}\left[\sqrt{5}\right]$, because $11 = \left(4 - \sqrt{5}\right)\left(4 + \sqrt{5}\right) = 16 - 5$. Thus

$$\frac{\mathbb{Z}\left[\sqrt{5}\right]}{\langle 11 \rangle} \cong \frac{\mathbb{Z}\left[\sqrt{5}\right]}{\left\langle 4 - \sqrt{5} \right\rangle} \times \frac{\mathbb{Z}\left[\sqrt{5}\right]}{\left\langle 4 - \sqrt{5} \right\rangle} = \mathbb{F}_{11} \times \mathbb{F}_{11},$$

  which is no longer an ID.

Remark. An ideal $\mathfrak{p} \subsetneq R$ is **prime** if $ab \in \mathfrak{p}$ implies that $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. $(a + \mathfrak{p})(b + \mathfrak{p}) = 0$ in $R/\mathfrak{p}$ implies that $a + \mathfrak{p} = 0$, that is $a \in \mathfrak{p}$, or $b + \mathfrak{p} = 0$, that is $b \in \mathfrak{p}$. This is equivalent to asking that $R/\mathfrak{p}$ is an ID.

IDs are well-suited to studying divisibility. $a \mid b$ in R if there exists c such that $ac = b$.

Lemma 1.2.2. *Let R be an ID. If $a \mid b$ and $b \mid a$, then there exist $c, d \in R^\times$ such that $ac = b$ and $bd = a$.*

Proof. $a \mid b$ implies that there exists c such that $ac = b$ and $b \mid a$ implies that there exists d such that $bd = a$ for $c, d \in R$. Then $acd = bd = a$ if and only if $a(cd - 1) = 0$. R is an ID, so $a = 0$ or $cd = 1$. If $a = 0$, then $b = 0$, so $c = d = 1$. □

Definition 1.2.3. Let R be an ID.

- We say $a \in R$ is **irreducible** if
  - a is not a unit, and
  - $a = bc$ for $b, c \in R$ implies that either b or c is in $R^\times$.
- We say $a \in R$ is **prime** if
  - a is not a unit, and
  - $a \mid bc$ implies that $a \mid b$ or $a \mid c$.

$\langle 0 \rangle$ is prime if and only if R is an ID.

Remark. Over $\mathbb{Z}$, these two notions are equivalent, but not in general. If R is an ID and $a \in R \setminus \{0\}$ is prime, then a is irreducible. Let $b, c \in R$ be such that $a = bc$, so $b \mid a$ and $c \mid a$. Because a is prime, $a = bc$ implies that $a \mid b$ or $a \mid c$. Say $a \mid b$ happens. There exists $d \in R^\times$ such that $a = bd$. $a = bc$, so $b(d - c) = 0$. $b \neq 0$, because $a \neq 0$, so $d = c$, that is c is a unit.

Remark. If $a \in R \setminus \{0\}$ is irreducible, a does not have to be prime.

Example. $\mathbb{Z}\left[\sqrt{-5}\right] = \left\{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\right\}$ is the ring of integers of $\mathbb{Q}\left(\sqrt{-5}\right)$, an extension of $\mathbb{Q}$ of degree two, a subring of $\mathbb{C}$. $6 = 2 \cdot 3 = \left(1 + \sqrt{-5}\right) \cdot \left(1 - \sqrt{-5}\right)$. Claim that these are two factorisations of 6 into irreducible elements.

- 2 is irreducible. Why? Assume $2 = \alpha\beta$ for $\alpha, \beta \in \mathbb{Z}\left[\sqrt{-5}\right]$. The goal is that α or β is a unit. We will use

$$\begin{array}{rccc} N & : & \mathbb{Z}\left[\sqrt{-5}\right] & \longrightarrow & \mathbb{Z}_{\geq 0} \\ & & a + \sqrt{-5}b & \longmapsto & \left(a + \sqrt{-5}b\right)\left(a - \sqrt{-5}b\right) = a^2 + 5b^2 \end{array},$$

  which is multiplicative. $N(2) = 4 = N(\alpha)N(\beta)$. If $N(\alpha) = 1$, then α is a unit. $N(\alpha) = N(\beta) = 2$ implies that $a^2 + 5b^2 = 2$, which has no solutions, a contradiction.
- 2 and $1 + \sqrt{-5}$ do not differ by units, since $N(2) = 4$ and $N\left(1 + \sqrt{-5}\right) = 6$.

Upshot is that 2 is irreducible in $\mathbb{Z}\left[\sqrt{-5}\right]$ but not prime.

1.3 Unique factorisation domains

Let R be an ID. We define an equivalence relation $\sim$ on R by $a \sim b$ if $a \mid b$ and $b \mid a$, or there exist $c, d \in R^\times$ such that $a = bc$ and $b = da$.

Definition 1.3.1. An ID R has **unique factorisation** if for all $a \in R \setminus \{0\}$ there is a factorisation $a = u \cdot p_1 \cdot \cdots \cdot p_r$, where $u \in R^\times$ and the p_i are irreducible. This is unique in the sense that, if there exists another factorisation $v \cdot q_1 \cdot \cdots \cdot q_s$, where $v \in R^\times$ and the q_i are irreducible, then $r = s$, and up to reordering $p_i \sim q_i$, for $i = 1, \ldots, r = s$. An ID with this property is called an **unique factorisation domain (UFD)**.

Example. $\mathbb{Z}$, but not $\mathbb{Z}\left[\sqrt{-5}\right]$.

Lemma 1.3.2. *If R is a UFD, then $p \in R \setminus \{0\}$ is irreducible implies that p is prime.*

Proof. Exercise. □

Theorem 1.3.3. *Let R be an ID. The following conditions are equivalent.*

- *R is a UFD.*
- *R satisfies ascending chain condition for principal ideals, that is every infinite sequence*

$$\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \ldots$$

stabilises after finitely many steps, and every irreducible in R is prime.

If R is a UFD, can define $d(a) \in \mathbb{Z}_{\geq 0}$ as the number of irreducible factorisations of a. $d(a) = 0$ if and only if $a \in R^\times$ is a unit.

Lemma 1.3.4. *Let R be a UFD and $a \mid b$ for $a, b \in R$. Then*

- *$d(a) \leq d(b)$, and*
- *$b \mid a$ if and only if $d(a) = d(b)$.*

Lecture 4
Friday
18/01/19

Proof. Let $a = u \cdot p_1 \cdot \cdots \cdot p_{d(a)}$ and $b = v \cdot q_1 \cdot \cdots \cdot q_{d(b)}$. $a \mid b$, so $b = a \cdot c$ for $c \in R \setminus \{0\}$. Let $c = w \cdot r_1 \cdot \cdots \cdot r_{d(c)}$.

$$v \cdot q_1 \cdot \cdots \cdot q_{d(b)} = u \cdot w \cdot p_1 \cdot \cdots \cdot p_{d(a)} \cdot r_1 \cdot \cdots \cdot r_{d(c)}.$$

Uniqueness of factorisation implies that $d(b) = d(a) + d(c)$, so $d(b) \geq d(a)$. Equality if and only if $d(c) = 0$ if and only if c is a unit, if and only if $b \mid a$. □

Proof of Theorem 1.3.3.

$\Longrightarrow$ Assume R is a UFD. Irreducibles are prime. Let

$$\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \ldots.$$

Then $\cdots \mid a_2 \mid a_1$, so $d(a_1) \geq d(a_2) \geq \cdots \geq 0$. This sequence stabilises after finitely many steps. There exists n such that $d(a_n) = d(a_{n+1}) = \ldots$, so $a_n \sim a_{n+1} \sim \ldots$, so $\langle a_n \rangle = \langle a_{n+1} \rangle = \ldots$.

$\Longleftarrow$ For all $a \in R \setminus \{0\}$, claim that a has a factorisation into irreducibles. If $a_1 = a$, irreducible. Otherwise $a = b \cdot c$ for $b, c \in R \setminus \{0\}$ not units. If both irreducible, done. If not, say b not irreducible, $a_2 = b$. $a = b \cdot c$ for c not a unit, so $\langle a \rangle \subsetneq \langle b \rangle$. Redoing the process here,

$$\langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \ldots.$$

By ascending chain condition, this process terminates, getting a contradiction, so a has factorisation into irreducibles. The factorisation of a is unique, up to units and reordering. Let

$$a = u \cdot p_1 \cdot \cdots \cdot p_r = v \cdot q_1 \cdot \cdots \cdot q_s.$$

p_1 is irreducible, so p_1 is prime, so $p_1 \mid q_i$ for some i, where q_i is irreducible, so $p_1 \sim q_i$. Cancel out p_1, q_i and repeat.

□

Remark. $\mathbb{Z}\left[\sqrt{-5}\right]$ is not a UFD because 2 is irreducible but not prime.

1.4 Principal ideal domains

Definition 1.4.1. An ID R is a **principal ideal domain (PID)** if every ideal of R is principal.

Example.

- Fields.
- $\mathbb{Z}$ follows from Euclid's algorithm.

Theorem 1.4.2. *A PID R is a UFD.*

Proof. Check two characterising properties.

- Ascending chain condition. Let
$$\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \dots .$$
Consider
$$I = \bigcup_{n=1}^{\infty} \langle a_n \rangle .$$
Claim that I is an ideal of R. Say $x \in I$ and $r \in R$. Want $rx \in I$. There exists $n \in \mathbb{Z}_{\geq 1}$ such that $x \in \langle a_n \rangle$, so $rx \in \langle a_n \rangle$ and $rx \in I$. Say $x, y \in I$. Then $x \in \langle a_n \rangle$ for $n \in \mathbb{Z}_{\geq 1}$ and $y \in \langle a_m \rangle$ for $m \in \mathbb{Z}_{\geq 1}$. If $m \geq n$ then $x \in \langle a_m \rangle$, so $x + y \in \langle a_m \rangle$, so $x + y \in I$. Otherwise $y \in \langle a_n \rangle$, so $x + y \in \langle a_n \rangle$, so $x + y \in I$. Hence $I \subseteq R$ is an ideal, so I is principal, that is there exists $a \in R$ such that $I = \langle a \rangle$. There exists $n \in \mathbb{Z}_{\geq 1}$ such that $a \in \langle a_n \rangle$. Have inclusions
$$\langle a \rangle \subseteq \langle a_n \rangle \subseteq \langle a_m \rangle \subseteq \langle a \rangle .$$
All inclusions are equalities, so $\langle a_m \rangle = \langle a_n \rangle$ for all $m \geq n$.
- Exercise: irreducibles are prime.

□

Remark.

- $\mathbb{Z}\left[\sqrt{-5}\right]$ is not a PID. Follows from Theorem 1.4.2 and failure of unique factorisation. $\left\langle 2, 1 + \sqrt{-5} \right\rangle$ is not a principal ideal. (Exercise: check this)
- A UFD that is not a PID. $\mathbb{Q}[x, y]$ is a UFD but $\langle x, y \rangle$ is not principal. $\mathbb{Z}[x]$ is a UFD but $\langle 2, x \rangle$ is not principal.

1.5 Euclidean domains

Definition 1.5.1.

- A **Euclidean norm** on an ID R is a function $\phi : R \setminus \{0\} \to \mathbb{Z}_{\geq 1}$ such that for all $a, b \in R \setminus \{0\}$ there exist $q, r \in R$ such that $a = qb + r$ and
  - either $r = 0$,
  - or $\phi(r) < \phi(b)$.
- An ID that admits a Euclidean norm is called a **Euclidean domain**.

Sometimes, add condition

$$\phi(ab) \geq \phi(b). \tag{1}$$

If ϕ is a Euclidean norm as in definition, can use ϕ to construct ψ Euclidean norm satisfying (1).

Theorem 1.5.2. *If R is a Euclidean domain, then R is a PID, so R is a UFD.*

Lecture 5
Monday
21/01/19

Proof. Let $I \subseteq R$ be an ideal. Assume $I \neq \langle 0 \rangle$. The goal is that I is generated by one element $a \in R \setminus \{0\}$. Let $0 \neq a \in I$ be an element such that $\phi(a)$ is minimal along the values of ϕ on I. $\langle a \rangle \subseteq I$. We will show that we have an equality. Let $b \in I \setminus \langle a \rangle$. Applying property of ϕ to b and a, $b = qa + r$. $r \neq 0$, otherwise $a \mid b$, so $b \in \langle a \rangle$. $r = b - qa \in I$ but $\phi(r) < \phi(a)$, a contradiction. □

Example.

- $\mathbb{Z}$, with Euclidean norm
$$\begin{array}{ccc} \mathbb{Z} \setminus \{0\} & \longrightarrow & \mathbb{Z}_{\geq 1} \\ n & \longmapsto & |n| \end{array}.$$
- Gaussian integers. $\mathbb{Z}[i]$, with Euclidean norm given by restriction to $\mathbb{Z}[i] \subset \mathbb{C}$ of complex absolute value
$$\begin{array}{ccc} \mathbb{Z}^2 \setminus \{(0,0)\} & \longrightarrow & \mathbb{Z}_{\geq 1} \\ a + ib & \longmapsto & (a+ib)(a-ib) = a^2 + b^2 \end{array}.$$
- Eisenstein integers. Let $1 \neq \omega \in \mathbb{C}$ be a primitive cube root of unity, so $\omega = \frac{-1+\sqrt{-3}}{2}$. The subring
$$\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$$
is Euclidean, with Euclidean norm given by
$$\begin{array}{ccc} \mathbb{Z}^2 \setminus \{(0,0)\} & \longrightarrow & \mathbb{Z}_{\geq 1} \\ a + b\omega & \longmapsto & a^2 - ab + b^2 \end{array}.$$

Remark.

- In all these examples, norm is multiplicative. This does not have to hold true, such as $\mathbb{Q}[x]$, with Euclidean norm $f \mapsto \deg(f)$.
- There are PIDs that do not admit a Euclidean norm, such as $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$.

1.6 Summary of rings

$$\{\text{commutative rings}\} \supsetneq \{\text{IDs}\} \supsetneq \{\text{UFDs}\} \supsetneq \{\text{PIDs}\} \supsetneq \{\text{Euclidean domains}\}.$$

- $\mathbb{Q}[x, y]/xy, \mathbb{Z}/6\mathbb{Z}, \mathbb{F}_3[x]/x^2$ are commutative rings but not IDs.
- $\mathbb{Z}\left[\sqrt{-5}\right]$ is an ID but not a UFD, since $6 = 2 \cdot 3 = \left(1 + \sqrt{-5}\right) \cdot \left(1 - \sqrt{-5}\right)$.
- $\mathbb{Z}[x]$ is a UFD but not a PID, since $\langle 2, x \rangle$ is not principal.
- $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ is a PID but not a Euclidean domain.

1.7 Gaussian integers

The **Gaussian integers** are

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subset \mathbb{Q}(i) \subset \mathbb{C}.$$

We will crucially use the norm

$$\begin{array}{rccc} N & : & \mathbb{Z}[i] & \longrightarrow & \mathbb{Z}_{\geq 0} \\ & & a + bi & \longmapsto & (a+bi)(a-bi) = a^2 + b^2 \end{array},$$

which is not the same as the Euclidean norm.

Note. This is multiplicative.

Proposition 1.7.1. *If $u \in \mathbb{Z}[i]^\times$ then $N(u) = 1$.*

Proof. $N|_{\mathbb{Z}[i]\setminus\{0\}}(u) \geq 1$, N is multiplicative, and $N(1) = 1$. $uv = 1$ implies that $N(u) \cdot N(v) = 1$, so $N(u) \geq 1$ and $N(v) \geq 1$, so $N(u) = N(v) = 1$. □

$N(u) = u \cdot \overline{u} = 1$. $u = a + bi \in \mathbb{Z}[i]^\times$ if and only if $a^2 + b^2 = 1$, if and only if $(a, b) = (\pm 1, 0)$, that is $u = \pm 1$, or $(a, b) = (0, \pm 1)$, that is $u = \pm i$.

Remark. $\mathbb{Z}[i]^\times \cong (\mathbb{Z}/4\mathbb{Z}, +)$ as groups.

Proposition 1.7.2. *Given $\alpha, \beta \in \mathbb{Z}[i]$, for $\beta \neq 0$, there exist $\kappa, \lambda \in \mathbb{Z}[i]$ such that $\alpha = \kappa\beta + \lambda$ and either $\lambda = 0$ or $N(\lambda) < N(\beta)$, so N is Euclidean and $\mathbb{Z}[i]$ has unique factorisation.*

Proof. $\mathbb{Z}[i] \subset \mathbb{C}$ is a lattice. $\alpha = \kappa\beta + \lambda$ if and only if $\alpha/\beta = \kappa + \lambda/\beta$ in $\mathbb{C}$ for $\beta \neq 0$. $\alpha/\beta \in \mathbb{C}$ lands inside one of the unit squares in the lattice spanned by $\mathbb{Z}[i]$. Open unit discs centred at the vertices of the unit square cover the entire square. α/β is in the unit disc centred at κ if and only if $N(\alpha/\beta - \kappa) < 1$. Let $\lambda/\beta = \alpha/\beta - \kappa$ and $N(\lambda/\beta) < 1$ if and only if $N(\lambda) < N(\beta)$. Choose κ to be one vertex such that α/β is in the open unit disc centred at κ. $\lambda = \beta(\alpha/\beta - \kappa)$, so $N(\lambda) < N(\beta)$. □

Lemma 1.7.3 (Special case of quadratic reciprocity)**.** *If p is an odd prime, then -1 is a square mod p if and only if $p \equiv 1 \mod 4$.*

The following is the decomposition of primes in $\mathbb{Z}[i]$.

- $2 = (1+i)(1-i) = (-i)(1+i)^2$. Notice that $i(1+i) = i - 1 = -(1-i)$. Up to units in $\mathbb{Z}[i]^\times$ these prime factors are the same. This is a **ramified** prime.
- $p \equiv 1 \mod 4$. $p = (a+bi)(a-bi)$, which are distinct primes in $\mathbb{Z}[i]$. This is a **split** prime.
- $p \equiv 3 \mod 4$. p stays prime. If not, $a + bi \mid p$, so $N(a+bi) \mid N(p) = p^2$, so $N(a+bi) = p = a^2 + b^2$, which cannot happen. This is an **inert** prime.

Lecture 6
Tuesday
22/01/19

Quadratic reciprocity implies that there exists $n \in \mathbb{Z}$ such that $p \mid n^2 + 1 = (n+i)(n-i)$. Assume p stays prime, or irreducible, in $\mathbb{Z}[i]$, so $p \mid n + i$ or $p \mid n - i$. By conjugating, we see $p \mid n + i$ if and only if $p \mid n - i$, so $p \mid (n+i) - (n-i) = 2i$. Taking N, see $N(p) = p^2 \nmid 4 = N(2i)$, a contradiction.

Theorem 1.7.4. *$n \in \mathbb{Z}_{>0}$ is of the form $n = a^2 + b^2$ for $a, b \in \mathbb{Z}$ if and only if for all $p \mid n$ such that $p \equiv 3 \mod 4$ the exponent of p in n is even.*

Theorem 1.7.5. *The only solutions to the Diophantine equation $x^2 + 1 = y^3$ are $x = 0$ and $y = 1$.*

Proof. $(x+i)(x-i) = y^3$. Are $x + i, x - i$ coprime in $\mathbb{Z}[i]$? If $\mathfrak{p}$ is a prime of $\mathbb{Z}[i]$ dividing both, then $\mathfrak{p} \mid 2i$, that is $N(\mathfrak{p}) \mid 4$, so $2 \mid y$, so $8 \mid y^3$. But $x^3 + 1 \equiv 1, 2, 5 \mod 8$, so $\gcd(x+i, x-i) = 1$, so

$$\begin{cases} x + i = uz^3 = (uz)^3 \\ x - i = \overline{uz}^3 = (\overline{uz})^3 \end{cases}, \qquad u \in \{\pm 1, \pm i\},$$

so

$$x - i = (a+bi)^3 = a^3 - b^3 i + 3a^2 bi - 3ab^2, \qquad a, b \in \mathbb{Z}.$$

Looking at coefficients of i, $1 = 3a^2 b - b^3$, so $a = 0$ and $b = -1$. Plugging this back in we get $x = 0$ and $y = 1$. □

1.8 Eisenstein integers

The **Eisenstein integers** are $\mathbb{Z}[\omega]$ for $\omega = \frac{-1+\sqrt{-3}}{2}$. This is a subring of $\mathbb{C}$, since

$$(a+b\omega)(c+d\omega) = ac + (ad+bc)\omega + bd\omega^2 = (ac-bd) + (ad+bc-bd)\omega.$$

What is $\mathbb{Z}\left[\sqrt{-3}\right] \subset \mathbb{Z}[\omega]$? Both are subrings of $\mathbb{Q}\left(\sqrt{-3}\right) = \mathbb{Q}[x]/\left\langle x^3+3\right\rangle$.

- In $\mathbb{Z}\left[\sqrt{-3}\right]$, $4 = 2\cdot 2 = \left(1+\sqrt{-3}\right)\cdot\left(1-\sqrt{-3}\right)$, where $2, 1+\sqrt{-3}, 1-\sqrt{-3}$ are all irreducible.
- $\pi = \frac{1+\sqrt{-3}}{2}$ is a unit in $\mathbb{Z}[\omega]$ and $\pi^6 = 1$, but $\pi \notin \mathbb{Z}\left[\sqrt{-3}\right]$.
- $\mathbb{Z}\left[\sqrt{-3}\right]$ is not integrally closed in $\mathbb{Q}\left(\sqrt{-3}\right)$, but $\mathbb{Z}[\omega]$ is its integral closure and it is integrally closed in $\mathbb{Q}\left(\sqrt{-3}\right)$.
- $\omega^2+\omega+1 = 0$, so ω is an algebraic integer in $\mathbb{Z}[\omega] \setminus \mathbb{Z}\left[\sqrt{-3}\right]$.

Proposition 1.8.1. *If $u \in \mathbb{Z}[\omega]^\times$ then $N(u) = 1$, where*

$$\begin{array}{rccc} N & : & \mathbb{Z}[\omega] & \longrightarrow & \mathbb{Z} \\ & & a+b\omega & \longmapsto & (a+b\omega)(a+b\overline{\omega}) = a^2-ab+b^2 \end{array}.$$

Proof. Multiplicative because it is the restriction of $z \in \mathbb{C} \mapsto |z|^2$ to $\mathbb{Z}[\omega]$. Holds true in any imaginary quadratic field $\mathbb{Q}\left(\sqrt{-d}\right)$. □

$a^2-ab+b^2 = 1$ if and only if $(a,b) = (\pm 1, 0)$, that is $u = \pm 1$, or $(a,b) = (0, \pm 1)$, that is $u = \pm\omega$, or $(a,b) = \pm(1,1)$, that is $u = \pm(1+\omega) = \pm\pi$.

Remark. $\mathbb{Z}[\omega]^\times \cong (\mathbb{Z}/6\mathbb{Z}, +)$.

Theorem 1.8.2. *$\mathbb{Z}[\omega]$ is a Euclidean domain, with Euclidean norm given by $N(a+b\omega) = a^2-ab+b^2$.*

Proof. Let $\alpha, \beta \in \mathbb{Z}[\omega]\setminus\{0\}$. There exists $\kappa, \lambda \in \mathbb{Z}[\omega]$ such that $\alpha = \kappa\beta + \lambda$ and $N(\lambda) < N(\beta)$. Use geometric proof. $\mathbb{Z}[\omega] = \{a+b\omega \mid a,b \in \mathbb{Z}\} \subset \mathbb{C}$ is tiled by parallelograms of $\mathbb{C}$, which are translates of a parallelogram at π. Want to take κ to be a vertex of a parallelogram such that $N(\kappa - \alpha/\beta) < 1$. Parallelogram covered by interior of unit discs centred at lattice points, so ok. Let $\lambda = \beta(\alpha/\beta - \kappa)$, so $N(\lambda)/N(\beta) < 1$. □

Lecture 7 Friday 25/01/19

Lecture 7 is a problem class.

Lemma 1.8.3 (Special case of quadratic reciprocity)**.** *If $p \neq 3$ is an odd prime, then -3 is a square mod p if and only if $p \equiv 1 \mod 3$.*

Lecture 8 Monday 28/01/19

The following is the decomposition of primes in $\mathbb{Z}[\omega]$.

- 3 ramifies. $3 = -\left(\sqrt{-3}\right)^2$, which is irreducible in $\mathbb{Z}[\omega]$.
- $p \equiv 2 \mod 3$ stays inert in $\mathbb{Z}[\omega]$. Because N is multiplicative and p cannot be written as a^2-ab+b^2 with $a, b \in \mathbb{Z}$.
- $p \equiv 1 \mod 3$ splits as a product of distinct prime factors $\mathfrak{p}, \overline{\mathfrak{p}} \in \mathbb{Z}[\omega]$. p divides a^2-ab+b^2 with $a,b \in \mathbb{Z}$ and $p \nmid a, b$, so p divides $(2a-b)^2+3b^2$. Take $z \in \mathbb{Z}$ odd such that $z^2 \equiv -3 \mod p$, and let $b = 1 \in \mathbb{Z}$ and $a = (z+1)/2 \in \mathbb{Z}$. To show that p splits in $\mathbb{Z}[\omega]$, let $p \mid a^2-a+1 = (a+\omega)(a+\overline{\omega})$ for $z \in \mathbb{Z}$. Using unique factorisation, $p \mid a+\omega$ or $p \mid a+\overline{\omega}$. In fact, since $a+\omega, a+\overline{\omega}$ are complex conjugates, $p \mid a+\omega$ and $p \mid a+\overline{\omega}$, so $p \mid \omega - \overline{\omega} = \frac{-1+\sqrt{-3}}{2} - \frac{-1-\sqrt{-3}}{2} = \sqrt{-3}$. But $(3,p) = 1$, a contradiction. Thus $p = \mathfrak{p}\overline{\mathfrak{p}} = N(\mathfrak{p})$. Check that $\mathfrak{p}/\overline{\mathfrak{p}} \neq u \in \mathbb{Z}[\omega]^\times$, (Exercise) so p splits.

Remark. These three possible behaviours have to do with the structure of $\mathbb{Z}[\omega]/\langle p\rangle$.

- If this is a field, p is inert.
- If this is of the form $\mathbb{F}_1 \times \mathbb{F}_2$, p is split.
- If this is of the form $\mathbb{F}[\epsilon]/\left\langle \epsilon^2\right\rangle$, p is ramified.

1.9 Other Euclidean domains

- $\mathbb{Z}[\omega]$ and $\mathbb{Z}[i]$ are norm Euclidean. Using geometric proof, $\mathbb{Z}[i], \mathbb{Z}[\omega] \subset \mathbb{C}$ are lattices.
- $\mathbb{Z}\left[\sqrt{-5}\right]$ is not a UFD, so not Euclidean, since

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

  What goes wrong if we try to adapt geometric proof from $\mathbb{Z}[i], \mathbb{Z}[\omega]$? Unit discs do not cover all of the area of $\mathbb{C}$.

- The ring of integers $\mathcal{O}_7 \subset \mathbb{Q}\left(\sqrt{-7}\right)$ and $\mathcal{O}_{11} \subset \mathbb{Q}\left(\sqrt{-11}\right)$ both are norm Euclidean. Adopt proof from $\mathbb{Z}[i], \mathbb{Z}[\omega]$.
- It is hard to tell which fields are Euclidean and which are not. For example, $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ is not Euclidean but is a PID and a UFD.
- Among real quadratic fields, $\mathbb{Z}\left[\sqrt{2}\right]$ is Euclidean. The same geometric proof will not work because $\mathbb{Z}\left[\sqrt{2}\right] \subset \mathbb{R}$. (Exercise: $\mathbb{Z}\left[\sqrt{2}\right]$ is dense in $\mathbb{R}$) We do have a geometric way to think about this.

$$\frac{\mathbb{Q}\left(\sqrt{2}\right)}{\mathbb{Q}} = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\}$$

  is a two-dimensional $\mathbb{Q}$-vector space.

$$\begin{array}{rccc} \sigma & : & \mathbb{Q}\left(\sqrt{2}\right) & \longrightarrow & \mathbb{Q}\left(-\sqrt{2}\right) \\ & & a + b\sqrt{2} & \longmapsto & a - b\sqrt{2} \end{array}$$

  is a field automorphism that preserves $\mathbb{Q}$.

$$\begin{array}{rcl} \mathbb{Z}\left[\sqrt{2}\right] \subset \mathbb{Q}\left(\sqrt{2}\right) & \hookrightarrow & \mathbb{R}^2 \\ a + b\sqrt{2} & \mapsto & \left(a + b\sqrt{2}, a - b\sqrt{2}\right) \\ 1 & \mapsto & \theta_1 = (1, 1) \\ \sqrt{2} & \mapsto & \theta_2 = \left(\sqrt{2}, -\sqrt{2}\right) \end{array}.$$

  θ_1, θ_2 generate a lattice in $\mathbb{R}^2$. Can do a geometric proof in this, but use $N(x, y) = x \cdot y$ and areas under hyperbolas.

2 Ring of integers in number fields

Lecture 9
Tuesday
29/01/19

Useful for describing the ring of integers $\mathcal{O}_K \subset K$ for a finite extension $K/\mathbb{Q}$ and $\mathcal{O}^\times$, the group of units in $\mathcal{O}_K$, by Dirichlet's unit theorem.

2.1 Modules

Definition 2.1.1. Let R be a ring. An **R-module** M is a set, together with

- an additive structure on M, so $m_1, m_2 \in M$ implies that $m_1 + m_2 \in M$, and
- an action of R on M,
$$\begin{array}{ccc} R \times M & \longrightarrow & M \\ (r, m) & \longmapsto & rm \end{array},$$
satisfying
  - $r(m_1 + m_2) = rm_1 + rm_2$,
  - $1 \cdot m = m$,
  - $r_1(r_2 m) = (r_1 r_2) m$,
  - $(r_1 + r_2) m = r_1 m + r_2 m$, and
  - $0 \cdot m = 0$.

Note.

- If R is a field, then an R-module is just an R-vector space.
- If $R = \mathbb{Z}$, a $\mathbb{Z}$-module M is an abelian group.

Definition 2.1.2. A **free $\mathbb{Z}$-module of rank** n is a $\mathbb{Z}$-module M which has a basis $(e_1, \ldots, e_n)$ such that all $m \in M$ can be written uniquely as $a_1 e_1 + \cdots + a_n e_n$ for $a_1, \ldots, a_n \in \mathbb{Z}$.

Example.

- $\mathbb{Z}$ is a free $\mathbb{Z}$-module of rank one.
- $\mathbb{Z}^n = \{(a_1, \ldots, a_n) \mid a_i \in \mathbb{Z}\}$ is a free $\mathbb{Z}$-module of rank n. Any free $\mathbb{Z}$-module of rank n is isomorphic to $\mathbb{Z}^n$, so there exists $\phi : M \xrightarrow{\sim} \mathbb{Z}^n$, where M is free of rank n, such that $\phi(m_1 + m_2) = \phi(m_1) + \phi(m_2)$, and $\phi(nm) = n\phi(m)$ that is redundant once you respect addition.
- $\mathbb{Z}/3\mathbb{Z}$ is not free because $3 \cdot 1 = 0$. 0 is not written uniquely in terms of basis.
- Any finite abelian group is a $\mathbb{Z}$-module, but not free.
- $\mathbb{Q} = \{r/s \mid (r, s) = 1,\ r, s \in \mathbb{Z},\ s > 0\}$ is a $\mathbb{Z}$-module but it is not free of finite rank. Assume that $\mathbb{Q}$ was free of rank n, for some $n \in \mathbb{Z}_{\geq 0}$. Let $e_1 = r_1/s_1, \ldots, e_n = r_n/s_n$ be a basis. Then
$$\frac{1}{s_1 \cdot \cdots \cdot s_n + 1} \notin e_1\mathbb{Z} \oplus \cdots \oplus e_n\mathbb{Z},$$
a contradiction. Alternatively, prove that e_1 and e_2 are linearly dependent over $\mathbb{Z}$, so rank would have to be one, and argue as above.
- $\mathbb{Z}[i], \mathbb{Z}[\omega], \mathbb{Z}\left[\sqrt{-5}\right]$ are free $\mathbb{Z}$-modules of rank two. We will later see that the ring of integers $\mathcal{O}_K \subset K$ is a free $\mathbb{Z}$-module of rank equal to the rank of $K/\mathbb{Q}$, or $\dim_{\mathbb{Q}}(K)$.

2.2 Structure theorem for finitely generated abelian groups

Theorem 2.2.1 (Structure theorem, weak form)**.** *Let M be a free $\mathbb{Z}$-module of finite rank n, and $M' \subseteq M$ be a $\mathbb{Z}$-submodule. Then M' is free of rank $m \leq n$.*

Proof. We will prove this by induction on $n = rk(M)$. We have a basis $e_1, \ldots, e_n$ of M and projections

$$\begin{array}{rccc} p_i & : & M & \longrightarrow & \mathbb{Z} \\ & & a_1 e_1 + \cdots + a_n e_n & \longmapsto & a_i \end{array},$$

which are module homomorphisms. If $p_i(M') = 0$ for every $i = 1, \ldots, n$, then $M' = 0$. If $M' \neq 0$, we can assume without loss of generality that $p_1(M') \neq 0$.

- $p_1(M')$ will be an ideal of $\mathbb{Z}$, therefore it will be a principal ideal. There exists $x \in M'$ such that $p_1(M') = \langle p_1(x) \rangle$.
- $N = Ker(p_1) \hookrightarrow M$ is a submodule of M free of rank $n-1$ because it is generated by $e_2, \ldots, e_n$.

Consider $N' = N \cap M'$, a submodule of N, M', M. We have an isomorphism of $\mathbb{Z}$-modules

$$N' \oplus x\mathbb{Z} = \{n' + n \cdot x \mid n' \in N',\ n \in \mathbb{Z}\} \cong M'.$$

(Exercise: prove) N is free of rank $n-1$, so by induction hypothesis N' is free of rank $m' \leq n-1$. M' is free of rank $m' + 1 \leq n$. Have a basis $(e_1', \ldots, e_{m'}', x)$ for M', where $(e_1, \ldots, e_{m'}')$ is a basis for N'. □

Theorem 2.2.2 (Structure theorem, strong form)**.** *Let M be a free $\mathbb{Z}$-module of rank n. Let $M' \subseteq M$ be a submodule. Then there exist*

- *a basis $(e_1, \ldots, e_n)$ of M, and*
- *$a_1, \ldots, a_q \in \mathbb{Z} \setminus \{0\}$ for $q \leq n$ such that M' has a basis $(a_1 e_1, \ldots, a_q e_q)$ and such that $a_1 \mid \cdots \mid a_q$.*

Corollary 2.2.3. *Let G be a finitely generated abelian group. Then there exist $a_1, \ldots, a_n \in \mathbb{Z}$ such that $a_1 \mid \cdots \mid a_n$ and*

$$G \cong \frac{\mathbb{Z}}{a_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{a_n\mathbb{Z}}.$$

Lecture 10
Friday
01/02/19

Remark. In Corollary 2.2.3, we are allowing $a_i = 0$ for some $i \in \{1, \ldots, n\}$.

Proof. Consider $e_1, \ldots, e_n$, the generators of G, and let M be the free $\mathbb{Z}$-module spanned by $e_1, \ldots, e_n$. $\phi : M \twoheadrightarrow G$ is a surjective $\mathbb{Z}$-module homomorphism. Have isomorphism of $\mathbb{Z}$-modules $M/M' \subseteq G$, induced by ϕ. Theorem 2.2.2 implies that

$$M = e_1\mathbb{Z} \oplus \cdots \oplus e_n\mathbb{Z}, \qquad M' = a_1 e_1 \mathbb{Z} \oplus \cdots \oplus a_q e_q \mathbb{Z}, \qquad a_{q+1} = \cdots = a_n = 0.$$

Thus

$$\frac{M}{M'} \cong \frac{\mathbb{Z}}{a_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{a_q\mathbb{Z}} \times \frac{\mathbb{Z}}{a_{q+1}\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{a_n\mathbb{Z}} \cong \frac{\mathbb{Z}}{a_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{a_q\mathbb{Z}} \times \mathbb{Z} \times \cdots \times \mathbb{Z}.$$

□

Lemma 2.2.4. *Let M be a free $\mathbb{Z}$-module of rank n, and $x \in M$. Let $p_1 : M \to \mathbb{Z}$ and $p_2 : M \to \mathbb{Z}$. There exists a homomorphism $M \to \mathbb{Z}$ such that $p(x) \mid p_1(x)$ and $p(x) \mid p_2(x)$.*

Proof. Find $a, b \in \mathbb{Z}$ such that $\gcd(p_1(x), p_2(x)) = ap_1(x) + bp_2(x)$, by Euclid's algorithm. Define $p = ap_1 + bp_2$. □

Lemma 2.2.5. *Let R be a PID. Let S be a set of ideals of R. There exists an ideal $I \in S'$ such that $I \subseteq J$ and $J \in S'$ implies that $I = J$, that is such that I is maximal with respect to inclusion.*

Proof. We will use the ascending chain condition, ok because R is a PID, to argue by contradiction. If Lemma 2.2.5 were not true, would set $I_1 \subsetneq I_2 \subsetneq \ldots$ with $I_i \in S$, a contradiction. □

Lemma 2.2.6. *Let M be a free $\mathbb{Z}$-module of rank n, and $x \in M$. Then there exists a homomorphism $p : M \to \mathbb{Z}$ such that $p(x) \mid q(x)$ for every $q : M \to \mathbb{Z}$.*

Proof. Look at the set of all ideals $\langle q(x)\rangle \subseteq \mathbb{Z}$. Applying Lemma 2.2.5, there exists $\langle p(x)\rangle \subseteq \mathbb{Z}$, where $p : M \to \mathbb{Z}$, which is maximal with respect to inclusion. Want $p(x) \mid q(x)$ for all $q : M \to \mathbb{Z}$. Applying Lemma 2.2.4 to p, q gives $r : M \to \mathbb{Z}$ such that $r(x) \mid q(x)$ and $r(x) \mid p(x)$, so $\langle r(x)\rangle \supseteq \langle p(x)\rangle$. Because p is maximal, have equality $r(x) \sim p(x)$, so $p(x) \mid q(x)$. □

Proof of Theorem 2.2.2. Argue by induction on $n = rk_{\mathbb{Z}}(M)$.

- Let $M' \subseteq M$. If $p : M \to \mathbb{Z}$, then $p(M') \subseteq M$. Choose p such that $p(M')$ is maximal with respect to inclusion among all $q : M \to \mathbb{Z}$.
- What is $p(M) \subseteq \mathbb{Z}$? We have $p(M) = a\mathbb{Z}$ for $a \in \mathbb{Z} \setminus \{0\}$. If $a \neq \pm 1$, could define $p'(x) = p(x)/a$ for all $x \in M$. $p'(M') \supsetneq p(M')$ contradicts the maximality of p with respect to M'. Thus $p(M) = \mathbb{Z}$.
- Let $N = Ker(p) \subseteq M$, where $p : M \twoheadrightarrow \mathbb{Z}$. N is free of rank $n-1$, and $N' = M' \cap N$ be a submodule.

$$\begin{array}{ccc} N' & \hookrightarrow & N \\ \downarrow & & \downarrow \\ M' & \hookrightarrow & M \\ \downarrow & & \downarrow \\ p(M') & \hookrightarrow & \mathbb{Z} \end{array}.$$

- Apply induction hypothesis to (N, N'). N has a basis $(e_2, \dots, e_n)$. Can complete $(e_2, \dots, e_n)$ to a basis for M. Choose $e_1' \in M$ such that $p(e_1') = 1$. Have a basis $(e_1', e_2, \dots, e_n)$ of M.
- There exist $a_2, \dots, a_q \in \mathbb{Z} \setminus \{0\}$ such that N' has a basis $(a_2e_2, \dots, a_qe_q)$ and $a_2 \mid \cdots \mid a_q$. $M' \twoheadrightarrow p(M') = a_1\mathbb{Z}$ for $a_1 \in \mathbb{Z} \setminus \{0\}$, assuming $M' \neq 0$. Choose $x \in M'$ such that $p(x) = a_1$. We may assume $p(x) \mid q(x)$ for every $q : M \to \mathbb{Z}$. Look at $(e_1', e_2, \dots, e_n)$, a basis of M. Let $p_i : M \to \mathbb{Z}$ be the projection onto the i-th coordinate. $a_1 \mid p_i(x)$ for all $i = 1, \dots, n$, by maximality property of p and $p(x) = a_1$. Can find a basis $(e_1, \dots, e_n)$ of M such that $x = a_1e_1$, where

$$e_1 = e_1' + \frac{p_2(x)}{a_1}e_2 + \cdots + \frac{p_n(x)}{a_1}e_n, \qquad \frac{p_2(x)}{a_1}, \dots, \frac{p_n(x)}{a_1} \in \mathbb{Z}.$$

- Left to prove that $a_1 \mid a_2$. Let $d = (a_1, a_2) = b_1a_1 + b_2a_2$. There exists $d : M \to \mathbb{Z}$ such that $d(x) = b_1p_1(x) + b_2p_2(x)$, where $p_1(x) = p(x) = a_1$ and $p_2(x) = a_2$. This will contradict maximality of $p_1 = p$.

□

Lecture 11
Monday
04/02/19

Definition 2.2.7.

- If M is a $\mathbb{Z}$-module, an element $x \in M \setminus \{0\}$ is called a **torsion element** if there exists $a \in \mathbb{Z} \setminus \{0\}$ such that $ax = 0$.
- We say that a $\mathbb{Z}$-module M is **torsion-free** if it does not contain torsion elements, that is if $ax = 0$ for $a \in \mathbb{Z}$ and $x \in M$, then $a = 0$ or $x = 0$.

Example.

- If G is any finite group, all elements of G are torsion.
- If M is a free $\mathbb{Z}$-module, then M is torsion-free, such as $\mathbb{Z}^n$ for $n \in \mathbb{Z}_{\geq 1}$.
- $\mathbb{Q}$ is torsion-free, even though it is not free of finite rank.

Proposition 2.2.8. *If M is a finitely generated $\mathbb{Z}$-module and torsion-free, then M is free of finite rank.*

Proof. Using structure theorem,

$$M \cong \frac{\mathbb{Z}}{a_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{a_n\mathbb{Z}}, \qquad a_1, \dots, a_n \in \mathbb{Z}, \qquad a_1 \mid \cdots \mid a_n.$$

Want $a_1 = \cdots = a_n = 0$. If not, there exists $a_i \neq 0$ such that all $x \in \mathbb{Z}/a_i\mathbb{Z} \setminus \{0\}$ are torsion elements, so M cannot be a torsion-free, a contradiction. □

2.3 Integral elements

Definition 2.3.1. An element $x \in \mathbb{C}$ is called

- an **algebraic number** if it satisfies an equation
$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0, \qquad a_i \in \mathbb{Q},$$
- an **algebraic integer** if $a_i \in \mathbb{Z}$.

Example.

- $x = i$ is an algebraic integer, since $x^2 + 1 = 0$.
- $x = \sqrt{2}$ is an algebraic integer, since $x^2 - 2 = 0$.
- $x = \sqrt{2} + i$ is an algebraic integer, since
$$x - \sqrt{2} = i \qquad \Longrightarrow \qquad x^2 - 2\sqrt{2}x + 3 = 0 \qquad \Longrightarrow \qquad x^4 - 2x^2 + 9 = 0.$$

In general, sum of product of algebraic integers are algebraic integers.

Definition 2.3.2. Let R be a ring and $A \subseteq R$. An element $x \in R$ is said to be **integral** over A if there exists a monic polynomial equation
$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0, \qquad a_0, \ldots, a_{n-1} \in A.$$

Theorem 2.3.3. *Let R be an ID and $A \subseteq R$ a subring. Then if $a, b \in R$ are integral over A, so are $a + b, a - b, ab$.*

Lemma 2.3.4. *Let R be an ID. Let*
$$M = (a_{ij})_{1 \le i,j \le n} \in M_n(R)$$
be an $n \times n$ matrix with coefficients in R. Assume $v = (v_1, \ldots, v_n) \in R^n$ for $x \in R$ such that $Mv = x \cdot v$, that is v is an eigenvector of M with eigenvalue x. Let $P \in R[X]$ be the characteristic polynomial of M. Then $P(x) = 0$, that is x is a root of P.

Proof.
$$P(X) = \det(X \cdot I_n - M) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$$
is monic of degree n with coefficients in R. Cayley-Hamilton theorem implies that
$$M^n + a_{n-1}M^{n-1} + \cdots + a_0 I_n = 0_n \in R^n,$$
so
$$M^n v + a_{n-1}M^{n-1}v + \cdots + a_0 I_n v = 0_n \in R^n.$$
Since $Mv = x \cdot v$, we get
$$x^n \cdot v + a_{n-1}x^{n-1} \cdot v + \cdots + a_0 \cdot v = 0_n \in R^n,$$
so
$$\left(x^n + a_{n-1}x^{n-1} + \cdots + a_0\right) \cdot v = 0_n \in R^n.$$
$v \neq 0$, so
$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0 \in R,$$
so x is a root of P. □

Proof of Theorem 2.3.3. Let $x = a + b$. The proof is similar for $a - b$ and ab. a is integral over A, so there exists a polynomial $f \in A[x]$ for $n = \deg(f)$ such that

$$f(a) = a^n + a_{n-1}a^{n-1} + \cdots + a_0 = 0, \tag{2}$$

so $a^n = -a_{n-1}a^{n-1} - \cdots - a_0$ is in the A-linear span of $a^{n-1}, \ldots, 1$. Similarly for b, there exists $g \in A[x]$ for $m = \deg(g)$ such that

$$g(b) = b^m + b_{m-1}b^{m-1} + \cdots + b_0 = 0, \tag{3}$$

so b^m is in the A-linear span of $b^{m-1}, \ldots, 1$.

$$(a+b) \cdot a^i b^j = a^{i+1}b^j + a^i b^{j+1}, \qquad i = 0, \ldots, n-1, \qquad j = 0, \ldots, m-1.$$

If $i + 1 = n$ use equation (2). If $j + 1 = m$ use equation (3). Then $(a + b) \cdot a^i b^j$ is an A-linear combination of $a^k b^l$ for $k \in \{0, \ldots, n-1\}$ and $l \in \{0, \ldots, m-1\}$. Consider

$$v = \begin{pmatrix} 1 \\ \vdots \\ a^{n-1}b^{m-1} \end{pmatrix} \in R^{m \cdot n}.$$

$(a + b) \cdot v = M \cdot v$ for some $n \cdot m \times n \cdot m$ matrix $M \in M_{n \cdot m}(A)$. Lemma 2.3.4 implies that $a + b$ is a root of $\det(I_{n \cdot m}X - M) \in A[X]$, that is $a + b$ is integral over A. □

Corollary 2.3.5. *If R is an integral domain and $A \subseteq R$. Then the set $A' = \{x \in R \mid x \text{ integral over } A\}$ is a subring of R, containing A. A' is the **integral closure** of A in R.*

Definition 2.3.6.

- Let R be an ID with field of fractions K. The **integral closure** of R is the integral closure of R in K.
- We say R is **integrally closed** if R is the integral closure of R.

Example.

- $\mathbb{Z}, \mathbb{Z}[\omega], \mathbb{Z}[x]$ are integrally closed.
- $R = \mathbb{Z}\left[\sqrt{-3}\right]$ is not integrally closed. If $\omega = \frac{-1+\sqrt{-3}}{2}$ then $\omega \in K = \mathbb{Q}\left(\sqrt{-3}\right)$ and $\omega^2 + \omega + 1 = 0$, so ω is integral over $\mathbb{Z}\left[\sqrt{-3}\right]$ but not in $\mathbb{Z}\left[\sqrt{-3}\right]$. Integral closure of $\mathbb{Z}\left[\sqrt{-3}\right]$ is $\mathbb{Z}[\omega]$, the Eisenstein integers.
- $\mathbb{Q}[x, y] / \langle x^2 - y^3 \rangle$ is not integrally closed. $t = x/y \in Frac\left(\mathbb{Q}[x, y] / \langle x^2 - y^3 \rangle\right)$ satisfies monic polynomial equations $t^2 - y = 0$ and $t^3 - x = 0$.

Lecture 12
Tuesday
05/02/19

Proposition 2.3.7. *Let R be a UFD. Then R is integrally closed.*

Proof. Let $K = Frac(R)$. Let $x \in K$ be integral over R. Want $x \in R$. x satisfies a monic polynomial equation

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0, \qquad a_{n-1}, \ldots, a_0 \in R. \tag{4}$$

Write $x = a/b$ with $a, b \in R \setminus \{0\}$. Can we ensure that a, b have no irreducible factor in common? Yes. Among all possible representations $x = a/b$, choose the one for which $d(b) \in \mathbb{Z}_{\geq 0}$, the number of irreducible factors of b, is the smallest. If $\mathfrak{p} \mid a$ and $\mathfrak{p} \mid b$ then $a' = a/\mathfrak{p}$ and $b' = b/\mathfrak{p}$, so $x = a/b = a'/b'$, where $d(b') = d(b) - 1$, a contradiction. Multiplying (4) by b^n,

$$a^n + a_{n-1}a^{n-1}b + \cdots + a_0 b^n = 0,$$

so

$$b\left(a_{n-1}a^{n-1}b + \cdots + a_0\right) = -a^n,$$

so $b \mid a^n$, but $\gcd(a, b) = 1$. Thus $b \in R^\times$ is a unit, so $x = a/b \in R$. □

Theorem 2.3.8. *Let $R \subset S$ be an inclusion of IDs. Let R' be the integral closure of R in S. Then R' is integrally closed in S.*

Example. Let $\mathbb{Z} \subset R$, where $R/\mathbb{Q}$ is a finite extension. Let $\mathcal{O}_K$ be the integral closure of $\mathbb{Z}$ in K, the ring of integers of K. Then $\mathcal{O}_K$ is integrally closed. Applies to $\mathbb{Z}[i], \mathbb{Z}[\omega], \mathbb{Z}\left[\sqrt{-5}\right]$.

2.4 Quadratic fields

A **number field** K is a field containing $\mathbb{Q}$ such that $\dim_{\mathbb{Q}}(K)$ is finite. Any finite field extension of $\mathbb{Q}$ is a number field. The **degree** of the number field is by definition $\dim_{\mathbb{Q}}(K)$. A **quadratic field** is an extension of $\mathbb{Q}$ of degree two. The **ring of integers** $\mathcal{O}_K \subset K$ is the integral closure of $\mathbb{Z}$ in K.

Lemma 2.4.1. *Every quadratic field $K/\mathbb{Q}$ is of the form*

$$\mathbb{Q}\left(\sqrt{d}\right) = \left\{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\right\},$$

for some square-free $d \in \mathbb{Z}$.

Proof. Let $x \in K \setminus \mathbb{Q}$. Then $\langle 1, x\rangle$ is a $\mathbb{Q}$-basis of K. $x^2 + \alpha x + \beta \in K$ for $\alpha, \beta \in \mathbb{Q}$ implies that $x = \left(\alpha \pm \sqrt{\alpha^2 + 4\beta}\right)/2$, and $d = \alpha^2 + 4\beta \in \mathbb{Q}$, so $K = \mathbb{Q}\left(\sqrt{d}\right)$. Multiplying d by n^2, for all $n \in \mathbb{Z}$, $\mathbb{Q}\left(\sqrt{d}\right) = \mathbb{Q}\left(\sqrt{dn^2}\right)$, so can assume $d \in \mathbb{Z}$. Similarly, can assume d is square-free. Thus $\left\langle 1, \sqrt{d}\right\rangle$ is a basis over $\mathbb{Q}$. □

Remark. If $d < 0$, $\mathbb{Q}\left(\sqrt{d}\right)$ is called an **imaginary quadratic field**. If $d > 0$, $\mathbb{Q}\left(\sqrt{d}\right)$ is called a **real quadratic field**.

Theorem 2.4.2. *Let $K = \mathbb{Q}\left(\sqrt{d}\right)$ with $d \in \mathbb{Z}$ square-free. Note that $d \not\equiv 0 \mod 4$.*

1. *If $d \equiv 2, 3 \mod 4$ then*
$$\mathcal{O}_K = \mathbb{Z}\left[\sqrt{d}\right] = \left\{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\right\}.$$
2. *If $d \equiv 1 \mod 4$ then*
$$\mathcal{O}_K = \left\{\tfrac{u+v\sqrt{d}}{2} \mid u, v \in \mathbb{Z},\ u \equiv v \mod 2\right\} \supsetneq \mathbb{Z}\left[\sqrt{d}\right].$$
In this case $\mathcal{O}_K$ is the $\mathbb{Z}$-linear span of 1 and $\frac{1+\sqrt{d}}{2}$.

Example.

1. $\mathbb{Z}[i], \mathbb{Z}\left[\sqrt{-2}\right], \mathbb{Z}\left[\sqrt{2}\right], \mathbb{Z}\left[\sqrt{-5}\right]$.
2. $\mathbb{Z}[\omega], \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$.

Proof. Let $\mathcal{O}_K$ be the integral closure of $\mathbb{Z}$ in $\mathbb{Q}\left(\sqrt{d}\right) = K$. Let $x = a + b\sqrt{d}$ for $a, b \in \mathbb{Q}$. Assume x is an algebraic integer. Let $\overline{x} = a - b\sqrt{d}$. Then $x, \overline{x}$ satisfy the same polynomial equation with $\mathbb{Z}$ coefficients, so $\overline{x} = a - b\sqrt{d}$ is also an algebraic integer.

- $x\overline{x} = \left(a + b\sqrt{d}\right)\left(a - b\sqrt{d}\right) = a^2 - b^2 d \in \mathbb{Q}$ is an algebraic integer, so $a^2 - b^2 d \in \mathbb{Z}$.
- $x - \overline{x} = 2b\sqrt{d}$, so $4b^2 d \in \mathbb{Z}$, so $2b \in \mathbb{Z}$, because d is square-free.
- $x + \overline{x} = 2a$, so $2a \in \mathbb{Z}$.

Let $a = u/2$ and $b = v/2$.

1. If $d \equiv 2, 3 \mod 4$,
$$a^2 - b^2 d = \frac{u^2 - v^2 d}{4} \in \mathbb{Z} \quad \Longrightarrow \quad 4 \mid u^2, v^2 \quad \Longrightarrow \quad 2 \mid u, v \quad \Longrightarrow \quad a, b \in \mathbb{Z}.$$
2. If $d \equiv 1 \mod 4$,
$$a^2 - db^2 = \frac{u^2 - v^2 d}{4} \in \mathbb{Z} \quad \Longrightarrow \quad 4 \mid u^2 - dv^2 \quad \Longrightarrow \quad u \equiv v \mod 2.$$

□

Lecture 13 is a problem class.

Lecture 13
Friday
08/02/19

2.5 Traces and norms

Lecture 14
Monday
11/02/19

Let $K/\mathbb{Q}$ be a quadratic field. The conjugate is

$$\begin{array}{ccc} K & \longrightarrow & K \\ \alpha = a + b\sqrt{d} & \longmapsto & \overline{\alpha} = a - b\sqrt{d} \end{array}.$$

Then

$$\begin{array}{ccccc} Tr & : & K & \longrightarrow & \mathbb{Q} \\ & & \alpha & \longmapsto & \alpha + \overline{\alpha} \end{array}, \qquad \begin{array}{ccccc} Nm & : & K & \longrightarrow & \mathbb{Q} \\ & & \alpha & \longmapsto & \alpha \cdot \overline{\alpha} \end{array},$$

and $Tr : \mathcal{O}_K \to \mathbb{Z}$ and $Nm : \mathcal{O}_K \to \mathbb{Z}$. $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank two. The goal is to discuss trace and norm for general number fields. Motivation is that $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $\deg(K/\mathbb{Q})$.

Proposition 2.5.1. *Let $F \subseteq \mathbb{C}$ be a subfield. Let K/F be a finite extension of degree n. Then there exist exactly n embeddings $\sigma : K \hookrightarrow \mathbb{C}$ such that $\sigma|_F = id_F$.*

Proof. Assume first that $K = F(x)$, where x is a root of a minimal polynomial $P(t) \in F[t]$. P has degree n, since x^n is an F-linear combination of $1, \ldots, x^{n-1}$. P has n distinct roots in $\mathbb{C}$. Let α be a root of $P(t)$ in $\mathbb{C}$. This determines

$$\begin{array}{ccccc} \sigma & : & K & \longrightarrow & \mathbb{C} \\ & & x & \longmapsto & \sigma(x) = \alpha \end{array}, \qquad \sigma|_F = id_F.$$

Conversely, if $\sigma : K \hookrightarrow \mathbb{C}$ such that $\sigma|_F = id_F$, $\sigma(P(t)) = P(t)$ and $\sigma(x)$ is some root of $P(t)$ in $\mathbb{C}$. In general, use induction on $\deg(K/F) = n$.

- $n = 1$ is ok. $K = F$, so only one embedding.
- $n > 1$. Choose $x \in K \setminus F$. $K/F(x)/F$, so apply induction hypothesis on $\deg(K/F(x)) < \deg(K/F)$.

$$n = \deg(K/F) = \deg(K/F(x)) \cdot \deg(F(x)/F) = k \cdot m.$$

Have m embeddings $\tau : F(x) \hookrightarrow \mathbb{C}$ such that $\tau|_F = id_F$. By induction, have k embeddings $\sigma : K \hookrightarrow \mathbb{C}$ such that $\sigma|_{F(x)} = \tau$. Overall, have $n = k \cdot m$ embeddings $K \hookrightarrow \mathbb{C}$ which are id_F on F.

□

Notation. Let $e(K/F)$ denote the set of embeddings as in Proposition 2.5.1.

Let $x \in K$. Think of

$$\begin{array}{ccc} K & \longrightarrow & K \\ y & \longmapsto & x \cdot y \end{array}$$

as an F-linear transformation on K. Let $char_{K/F}(x)$ denote the characteristic polynomial of multiplication by x in K. $char_{K/F}(x) \in F[t]$ has degree $n = [K : F]$.

Example. Let $K/\mathbb{Q}$ be quadratic and $x = \sqrt{d}$. Then

$$a + b\sqrt{d} \mapsto x \cdot \left(a + b\sqrt{d}\right) = a\sqrt{d} + bd.$$

If $K \cong \mathbb{Q}^2$, then

$$x = \begin{pmatrix} 0 & d \\ 1 & 0 \end{pmatrix}, \qquad char_{K/\mathbb{Q}}(x) = t^2 - d = \left(t - \sqrt{d}\right)\left(t + \sqrt{d}\right).$$

Proposition 2.5.2. *Let K/F be a finite extension of degree n. Then*

$$char_{K/F}(x) = \prod_{\sigma \in e(K/F)} (t - \sigma(x)) \in F[t], \qquad x \in K.$$

Proof. First assume $K = F(x)$. Then the right hand side is just the minimal polynomial $P(t) \in F[t]$ of x. For any root α of $P(t)$, $char_{K/F}(x)(\alpha) = 0$, since

$$\begin{array}{ccc} K & \longrightarrow & \mathbb{C} \\ x & \longmapsto & \alpha \end{array}$$

has an F-basis given by $1, \ldots, \alpha^{n-1}$, and multiplication by α shifts this. Every root of $P(t)$ is also a root of $char_{K/F}(x)$, and they are both monic polynomials of degree n, so $P(t) = char_{K/F}(x)$. In general, $K/F(x)/F$. Choose a basis $e_1, \ldots, e_m$ of K over $F(x)$. For any $i = 1, \ldots, m$ multiplication by x leaves $e_i F(x) \subset K$ stable and has characteristic polynomial equal to

$$\prod_{\sigma \in e(F(x)/F)} (t - \sigma(x)),$$

where $e_i F(x) \subset K$ is an F-vector subspace of dimension $\deg(F(x)/F)$. Thus

$$char_{K/F}(x) = \prod_{\sigma \in e(F(x)/F)} (t - \sigma(x))^m = \prod_{\sigma \in e(F(x)/F)} \left(\prod_{\tau \in e(K/F(x)),\ \tau_{F(x)} = \sigma} (t - \tau(x)) \right).$$

□

Lecture 15
Tuesday
12/02/19

Definition 2.5.3. $Tr : K \to F$ is the trace of multiplication by x and $Nm : K \to F$ is the determinant of multiplication by x. These are coefficients of $char_{K/F}(x)$.

Theorem 2.5.4. *Let $R \subseteq F$ be an integrally closed domain. Let S be the integral closure of R in K. Then if $x \in S$, $char_{K/F}(x) \in R[t]$.*

Corollary 2.5.5. *Let K, F, S, R as in Theorem 2.5.4. We have $Tr : S \to R$ and $Nm : S \to R$.*

Example. Let $K/\mathbb{Q}$ be quadratic. Then $Tr : \mathcal{O}_K \to \mathbb{Z}$ and $Nm : \mathcal{O}_K \to \mathbb{Z}$.

Proof of Theorem 2.5.4. Let $x \in S$. Is

$$char_{K/F}(x) = \prod_{\sigma \in e(K/F)} (t - \sigma(x)) \in R[t]?$$

Let L be the **composite** of extensions $\sigma(K) \subseteq \mathbb{C}$, the smallest field extension of F containing all $\sigma(K)$. Let T be the integral closure of R in L.

$$\begin{array}{ccc} T & \subset & L \\ \uparrow & & \uparrow \\ S & \subset & K \\ \uparrow & & \uparrow \\ R & \subset & F \end{array}.$$

For all $\sigma \in e(K/F)$, $\sigma(x)$ is a root of the minimal polynomial $P(t) \in F[t]$ of x over F, and $x \in S$, so $P(t) \in R[t]$, so $\sigma(x) \in T$. The coefficients of $char_{K/F}(x)$ are symmetric polynomials in the $\sigma(x)$,

$$\sum_{\sigma \in e(K/F)} \sigma(x), \sum_{\sigma, \sigma' \in e(K/F)} \sigma(x)\sigma'(x), \cdots \in T,$$

therefore they are elements of T. Upshot is that $char_{K/F}(x) \in (F \cap T)[t] = R[t]$, since $F \cap T$ is the integral closure of R in F, which is R. □

Corollary 2.5.6. *If $K/\mathbb{Q}$ is a finite extension, so $F = \mathbb{Q}$, and $\mathcal{O}_K \subset K$ is the ring of integers, so $R = \mathbb{Z}$. Then $Tr : \mathcal{O}_K \to \mathbb{Z}$ and $Nm : \mathcal{O}_K \to \mathbb{Z}$.*

2.6 Bilinear forms

Definition 2.6.1. Let V be a finite dimensional $\mathbb{Q}$-vector space. A function

$$\begin{array}{rccc} \langle , \rangle & : & V \times V & \longrightarrow & \mathbb{Q} \\ & & (v, w) & \longmapsto & \langle v, w \rangle \end{array}$$

is

- **$\mathbb{Q}$-bilinear** if it is $\mathbb{Q}$-linear as a function of v and $\mathbb{Q}$-linear as a function of w,
- **symmetric** if $\langle v, w \rangle = \langle w, v \rangle$, and
- **non-degenerate** if for all $v \in V$ such that $v \neq 0$, there exists $w \in V$ such that $\langle v, w \rangle \neq 0$.

Example.

- Let $V = \mathbb{Q}$.
$$\begin{array}{ccc} V \times V & \longrightarrow & \mathbb{Q} \\ (v, w) & \longmapsto & 0 \end{array}$$
is symmetric and bilinear.
- Let $V = \mathbb{Q}^2$.
$$\begin{array}{ccc} V \times V & \longrightarrow & \mathbb{Q} \\ (v, w) & \longmapsto & \langle v, w \rangle = v \cdot w = v \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} w^t \end{array}$$
is the inner product, which is non-degenerate.
- Let $K/\mathbb{Q}$ be quadratic.
$$\begin{array}{rccc} Tr_{K/\mathbb{Q}}(,) & : & K \times K & \longrightarrow & \mathbb{Q} \\ & & (x, y) & \longmapsto & Tr_{K/\mathbb{Q}}(x \cdot y) \in \mathbb{Q} \end{array}$$
is
  - symmetric, because $x \cdot y = y \cdot x$, that is multiplication in K is commutative,
  - non-degenerate, because for all $x \in K^\times$, take $y = x^{-1}$,
  $$Tr_{K/\mathbb{Q}}(x, y) = Tr_{K/\mathbb{Q}}\left(xx^{-1}\right) = Tr_{K/\mathbb{Q}}(1) = 2 \neq 0,$$
  - bilinear, because $Tr_{K/\mathbb{Q}}$ is $\mathbb{Q}$-linear.
- Let $K = \mathbb{Q}(i)$, $x = a + bi$, and $y = c + di$.
$$Tr_{\mathbb{Q}(i)/\mathbb{Q}}(x, y) = Tr_{\mathbb{Q}(i)/\mathbb{Q}}((a + bi)(c + di)) = Tr_{\mathbb{Q}(i)/\mathbb{Q}}(ac - bd + ibc + iad) = 2(ac - bd),$$
so $x, y \in \mathbb{Z}[i]$, so $Tr_{\mathbb{Q}(i)/\mathbb{Q}}(x, y) \in \mathbb{Z}$.

2.7 Lattices

Lecture 16
Friday
15/02/19

Definition 2.7.1. Let V be a finite dimensional $\mathbb{Q}$-vector space. A **free $\mathbb{Z}$-lattice**, or **lattice**, in V is a $\mathbb{Z}$-submodule $M \subseteq V$ that is free of rank $\dim_{\mathbb{Q}}(V)$.

Example.

- $\mathbb{Q}\left(\sqrt{-3}\right) \supset \mathbb{Z}\left[\sqrt{-3}\right], \mathbb{Z}\left[2\sqrt{-3}\right], \mathbb{Z}[\omega/2]$ are lattices.
- $\mathbb{Z}, \sqrt{-3}\mathbb{Z}$ are not lattices.

Lemma 2.7.2. *Let $M \subseteq V$ be a lattice. If $e_1, \dots, e_n$ is a $\mathbb{Z}$-basis for M then $e_1, \dots, e_n$ is a $\mathbb{Q}$-basis for V.*

Proof. Notice that $\dim_{\mathbb{Q}}(V) = n$, since $rk_{\mathbb{Z}}(M) = n$. If $e_1, \dots, e_n$ are $\mathbb{Q}$-linearly independent then $e_1, \dots, e_n$ generate $W \subseteq V$ with $\dim_{\mathbb{Q}}(W) = n = \dim_{\mathbb{Q}}(V)$, so $W = V$. Assume there exist $a_1, \dots, a_n \in \mathbb{Q}$ such that

$$a_1 e_1 + \cdots + a_n e_n = 0.$$

Multiply this equation by the product of the denominators of the a_i, which is not zero,

$$a_1' e_1 + \cdots + a_n' e_n = 0, \qquad a_1', \dots, a_n' \in \mathbb{Z},$$

so $a_1' = \cdots = a_n' = 0$. Thus $a_1 = \cdots = a_n = 0$. □

Let $M \subseteq V/\mathbb{Q}$ be a lattice. Let $\langle , \rangle$ be a non-degenerate symmetric bilinear form on V. Define

$$M^V = \{w \in V \mid \langle v, w \rangle \in \mathbb{Z} \text{ for all } v \in M\}.$$

Proposition 2.7.3. *$M^V \subseteq V$ is also a lattice.*

Example. Let $K = \mathbb{Q}\left(\sqrt{-3}\right)$, $Tr_{K/\mathbb{Q}}(,)$, and $M = \mathbb{Z}\left[\sqrt{-3}\right]$. Then

$$Tr_{K/\mathbb{Q}}\left(a + b\sqrt{-3}, c + d\sqrt{-3}\right) = Tr_{K/\mathbb{Q}}\left(ac - 3bd + \sqrt{-3}(ad + bc)\right) = 2(ac - 3bd).$$

- $\left\langle 1, c + d\sqrt{-3} \right\rangle = 2c \in \mathbb{Z}$.
- $\left\langle \sqrt{-3}, c + d\sqrt{-3} \right\rangle = -6d \in \mathbb{Z}$.

Thus

$$M^V = \left\{c + d\sqrt{-3} \mid c \in \tfrac{1}{2}\mathbb{Z},\ d \in \tfrac{1}{6}\mathbb{Z}\right\} = \left\langle \tfrac{1}{2}, \tfrac{\sqrt{-3}}{6} \right\rangle \supseteq \mathbb{Z}[\omega] \supseteq M.$$

$1^V = 1/2$ and $\left(\sqrt{-3}\right)^V = \sqrt{-3}/6$.

Proof. Want that $M^V \subseteq V$ is a lattice. Let $e_1, \dots, e_n$ be a $\mathbb{Z}$-basis of M, so a $\mathbb{Q}$-basis of V. Given $\langle , \rangle : V \times V \to \mathbb{Q}$ define $e_1^V, \dots, e_n^V$ to be the dual basis to $e_1, \dots, e_n$,

$$\left\langle e_i, e_j^V \right\rangle = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}.$$

Claim that $e_1^V, \dots, e_n^V$ is a $\mathbb{Z}$-basis for M^V.

- $e_1^V, \dots, e_n^V$ are $\mathbb{Z}$-linearly independent because $\mathbb{Q}$-linearly independent.

  $$w = a_1 e_1^V + \cdots + a_n e_n^V = 0, \qquad a_i \in \mathbb{Z} \subseteq \mathbb{Q},$$

  so $a_i = \langle e_i, w \rangle = 0$.
- $e_i^V \in M^V$, by using definition of M^V. Want $\left\langle v, e_i^V \right\rangle \in \mathbb{Z}$ for all $v \in M$. $v \in M$, so

  $$v = b_1 e_1 + \cdots + b_n e_n, \qquad b_i \in \mathbb{Z},$$

  so $\left\langle v, e_i^V \right\rangle = b_i \in \mathbb{Z}$.
- For all $w \in M^V \subseteq V$,

  $$w = c_1 e_1^V + \cdots + c_n e_n^V, \qquad c_i \in \mathbb{Z}.$$

  Can do this with $c_i \in \mathbb{Q}$ for $i = 1, \dots, n$. Need to show they are in $\mathbb{Z}$. Have $\langle e_i, w \rangle = c_i$ and $w \in M^V$, so $c_i \in \mathbb{Z}$.

□

2.8 $\mathcal{O}_K$ is a lattice

Theorem 2.8.1. *Let $K/\mathbb{Q}$ be a number field of degree n, with ring of integers $\mathcal{O}_K$. Then $\mathcal{O}_K$ is a lattice in K.*

Proof. The idea is

1. find lattice $M \subseteq \mathcal{O}_K$, and
2. show $M^V \supseteq \mathcal{O}_K$, the dual with respect to $Tr_{K/\mathbb{Q}}(,)$.

By structure theorem,

$$M^V \supseteq \mathcal{O}_K \supseteq M,$$

so

$$rk(M) \leq rk(\mathcal{O}_K) \leq rk\left(M^V\right).$$

1. We can find n $\mathbb{Q}$-linearly independent algebraic numbers $e_1, \ldots, e_n \in K$, because $\dim_{\mathbb{Q}}(K) = n$, so any $\mathbb{Q}$-basis of K will work. e_i is an algebraic number, but may not be an algebraic integer.

   $$e_i^n + \alpha_1 e_i^{n-1} + \cdots + \alpha_{n-1} = 0, \qquad \alpha_1, \ldots, \alpha_{n-1} \in \mathbb{Q}.$$

   Multiply equation by n-th power A^n of denominators of α_i. Let $e_i' = Ae_i$, so

   $$(Ae_i)^n + (A\alpha_1)(Ae_i)^{n-1} + \cdots + (A^n\alpha_{n-1}) = 0, \qquad A\alpha_1, \ldots, A^n\alpha_{n-1} \in \mathbb{Z}.$$

   Can assume $e_i \in \mathcal{O}_K$, that is algebraic integers. Let $M \subseteq \mathcal{O}_K$ be the $\mathbb{Z}$-span of $e_1, \ldots, e_n$.

2. $M^V \subseteq K$ is a lattice by Proposition 2.7.3. Show that $\alpha \in \mathcal{O}_K \subseteq M^V$. For all $\beta \in M$, $Tr_{K/\mathbb{Q}}(\beta, \alpha) = Tr_{K/\mathbb{Q}}(\alpha \cdot \beta) \in \mathbb{Z}$, since we know $\alpha \cdot \beta \in \mathcal{O}_K$ and $Tr_{K/\mathbb{Q}}\big|_{\mathcal{O}_K} : \mathcal{O}_K \to \mathbb{Z} \subset \mathbb{Q}$.

□

3 Dedekind domains

Lecture 17
Monday
18/02/19

The goal is to discuss Dedekind domains. A number field $K/\mathbb{Q}$ gives the ring of integers $\mathcal{O}_K$, which is not usually a UFD.

- We will show that unique factorisation of ideals holds in Dedekind domains and $\mathcal{O}_K$ is a Dedekind domain.
- We will introduce the ideal class group, which measures how far $\mathcal{O}_K$ is from being a PID or UFD.

3.1 Dedekind domains

Recall that $\mathfrak{m} \subsetneq R$ is a maximal ideal if for all $\mathfrak{m} \subseteq \mathfrak{n} \subseteq R$ either $\mathfrak{n} = \mathfrak{m}$ or $\mathfrak{n} = R$.

Definition 3.1.1. A ring R is called a **Dedekind domain** if R is an integrally closed Noetherian domain and every non-zero proper prime ideal of R is a maximal ideal.

Proposition 3.1.2. *If R is a PID, then R is a Dedekind domain.*

Lemma 3.1.3. *An element $a \in R \setminus \{0\}$ is irreducible if and only if $\langle a \rangle$ is a maximal ideal among principal ideals.*

Proof. $a = bc$ is irreducible if and only if

$$\begin{cases} b \in R^\times,\ a \mid c \\ c \in R^\times,\ a \mid b \end{cases} \iff \begin{cases} \langle b \rangle = R,\ \langle c \rangle = \langle a \rangle \\ \langle c \rangle = R,\ \langle b \rangle = \langle a \rangle \end{cases}.$$

$\implies$ Assume $\langle a \rangle \subseteq \langle b \rangle \subseteq R$. $b \mid a$, so $b \in R^\times$, so $\langle b \rangle = R$, or $a \mid b$, so $\langle b \rangle = \langle a \rangle$. Thus a is irreducible.

$\impliedby$ Assume $a = bc$. $b \mid a$, so $R \supseteq \langle b \rangle \supseteq \langle a \rangle$, so either $\langle b \rangle = R$ if and only if $b \in R^\times$, or $\langle b \rangle = \langle a \rangle$ if and only if $a \mid b$ and $c \in R^\times$.

□

Proof of Proposition 3.1.2. R is a PID implies that R is an integrally closed Noetherian domain. Let $a \in R \setminus \{0\}$ be such that $\langle a \rangle$ is prime, if and only if a is prime, so a is irreducible. Lemma 3.1.3 implies that $\langle a \rangle$ is maximal. □

Example.

- $\mathbb{Z}, \mathbb{Z}[i], \mathbb{Z}[\sqrt{2}], \mathbb{Z}[\omega]$ are PIDs.
- $\mathbb{Z}[\sqrt{-3}]$ is not a Dedekind domain because it is not integrally closed.
- $\mathbb{Z}[\sqrt{-5}], \mathbb{Q}[x]$ are Dedekind domains.
- $\mathbb{Z}[x]$ is not a Dedekind domain, since $0 \subsetneq \langle x \rangle \subsetneq \langle 2, x \rangle$ are prime but $\langle x \rangle$ is not zero or maximal.

3.2 Ideal norms

Definition 3.2.1. Let K be a number field, with ring of integers $\mathcal{O}_K$ and a prime ideal $0 \neq \mathfrak{n} \subseteq \mathcal{O}_K$. Then $\mathcal{O}_K/\mathfrak{n}$ is finite and define $Nm(\mathfrak{n}) = \#\mathcal{O}_K/\mathfrak{n}$.

If $0 \neq a \in \mathfrak{n} \cap \mathbb{Z}$, then $\mathfrak{n} \supseteq \langle a \rangle$ and

$$\frac{\mathcal{O}_K}{\langle a \rangle} = \left(\frac{\mathbb{Z}}{a\mathbb{Z}}\right)^{\deg(K/\mathbb{Q})}$$

is finite, so $\mathcal{O}_K/\langle a \rangle \twoheadrightarrow \mathcal{O}_K/\mathfrak{n}$ and

$$\#\frac{\mathcal{O}_K}{\mathfrak{n}} \leq \#\frac{\mathcal{O}_K}{\langle a \rangle}$$

is finite.

Example.

- Let $\langle p\rangle \subsetneq \mathbb{Z}$ for p prime. Then
$$Nm\left(\langle p\rangle\right) = \#\frac{\mathbb{Z}}{\langle p\rangle} = \#\frac{\mathbb{Z}}{p\mathbb{Z}} = p.$$
- Let $a \in \mathbb{Z} \hookrightarrow \mathcal{O}_K$. Then
$$Nm\left(\langle a\rangle\right) = \#\frac{\mathcal{O}_K}{\langle a\rangle} = a^{\deg(K/\mathbb{Q})} = Nm_{K/\mathbb{Q}}\left(a\right).$$
If $x \in \mathcal{O}_K$, then $Nm\left(\langle x\rangle\right) = Nm_{K/\mathbb{Q}}\left(x\right)$.
- Let $\mathcal{O}_K = \mathbb{Z}\left[\sqrt{-5}\right] \supsetneq \left\langle 2, 1+\sqrt{-5}\right\rangle$. Then $Nm\left(\left\langle 2, 1+\sqrt{-5}\right\rangle\right) = 2$.
  - $$\frac{\mathcal{O}_K}{\left\langle 2, 1+\sqrt{-5}\right\rangle} = \frac{\mathbb{Z}\left[x\right]}{\left\langle x^2+5, 2, 1+x\right\rangle} = \frac{\mathbb{Z}}{2\mathbb{Z}},$$
  - Alternatively, use structure theorem of finitely generated abelian groups. Have (e_1, e_2) a basis for $\mathcal{O}_K$ over $\mathbb{Z}$ and $a_1, a_2 \in \mathbb{Z}\setminus\{0\}$ such that $a_1 \mid a_2$ and (a_1e_1, a_2e_2) a basis for $\left\langle 2, 1+\sqrt{-5}\right\rangle$.
    - $\mathcal{O}_K$ is generated by $1+\sqrt{-5}, 1$, and
    - $\left\langle 2, 1+\sqrt{-5}\right\rangle$ is generated by $1+\sqrt{-5}, 2$,

    so $a_1 = 1$ and $a_2 = 2$. Thus $Nm\left(\left\langle 2, 1+\sqrt{-5}\right\rangle\right) = a_1 \cdot a_2$.
  - Alternatively, in the standard basis of $\mathcal{O}_K$, where $e_1 = 1$ and $e_2 = \sqrt{-5}$,
    $$\left\langle 2, 1+\sqrt{-5}\right\rangle = \begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix} \cdot \mathcal{O}_K.$$
    Then
    $$Nm\left(\left\langle 2, 1+\sqrt{-5}\right\rangle\right) = \left|\det\begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix}\right|$$
    is the absolute value of the determinant.

Lecture 18
Tuesday
19/02/19

Remark. $Nm\left(\mathfrak{n}\right) \in \mathfrak{n}$ because $Nm\left(\mathfrak{n}\right)$ in $\mathcal{O}_K/\mathfrak{n}$ is equal to zero, because the order of a finite group is always equal to zero in that finite group.

3.3 $\mathcal{O}_K$ is a Dedekind domain

The goal is to show that $\mathcal{O}_K$ is a Dedekind domain, that is it is an integrally closed Noetherian domain and non-zero prime ideals are maximal ideals. It is an integrally closed domain.

Proposition 3.3.1. *The ring of integers $\mathcal{O}_K$ in a number field K is Noetherian.*

Proof. Assume that
$$\mathfrak{a}_1 \subseteq \cdots \subseteq \mathfrak{a}_n \subseteq \ldots$$
is an ascending sequence of ideals in $\mathcal{O}_K$.
$$Nm\left(\mathfrak{a}_1\right) \geq \cdots \geq Nm\left(\mathfrak{a}_n\right) \geq \ldots,$$
since
$$\mathcal{O}_K/\mathfrak{a}_1 \twoheadrightarrow \cdots \twoheadrightarrow \mathcal{O}_K/\mathfrak{a}_n \twoheadrightarrow \ldots.$$
This must stabilise, so
$$Nm\left(\mathfrak{a}_n\right) = Nm\left(\mathfrak{a}_{n+1}\right) = \ldots.$$
$\mathfrak{a}_n \subseteq \mathfrak{a}_{n+1}$, so $\mathcal{O}_K/\mathfrak{a}_n \twoheadrightarrow \mathcal{O}_K/\mathfrak{a}_{n+1}$. Equality of norms implies that this must be a bijection, so $\mathfrak{a}_n = \mathfrak{a}_{n+1}$. (Exercise: $\mathfrak{a} \subseteq \mathfrak{b} \subseteq \mathcal{O}_K$ such that $Nm\left(\mathfrak{a}\right) = Nm\left(\mathfrak{b}\right)$ implies that $\mathfrak{a} = \mathfrak{b}$) □

Lemma 3.3.2. *Let R be an integral domain which is also a finite set. Then R is a field.*

Proof. Let $x \in R \setminus \{0\}$. Look at $x, x^2, \ldots$. Since R is finite, we must have $x^n = x^m$ for some $n, m \in \mathbb{Z}_{\geq 1}$. If $n > m$ then $x^{n-m} = 1$, so $x \in R^\times$. Thus R is a field. Alternatively,

$$\begin{array}{ccc} R & \longrightarrow & R \\ y & \longmapsto & x \cdot y \end{array}$$

is injective because R is an integral domain and bijective because R is a finite set. □

Lemma 3.3.3. *Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$. Then $\mathfrak{p}$ must be a maximal ideal.*

Proof. $\mathcal{O}_K/\mathfrak{p}$ is an integral domain and a finite set of cardinality $Nm(\mathfrak{p})$. □

Remark. Let $\mathfrak{p} \neq 0$ be a prime ideal of $\mathcal{O}_K$. Then $Nm(\mathfrak{p}) = p^r$ for some $p \in \mathbb{Z}$ prime and $r \in \mathbb{Z}_{\geq 1}$ because of the classification of finite fields.

Remark.

$$\ldots \subset \{\text{PIDs}\} \begin{array}{c} \subset \\ \\ \subset \end{array} \begin{array}{c} \{\text{UFDs}\} \\ \neq \\ \{\text{Dedekind domains}\} \end{array} \begin{array}{c} \subset \\ \\ \subset \end{array} \{\text{integrally closed domains}\} \subset \{\text{IDs}\} \subset \ldots .$$

- $\mathbb{Z}\left[\sqrt{-5}\right]$ is a Dedekind domain but not a UFD.
- $\mathbb{Z}[x]$ is a UFD but not a Dedekind domain.

3.4 Properties of ideal norms

Proposition 3.4.1. *Let $I \subseteq J \subseteq \mathcal{O}_K$ be a sequence of ideals. Then $Nm(J) \mid Nm(I)$.*

Proof. Let $\phi : \mathcal{O}_K/I \twoheadrightarrow \mathcal{O}_K/J$ be a ring homomorphism. Then

$$\frac{\frac{\mathcal{O}_K}{I}}{Ker(\phi)} \cong \frac{\mathcal{O}_K}{J},$$

so

$$Nm(I) = Nm(J) \cdot \#Ker(\phi).$$

Thus $Nm(J) \mid Nm(I)$. □

Example. Show that the ideals $I = \left\langle 11, 3 + \sqrt{31} \right\rangle$ and $J = \left\langle 6, 1 + \sqrt{31} \right\rangle$ in $\mathbb{Z}\left[\sqrt{31}\right]$ are relatively prime, that is $I + J = \mathbb{Z}\left[\sqrt{31}\right]$, if and only if $Nm(I + J) = 1$.

$$Nm(I) = \left|\det \begin{pmatrix} 11 & 0 \\ 3 & 1 \end{pmatrix}\right| = 11, \qquad Nm(I) = \left|\det \begin{pmatrix} 6 & 0 \\ 1 & 1 \end{pmatrix}\right| = 6.$$

$I \subset I+J$, so $Nm(I + J) \mid Nm(I) = 11$, and $J \subset I+J$, so $Nm(I + J) \mid Nm(J) = 6$. Thus $Nm(I + J) = 1$.

Let $a \in \mathcal{O}_K$. Structure theorem of finite generated abelian groups implies that if $e_1, \ldots, e_n$ is a basis for $\mathcal{O}_K$, where $n = \deg(K/\mathbb{Q})$, then $a_1 e_1, \ldots, a_n e_n$ is a basis for $\langle a \rangle$. Then

$$\frac{\mathcal{O}_K}{\langle a \rangle} = \frac{\mathbb{Z}}{a_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{a_n\mathbb{Z}},$$

so

$$Nm(\langle a \rangle) = a_1 \cdot \cdots \cdot a_n = \det(a) = Nm_{K/\mathbb{Q}}(a).$$

Lecture 19 is a problem class.

Lecture 19
Friday
22/02/19

3.5 Fractional ideals

Lecture 20
Monday
25/02/19

The goal is to show that unique factorisation of ideals into prime ideals always holds in a Dedekind domain.

Definition 3.5.1. Let R be an integral domain, with fraction field K. A **fractional ideal** $\mathfrak{n}$ of R is an R-submodule of K, that is

- an additive subgroup, so $x \in \mathfrak{n}$ and $y \in \mathfrak{n}$ implies that $x + y \in \mathfrak{n}$, and
- stable under multiplication by R, so $x \in \mathfrak{n}$ and $r \in R$ implies that $rx \in \mathfrak{n}$,

such that there exists $a \in R$ such that $a\mathfrak{n} = \{ax \mid x \in \mathfrak{n}\} \subseteq R$.

Example.

- Any ideal of R is also a fractional ideal with $a = 1$. Conversely, if $\mathfrak{n}$ is a fractional ideal and $\mathfrak{n} \subseteq R$, then $\mathfrak{n}$ is an integral ideal.
- Let $R = \mathbb{Z} \hookrightarrow \mathbb{Q}$. Then the fractional ideals of $\mathbb{Q}$ are $\frac{p}{q} \cdot \mathbb{Z}$ for $p, q \in \mathbb{Z}$ and $q \neq 0$. $\mathbb{Q}$ is not a fractional ideal, but it is a $\mathbb{Z}$-module.

We can multiply fractional ideals of R by

$$\mathfrak{m} \cdot \mathfrak{n} = \left\{ \sum_{i=1}^{k} x_i \cdot y_i \;\middle|\; x_i \in \mathfrak{m},\ y_i \in \mathfrak{n},\ k \in \mathbb{Z}_{\geq 0} \right\}.$$

Lemma 3.5.2. *If $\mathfrak{m}, \mathfrak{n}$ are fractional ideals of R then $\mathfrak{m} \cdot \mathfrak{n}$ is also a fractional ideal of R.*

Proof. $\mathfrak{m} \cdot \mathfrak{n}$ is additive. $\mathfrak{m} \cdot \mathfrak{n}$ is stable under multiplication by $r \in R$, since

$$r \left(\sum_{i=1}^{k} x_i \cdot y_i \right) = \sum_{i=1}^{k} r x_i \cdot y_i \in \mathfrak{m} \cdot \mathfrak{n}.$$

There exists $a, b \in R$ such that $a\mathfrak{m} \subseteq R$ and $b\mathfrak{n} \subseteq R$, so $ab \cdot \mathfrak{m} \cdot \mathfrak{n} \subseteq R$. □

Multiplication of fractional ideals is commutative, so $\mathfrak{m} \cdot \mathfrak{n} = \mathfrak{n} \cdot \mathfrak{m}$, is associative, and has unit $R \cdot \mathfrak{m} = \mathfrak{m} \cdot R = \mathfrak{m}$. If R is a Dedekind domain, we will show that every fractional ideal has a multiplicative inverse, that is given a fractional ideal $\mathfrak{m}$ of R, there exists a fractional ideal $\mathfrak{m}^{-1}$ of R such that $\mathfrak{m} \cdot \mathfrak{m}^{-1} = R$.

Example. $\mathbb{Z}[x]$ is not a Dedekind domain, since $\langle 2, x \rangle$ does not have an inverse with respect to multiplication.

Theorem 3.5.3. *Let R be a Dedekind domain. The set of non-zero fractional ideals of R forms a commutative group under multiplication.*

To prove Theorem 3.5.3, need some preliminary results.

Lemma 3.5.4. *Let $\mathfrak{p} \subsetneq R$ be a prime ideal in an integral domain. Assume $\mathfrak{p} \supseteq \mathfrak{a}_1\mathfrak{a}_2$ for ideals $\mathfrak{a}_1, \mathfrak{a}_2 \subseteq R$. Then $\mathfrak{p} \supseteq \mathfrak{a}_1$ or $\mathfrak{p} \supseteq \mathfrak{a}_2$.*

Proof. If $\mathfrak{p} \not\supseteq \mathfrak{a}_1$ there exists $x \in \mathfrak{a}_1 \setminus \mathfrak{p}$, so $x\mathfrak{a}_2 \subseteq \mathfrak{p}$. Let $y \in \mathfrak{a}_2$. Then $xy \in \mathfrak{p}$ and $x \notin \mathfrak{p}$, so $y \in \mathfrak{p}$, since $\mathfrak{p}$ is prime, so $\mathfrak{a}_2 \subseteq \mathfrak{p}$. □

Remark. Same Lemma 3.5.4 holds if $\mathfrak{p} \supseteq \mathfrak{a}_1, \ldots, \mathfrak{a}_n$ for $n \in \mathbb{Z}_{\geq 1}$ then $\mathfrak{p} \supseteq \mathfrak{a}_i$ for some i.

Lemma 3.5.5. *If $I \subseteq R$ is a non-zero ideal of a Noetherian domain, there exists $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \subseteq R$ non-zero prime ideals not necessarily distinct, such that $I \supseteq \mathfrak{p}_1 \ldots \mathfrak{p}_n$ for some finite $n \in \mathbb{Z}$.*

Proof. Assume Lemma 3.5.5 is false. Choose I for which condition in Lemma 3.5.5 fails and such that I is maximal with respect to inclusion, that is for all $J \supseteq I$, J satisfies the condition. I is not prime, otherwise it would satisfy the condition. There exists $a, b \in R$ such that $a \notin I$ and $b \notin I$ but $ab \in I$. Look at $I \subsetneq I + bR$ and $I \subsetneq I + aR$, both satisfying the condition. Let $I + bR \supseteq \mathfrak{p}_1 \dots \mathfrak{p}_r$ and $I + aR \supseteq \mathfrak{q}_1 \dots \mathfrak{q}_s$. Thus

$$\mathfrak{p}_1 \dots \mathfrak{p}_r \cdot \mathfrak{q}_1 \dots \mathfrak{q}_s \subseteq (I + bR) \cdot (I + aR) \subseteq I.$$

□

Proposition 3.5.6. *Let R be a Dedekind domain. Let $\mathfrak{m} \subsetneq R$ be a non-zero prime ideal, if and only if maximal ideal of R. Define*

$$\mathfrak{m}^{-1} = \{a \in K \mid a\mathfrak{m} \subseteq R\}.$$

Then $\mathfrak{m}^{-1}$ is a fractional ideal of R and $\mathfrak{m} \cdot \mathfrak{m}^{-1} = R$.

Lecture 21
Tuesday
26/02/19

Proof. $\mathfrak{m}^{-1}$ is a fractional ideal.

- $\mathfrak{m}^{-1}$ is an additive subgroup of K, since $x, y \in \mathfrak{m}^{-1}$ implies that $x \cdot \mathfrak{m}, y \cdot \mathfrak{m} \subseteq R$, so $(x + y)\mathfrak{m} \subseteq x\mathfrak{m} + y\mathfrak{m} \subseteq R$, so $x + y \in \mathfrak{m}^{-1}$.
- $\mathfrak{m}^{-1}$ is stable under multiplication by R, since $x \in \mathfrak{m}^{-1}$ implies that $x \cdot \mathfrak{m} \subseteq R$, so $rx \cdot \mathfrak{m} \subseteq R$, so $rx \in \mathfrak{m}^{-1}$.
- Let $a \in \mathfrak{m}$ such that $a \neq 0$. Then $a\mathfrak{m}^{-1} \subseteq R$ by definition of $\mathfrak{m}^{-1}$.

$\mathfrak{m} = \mathfrak{m} \cdot 1 \subseteq \mathfrak{m} \cdot \mathfrak{m}^{-1} \subseteq R$ is automatic by definition. Since $\mathfrak{m}$ is maximal, either $\mathfrak{m} = \mathfrak{m} \cdot \mathfrak{m}^{-1}$ or $\mathfrak{m} \cdot \mathfrak{m}^{-1} = R$. Assume $\mathfrak{m} = \mathfrak{m} \cdot \mathfrak{m}^{-1}$ and get a contradiction. Take $x \in \mathfrak{m}^{-1}$.

$$\dots \subseteq x^n \cdot \mathfrak{m} \subseteq \dots \subseteq x \cdot \mathfrak{m} \subseteq \mathfrak{m} \subsetneq R,$$

so $x^n \in \mathfrak{m}^{-1}$ for all $n \in \mathbb{Z}_{\geq 1}$. Let $R[x]$ be the subring of K generated by x, so $R[x] \subseteq \mathfrak{m}^{-1}$. Let $a \in R \setminus \{0\}$ be such that $a\mathfrak{m}^{-1} \subseteq R$. In particular $aR[x] \subseteq R$ is an integral ideal of R. R is Noetherian, so $aR[x]$ is generated over R by finitely many elements $y_1, \dots, y_k \in R$. $x \cdot y_i \in aR[x]$, so

$$x \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_k \end{pmatrix} = A \begin{pmatrix} y_1 \\ \vdots \\ y_k \end{pmatrix}, \qquad A = \begin{pmatrix} a_{11} & \dots & a_{1k} \\ \vdots & \ddots & \vdots \\ a_{k1} & \dots & a_{kk} \end{pmatrix} \in M_k(R),$$

a $k \times k$ matrix, so x is an eigenvalue of A with eigenvector $(y_1, \dots, y_k)^t$. Thus x is a root of $\det(tI_k - A)$, so x is integral over R. All $x \in \mathfrak{m}^{-1}$ satisfy $x \in R$ because R is integrally closed, so $\mathfrak{m}^{-1} = R$. Choose $a \in \mathfrak{m} \setminus \{0\}$. Then

$$\mathfrak{m} \supsetneq \langle a \rangle \supseteq \mathfrak{p}_1 \cdot \dots \cdot \mathfrak{p}_k,$$

where $\mathfrak{p}_i$ are prime, by Lemma 3.5.5. Lemma 3.5.4 from last time implies that $\mathfrak{m}$ must contain $\mathfrak{p}_i$ for some $i = 1, \dots, k$. Assume $\mathfrak{m} \supseteq \mathfrak{p}_1 \neq 0$, so $\mathfrak{m} = \mathfrak{p}_1$. Choose k such that it is minimal among all possible $\mathfrak{p}_1 \cdot \dots \cdot \mathfrak{p}_k$ contained in $\langle a \rangle$, so $\mathfrak{p}_2 \cdot \dots \cdot \mathfrak{p}_k \nsubseteq \langle a \rangle$, since $\mathfrak{p}_2 \cdot \dots \cdot \mathfrak{p}_k$ has length $k - 1$. Choose $0 \neq b \in \mathfrak{p}_2 \cdot \dots \mathfrak{p}_k \setminus \langle a \rangle$. Then $b/a \in K$ such that

1. $b/a \in R$, and
2. $b/a \in \mathfrak{m}^{-1}$

is a contradiction.

1. $b \in aR = \langle a \rangle$ is false, so $b/a \notin R$.
2. $b/a \in \mathfrak{m}^{-1}$ if $b/a \cdot \mathfrak{m} \subseteq R$, or equivalently

$$b \cdot \mathfrak{m} \in \mathfrak{p}_1 \cdot \dots \cdot \mathfrak{p}_k \subseteq \langle a \rangle.$$

$\mathfrak{m}^{-1} \neq R$, so $\mathfrak{m} \cdot \mathfrak{m}^{-1} \neq \mathfrak{m}$, so $\mathfrak{m} \cdot \mathfrak{m}^{-1} = R$, which is done. □

3.6 Unique factorisation of ideals

Theorem 3.6.1 (Unique factorisation of ideals)**.**

1. *Any non-zero fractional ideal I of R can be written as*
$$I = \mathfrak{p}_1^{k_1} \cdot \cdots \cdot \mathfrak{p}_r^{k_r}, \qquad k_i \in \mathbb{Z} \setminus \{0\},$$
where $\mathfrak{p}_1$ are non-zero prime ideals.
2. *This factorisation is unique up to order of the $\mathfrak{p}_i$.*

Remark. Given I,
$$I^{-1} = \mathfrak{p}_1^{-k_1} \cdot \cdots \cdot \mathfrak{p}_r^{-k_r}.$$
Get $I \cdot I^{-1} = R$, so any non-zero fractional ideal has a multiplicative inverse.

Proof.

1. There exists $a \in R \setminus \{0\}$ such that $aI \subseteq R$ is an integral ideal so we may assume I is an integral ideal. Assume Theorem 3.6.1 is false. Because R is Noetherian, there exists I such that I does not admit a factorisation and I is maximal with this property. Let $\mathfrak{m} \supseteq I$ be a maximal ideal. Then $J = \mathfrak{m}^{-1} \cdot I \subseteq R$, so J is an integral ideal. J admits a factorisation because
$$\mathfrak{m}^{-1} \cdot I = J \supsetneq I = 1 \cdot I,$$
since if $\mathfrak{m}^{-1} \cdot I = I$, argue as in proof of Proposition 3.5.6. Thus $I = \mathfrak{m} \cdot J$, a contradiction.
2. Let
$$\mathfrak{p}_1^{k_1} \cdot \cdots \cdot \mathfrak{p}_r^{k_r} = \mathfrak{q}_1^{k_1} \cdot \cdots \cdot \mathfrak{q}_r^{k_r}.$$
We may assume all $k_i, l_j > 0$. $\mathfrak{p}_1 \supseteq \mathfrak{q}_1^{l_1} \cdot \cdots \cdot \mathfrak{q}_s^{l_s}$, so $\mathfrak{p}_1 \supseteq \mathfrak{q}_1$. Both maximal, so $\mathfrak{p}_1 = \mathfrak{q}_1$.

□

Lecture 22
Friday
01/03/19

3.7 Ideal class groups

Definition 3.7.1. Let R be a Dedekind domain. The **ideal class group** of R is the quotient of the group of all non-zero fractional ideals by the subgroup of principal fractional ideals. This is denoted by $Cl(R)$.

If K is a number field, then $\mathcal{O}_K$ is a Dedekind domain and $Cl(K) = \mathcal{O}_K$.

Example.

- $Cl(K) = 1$ if $\mathcal{O}_K$ is a PID or UFD. For example if $K = \mathbb{Q}(i), \mathbb{Q}(\omega), \mathbb{Q}\left(\sqrt{-11}\right)$.
- $Cl(K) \neq 1$ if $K = \mathbb{Q}\left(\sqrt{-5}\right), \mathbb{Q}\left(\sqrt{-6}\right)$. $\left\langle 2, 1+\sqrt{-5}\right\rangle$ is not principal, and
$$\left\langle 2, 1+\sqrt{-5}\right\rangle^2 = \left\langle 4, 2+2\sqrt{-5}, -4+2\sqrt{-5}\right\rangle = \langle 2\rangle,$$
so $\mathbb{Z}/2\mathbb{Z}$ is a subgroup of $Cl(K)$. Claim that $\mathbb{Z}/2\mathbb{Z} \cong Cl(K)$. For example,
$$\left\langle 3, 1-\sqrt{-5}\right\rangle = \langle a\rangle \cdot \left\langle 2, 1+\sqrt{-5}\right\rangle, \qquad a = \tfrac{1-\sqrt{-5}}{2} \in \mathbb{Q}\left(\sqrt{-5}\right)^{\times},$$
because
  - $\left(1+\sqrt{-5}\right)a = \left(1+\sqrt{-5}\right)\left(1-\sqrt{-5}\right)/2 = 3$, and
  - $2a = 1-\sqrt{-5}$.

Theorem 3.7.2. *If K is a number field, then $Cl(K)$ is finite.*

Proof relies on an explicit bound. Every **ideal class**, a fractional ideal of $\mathcal{O}_K$ up to multiplication by principal ideals, contains a representative of norm less than an explicit bound depending on K.

4 Finiteness of ideal class groups

4.1 Discriminants

Let K be a number field. Recall $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $n = \deg(K/\mathbb{Q})$. Choose $e_1, \ldots, e_n$, a $\mathbb{Z}$-basis of $\mathbb{Q}$.

$$\begin{array}{rccc} Tr_{K/\mathbb{Q}}(,) & : & K \times K & \longrightarrow & \mathbb{Q} \\ & & (v,w) & \longmapsto & Tr_{K/\mathbb{Q}}(v \cdot w) \end{array}$$

is symmetric, $\mathbb{Q}$-bilinear, and non-degenerate. The **discriminant** of K is

$$Disc(K) = \det\left(Tr_{K/\mathbb{Q}}(e_i, e_j)_{i,j=1,\ldots,n}\right).$$

Remark. $Disc(K) \neq 0$ and $Disc(K) \in \mathbb{Z}$.

Lemma 4.1.1. *$Disc(K)$ is independent of choice of $\mathbb{Z}$-basis $e_1, \ldots, e_n$.*

Proof. If $f_1, \ldots, f_n$ is another $\mathbb{Z}$-basis, there exists $A \in M_n(\mathbb{Z})$ such that

$$A \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = \begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix}.$$

$\det(A) = \pm 1$ and

$$A^t \cdot \left(Tr_{K/\mathbb{Q}}(e_i, e_j)_{i,j}\right) \cdot A = \left(Tr_{K/\mathbb{Q}}(f_i, f_j)_{i,j}\right),$$

so

$$\det\left(Tr_{K/\mathbb{Q}}(e_i, e_j)_{i,j}\right) = \det\left(Tr_{K/\mathbb{Q}}(e_i, e_j)_{i,j}\right) \cdot (\det(A))^2 = \det\left(Tr_{K/\mathbb{Q}}(f_i, f_j)_{i,j}\right).$$

□

Example. Let $K/\mathbb{Q}$ be quadratic, so $K = \mathbb{Q}\left(\sqrt{d}\right)$. Then

$$Disc(K) = \begin{cases} 4d & d \equiv 2,3 \mod 4,\ \mathcal{O}_K = \left\langle 1, \sqrt{d} \right\rangle \\ d & d \equiv 1 \mod 4,\ \mathcal{O}_K = \left\langle 1, \frac{1+\sqrt{d}}{2} \right\rangle \end{cases},$$

since

$$\begin{pmatrix} Tr_{K/\mathbb{Q}}(1) & Tr_{K/\mathbb{Q}}\left(\sqrt{d}\right) \\ Tr_{K/\mathbb{Q}}\left(\sqrt{d}\right) & Tr_{K/\mathbb{Q}}(d) \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix}, \qquad \begin{pmatrix} Tr_{K/\mathbb{Q}}(1) & Tr_{K/\mathbb{Q}}\left(\frac{1+\sqrt{d}}{2}\right) \\ Tr_{K/\mathbb{Q}}\left(\frac{1+\sqrt{d}}{2}\right) & Tr_{K/\mathbb{Q}}\left(\frac{1+d+2\sqrt{d}}{4}\right) \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & \frac{d+1}{2} \end{pmatrix}.$$

4.2 Decomposition of primes in quadratic fields

Let $p \in \mathbb{Z}$ be a rational prime. How does $\langle p \rangle$ decompose, or factor, into prime ideals of $\mathcal{O}_K$?

- If $\mathcal{O}_K / \langle p \rangle \cong \mathbb{F}_p[x]/x^2$ we say $\langle p \rangle$ ramifies in $\mathcal{O}_K$. Then $\langle p \rangle = \mathfrak{p}^2$, where $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$.
- If $\mathcal{O}_K / \langle p \rangle \cong \mathbb{F}_p \times \mathbb{F}_p$ we say $\langle p \rangle$ splits in $\mathcal{O}_K$. Then $\langle p \rangle = \mathfrak{p}_1 \cdot \mathfrak{p}_2$, where $\mathfrak{p}_1 \neq \mathfrak{p}_2$ are distinct prime ideals of $\mathcal{O}_K$.
- If $\mathcal{O}_K / \langle p \rangle \cong \mathbb{F}_{p^2}$ we say $\langle p \rangle$ is inert in $\mathcal{O}_K$. Then $\langle p \rangle$ is a prime ideal of $\mathcal{O}_K$.

To see that these are the only possibilities when $K/\mathbb{Q}$ is quadratic, key observation is $\#(\mathcal{O}_K / \langle p \rangle) = p^2$, so $\mathcal{O}_K / \langle p \rangle$ is an $\mathbb{F}_p$-vector space of dimension two. The following is the criterion.

Lecture 23
Monday
04/03/19

- p is ramified if and only if $p \mid Disc(K)$. More precisely,
  - $p \mid 4d$ if $d \equiv 2, 3 \mod 4$, and
  - $p \mid d$ if $d \equiv 1 \mod 4$.
- If $d \equiv 1 \mod 4$, then 2 is
  - inert if $d \equiv 5 \mod 8$, and
  - split if $d \equiv 1 \mod 8$.
- If $p \neq 2$ and $p \nmid Disc(K)$, then p is
  - split if d is a quadratic residue mod p, and
  - inert if d is not a quadratic residue mod p.

  Choose standard basis $1, \delta$ of $\mathcal{O}_K$.

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

  Minimal polynomial equation of δ is

$$f(x) = \begin{cases} x^2 - d & d \equiv 2, 3 \mod 4 \\ x^2 - x - \frac{d-1}{4} & d \equiv 1 \mod 4 \end{cases}.$$

  Compute

$$\frac{\mathcal{O}_K}{\langle p \rangle} = \frac{\mathbb{Z}[x]}{\langle f(x), p \rangle} = \frac{\mathbb{F}_p[x]}{\langle f(x) \rangle}.$$

  p is inert if and only if $\mathbb{F}_p[x] / \langle f(x) \rangle \cong \mathbb{F}_{p^2}$, if and only if $f(x) = 0$.
  - If $d \equiv 2, 3 \mod 4$, then $x^2 - d = 0$ has no solutions if and only if d is not a quadratic residue mod p.
  - If $d \equiv 1 \mod 4$, then $x^2 - x - \frac{d-1}{4} = 0$ has no solutions if and only if d is not a quadratic residue mod p.

4.3 Standard form of ideals

The goal is that if K is an imaginary quadratic field, so $d < 0$, then $Cl(K)$ is finite. Use that every ideal class in $Cl(K)$ contains an integral ideal of norm less than explicit bound depending on K. Uses geometry of numbers and Minkowski's theorem. Let K be a quadratic field and $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\delta$ be the ring of integers, where

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

Proposition 4.3.1. *Let $I \subseteq \mathcal{O}_K$ be an integral ideal. There exists $a, b, d \in \mathbb{Z}$ such that the following hold.*

- $I = d(\mathbb{Z}a + \mathbb{Z}(-b + \delta))$.
- $a \mid Nm_{K/\mathbb{Q}}(-b + \delta)$.

Conversely, every subset of $\mathcal{O}_K$ of this form is an integral ideal. The expression

$$I = d(\mathbb{Z}a + \mathbb{Z}(-b + \delta))$$

is called the **standard form** of I.

Proof. Let K be imaginary quadratic. $\mathcal{O}_K$ is a lattice Λ_0 generated by $1, \delta$ in K. I is a lattice $\Lambda \subseteq \Lambda_0$. There exists $\gamma \in M_2(\mathbb{Z})$ such that $\Lambda = \gamma \cdot \Lambda_0$. Can assume

$$\gamma = \begin{pmatrix} a' & b' \\ 0 & d \end{pmatrix}, \qquad a', b', d \in \mathbb{Z}.$$

$I = \mathbb{Z}a' + \mathbb{Z}(b' + d\delta)$ is an ideal and $a' \in I$, so

$$a'\delta = a'b + (b' + d\delta)a \in I, \qquad a, b \in \mathbb{Z},$$

so

$$a'(\delta - b) = (b' + d\delta)a.$$

The coefficients of δ implies that $a' = da$, and the coefficients of 1 implies that $-a'b = ab'$, so $b' = -db$. Left to check that $a \mid Nm_{K/\mathbb{Q}}(-b + \delta)$. For simplicity assume $d = 1$. I is an ideal and $-b + \delta \in I$, so

$$\delta(-b + \delta) = af + (-b + \delta)e \in I, \qquad e, f \in \mathbb{Z},$$

so

$$(e - \delta)(-b + \delta) = -af \in \mathbb{Z}.$$

If $e - \delta = -b + \overline{\delta}$ the product would be

$$\left(-b + \overline{\delta}\right)(-b + \delta) = Nm_{K/\mathbb{Q}}(-b + \delta) = -af \in \mathbb{Z},$$

if and only if $a \mid Nm_{K/\mathbb{Q}}(-b + \delta)$. Conversely,

$$-af = (e - \delta)(-b + \delta) = \left(e - \delta + b - \overline{\delta} + \left(-b + \overline{\delta}\right)\right)(-b + \delta) = \left(e - \delta + b - \overline{\delta}\right)(-b + \delta) + Nm_{K/\mathbb{Q}}(-b + \delta).$$

Then

$$-af \in \mathbb{Z}, \qquad Nm_{K/\mathbb{Q}}(-b + \delta) \in \mathbb{Z}, \qquad e - \delta + b - \overline{\delta} \in \mathbb{Z}, \qquad -b + \delta \in \mathcal{O}_K \setminus \mathbb{Z},$$

so $e - \delta + b - \overline{\delta} = 0$. □

An observation is that if $I = d(\mathbb{Z}a + \mathbb{Z}(-b + \delta))$ is in standard form, $Nm(I) = d^2 \cdot a$, since

$$\det \begin{pmatrix} a & -b \\ 0 & 1 \end{pmatrix} = 0.$$

Lecture 24
Tuesday
05/03/19

Example. Let

$$I = \langle 2+i \rangle = (2+i)\,\mathbb{Z} + (2+i)\,i\mathbb{Z} = (2+i)\,\mathbb{Z} + (2i-1)\,\mathbb{Z} = \begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix} \cdot \mathbb{Z}[i] \subsetneq \mathbb{Z}[i].$$

Column-reducing,

$$\begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix} \sim \begin{pmatrix} 2 & -5 \\ 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 5 & 2 \\ 0 & 1 \end{pmatrix}.$$

Standard form is $I = 5\mathbb{Z} + (2+i)\,\mathbb{Z}$. (Exercise: check that $5 = Nm_{\mathbb{Z}[i]/\mathbb{Z}}(2+i)$)

Let K be an imaginary quadratic field and

$$J = q\,(\mathbb{Z}a + \mathbb{Z}\,(-b+\delta)) \subsetneq K, \qquad a, b \in \mathbb{Z}, \qquad q \in \mathbb{Q}^\times,$$

be a fractional ideal of $\mathcal{O}_K$. $Nm\,(J) = q^2 \cdot a$, by extending norm from ideals to fractional ideals multiplicatively. Standard form of J has fundamental parallelogram with vertices

$$0,\ qa,\ q\,(-b+\delta),\ qa + q\,(-b+\delta).$$

Let $A\,(J)$ be the area of the fundamental parallelogram of J.

Proposition 4.3.2.

$$A\,(J) = \frac{Nm\,(J) \cdot \sqrt{Disc\,(K)}}{2}.$$

Proof.

$$A\,(J) = qa \cdot q|\Im\,(\delta)| = q^2 \cdot a \cdot |\Im\,(\delta)| = \frac{q^2 \cdot a \cdot \sqrt{Disc\,(K)}}{2} = \frac{Nm\,(J) \cdot \sqrt{Disc\,(K)}}{2}.$$

□

4.4 Minkowski's theorem

If J is a fractional ideal of K, goal is to show that there exists $\alpha \in J$ such that $Nm\,(\alpha) < C_K \cdot Nm\,(J)$, where C_K is an explicit bound in terms of K, so $Nm\left(\alpha \cdot J^{-1}\right) < C_K$. Up to multiplication by a principal ideal, can get $Nm\left(J^{-1}\right) < C_K$. The idea is to use Minkowski's theorem. Have a lattice $\Lambda \subset \mathbb{R}^2$ and a nice region $S \subset \mathbb{R}^2$. Let $A\,(\Lambda)$ be the area of the fundamental parallelogram of Λ.

Theorem 4.4.1 (Minkowski's theorem)**.** *If $A\,(S) > 4A\,(\Lambda)$ then S contains a non-zero lattice point, that is $S \cap \Lambda \neq \emptyset$.*

S is **nice**

- if $x \in S$ then $-x \in S$, and
- S is convex, that is if $x, y \in S$ then the segment $[x, y] \subset S$.

Example. Let S be the closed or open disc of radius $r > 2/\sqrt{\pi}$ and $\Lambda = \mathbb{Z}[i] \subset \mathbb{C}$. Then $A\,(S) = \pi r^2 > 4 = 4A\,(\Lambda)$.

Proof. Consider all parallelograms of 2Λ that intersect S. Translate elements of 2Λ until they all overlap.

$$A\,(2\Lambda) = 4A\,(\Lambda) < A\,(S) = A\,(S_1) + \cdots + A\,(S_n).$$

There exists S_i, S_j for $i \neq j$ such that $S_i \cap S_j \neq \emptyset$ translated. There exists $x \in S \cap S_i$ and $y \in S \cap S_j$ for $i \neq j$ such that $x - y \in 2\Lambda$. Claim that $(x-y)/2 \in S \cap \Lambda$.

- $x - y \in 2\Lambda$, so $(x-y)/2 \in \Lambda$.
- $(x-y)/2 \in S$ because $y \in S$, so $-y \in S$, and $x \in S$, so $(x-y)/2 \in S$, which is the midpoint.

□

4.5 Minkowski bound for imaginary quadratic fields

Theorem 4.5.1. *Let K be an imaginary quadratic field. Then every ideal class in $Cl(K)$ contains a representative I such that I is an integral ideal of norm less than*

$$\frac{2\sqrt{Disc(K)}}{\pi}.$$

Proof. Back to $J = q(\mathbb{Z}a + \mathbb{Z}(-b+\delta))$ a fractional ideal of $\mathcal{O}_K$. Let S be the disc centred at the origin of radius

$$r = \sqrt{\frac{2\sqrt{Disc(K)} \cdot Nm(J)}{\pi}} + \epsilon.$$

Then

$$A(S) > \pi r^2 = 2\sqrt{Disc(K)} \cdot Nm(J) = 4A(J).$$

Minkowski implies that there exists $\alpha \in J$ such that $\alpha \neq 0$ and

$$Nm_{K/\mathbb{Q}}(\alpha) = |\alpha|^2 < \frac{2\sqrt{Disc(K)} \cdot Nm(J)}{\pi} + \epsilon.$$

Thus there exists $\alpha \in J$ such that

$$Nm_{K/\mathbb{Q}}(\alpha) < \frac{2\sqrt{Disc(K)}}{\pi} \cdot Nm(J).$$

□

(Exercise: prove $Cl\left(\mathbb{Q}\left(\sqrt{-5}\right)\right) = \mathbb{Z}/2\mathbb{Z}$)
Lecture 25 is a problem class.

Lecture 25
Friday
08/03/19

4.6 Minkowski bound for real quadratic fields

Let $K/\mathbb{Q}$ be a real quadratic field. The goal is that every ideal class in $Cl(K)$ contains a representative $I \subseteq \mathcal{O}_K$ such that $Nm(I) \leq \sqrt{Disc(K)}/2$. We will use Minkowski's theorem.

Lecture 26
Monday
11/03/19

Corollary 4.6.1. *If K is real quadratic, $Cl(K)$ is finite.*

If K is real quadratic and $J \subsetneq K$ is a fractional ideal, such as $\mathcal{O}_K$, then $J \subsetneq \mathbb{R}$ is a dense subset. We will use instead the embedding

$$\begin{array}{rccc} \iota & : & K & \longrightarrow & \mathbb{R}^2 \\ & & \alpha & \longmapsto & (\overline{\alpha}, \alpha) \end{array}.$$

Let

$$\alpha = a + b\sqrt{d}, \qquad \overline{\alpha} = a - b\sqrt{d}, \qquad a, b \in \mathbb{Q},$$

where $d \in \mathbb{Z}_{>0}$ is square-free, so

$$a + b\sqrt{d} \mapsto \left(a - b\sqrt{d}, a + b\sqrt{d}\right).$$

Lemma 4.6.2. *The image of a fractional ideal $J \subsetneq K$ under ι is a lattice in $\mathbb{R}^2$.*

Proof. J is a free $\mathbb{Z}$-module of rank two. Standard form is $J = q(a\mathbb{Z} + (-b+\delta)\mathbb{Z})$ for $q \in \mathbb{Q}^\times$, $a, b \in \mathbb{Z}$, and

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

$\iota(qa) = (qa, qa)$ and $\iota((-b+\delta)q) = \left(q\left(-b+\overline{\delta}\right), q(-b+\delta)\right)$ are linearly independent over $\mathbb{Z}$, since $\delta \notin \mathbb{Q}$, so $\overline{\delta} \neq \delta$, so $\iota(J)$ is the $\mathbb{Z}$-lattice spanned by (qa, qa) and $\left(q\left(-b+\overline{\delta}\right), q(-b+\delta)\right)$. □

Example. Let $K = \mathbb{Q}\left(\sqrt{5}\right)$. Then $\mathcal{O}_K \hookrightarrow \mathbb{R}^2$ is the lattice generated by $e_1 = (1,1)$ and $e_2 = \left(\frac{1-\sqrt{5}}{2}, \frac{1+\sqrt{5}}{2}\right)$.

$Nm(J) = q^2 a$ and $A(J)$ is the area of the fundamental parallelogram of J.

Proposition 4.6.3. *If $J = q(a\mathbb{Z} + (-b+\delta)\mathbb{Z})$ is an ideal in standard form, then*

$$A(J) = Nm(J) \cdot \sqrt{Disc(K)} = q^2 a \cdot \sqrt{Disc(K)}.$$

Proof. If $d \equiv 2,3 \mod 4$, then

$$\delta = \sqrt{d} = \frac{\sqrt{Disc(K)}}{2}, \qquad \overline{\delta} = -\sqrt{d} = -\frac{\sqrt{Disc(K)}}{2}.$$

If $d \equiv 1 \mod 4$, then

$$\delta = \frac{1+\sqrt{d}}{2} = \frac{1+\sqrt{Disc(K)}}{2}, \qquad \overline{\delta} = \frac{1-\sqrt{d}}{2} = \frac{1-\sqrt{Disc(K)}}{2}.$$

Component of $\left(q\left(-b+\overline{\delta}\right), q(-b+\delta)\right)$ along the line $x = -y$ is

$$\left(-q\frac{\sqrt{Disc(K)}}{2}, q\frac{\sqrt{Disc(K)}}{2}\right).$$

Component along $x = y$ is

$$\begin{cases} (-qb, -qb) & d \equiv 2,3 \mod 4 \\ \left(-qb+\frac{q}{2}, -qb+\frac{q}{2}\right) & d \equiv 1 \mod 4 \end{cases}.$$

Thus

$$A(J) = qa\sqrt{2} \cdot \frac{q\sqrt{Disc(K)}}{2} = q^2 a \cdot \sqrt{Disc(K)} = Nm(J) \cdot \sqrt{Disc(K)}.$$

□

Proposition 4.6.4. *If $J \subsetneq K$ is a fractional ideal then there exists $\alpha \in J$ such that*

$$Nm(\alpha) < \frac{\sqrt{Disc(K)} \cdot Nm(J)}{2}.$$

Corollary 4.6.5. *Every ideal class in $Cl(K)$ contains $I \subseteq \mathcal{O}_K$ such that*

$$Nm(I) < \frac{\sqrt{Disc(K)}}{2}.$$

Proof. Let $I = \alpha \cdot J^{-1}$. Then $I \subseteq \mathcal{O}_K$ is an integral ideal and $Nm(I) = Nm(\alpha) \cdot Nm(J)^{-1}$. Proposition 4.6.4 implies that $Nm(I) < \sqrt{Disc(K)}/2$. □

Proof of Proposition 4.6.4. Let

$$\begin{array}{ccc} K & \longrightarrow & \mathbb{R}^2 \\ \alpha & \longmapsto & (\overline{\alpha}, \alpha) \end{array}.$$

$Nm(\alpha) = \overline{\alpha} \cdot \alpha$ is the restriction of $Nm(x,y) = x \cdot y$. Let H be

$$|x \cdot y| < \frac{\sqrt{Disc(K)} \cdot Nm(J)}{2}.$$

If we chose S to be that, we could not apply Minkowski, since it is not convex. Let S be

$$|x+y| < \sqrt{2\sqrt{Disc(K)} \cdot Nm(J)}, \qquad |x-y| < \sqrt{2\sqrt{Disc(K)} \cdot Nm(J)}.$$

Then S is contained in H. Assume $x, y > 0$. $(x,y) \in S$, so $x + y < \sqrt{2\sqrt{Disc(K)} \cdot Nm(J)}$, so $4|x \cdot y| \leq (x+y)^2 < 2\sqrt{Disc(K)} \cdot Nm(J)$, because $(x-y)^2 \geq 0$. Thus $|x \cdot y| < \sqrt{Disc(K)} \cdot Nm(J)/2$, and

$$A(S) = 4\sqrt{Disc(K)} \cdot Nm(J) = 4A(J).$$

□

4.7 Computing ideal class groups

Lecture 27
Tuesday
12/03/19

Recall that Minkowski's theorem gives the following Minkowski bounds $\lambda(K)$.

- If K is an imaginary quadratic field then every ideal class in $Cl(K)$ contains a representative $I \subseteq \mathcal{O}_K$ with
$$Nm(I) < \frac{2\sqrt{|Disc(K)|}}{\pi}.$$
- If K is a real quadratic field then every ideal class in $Cl(K)$ contains a representative $I \subseteq \mathcal{O}_K$ with
$$Nm(I) < \frac{\sqrt{Disc(K)}}{2}.$$

Note. $\mathfrak{p} \subsetneq \mathcal{O}_K$, so
$$\overline{\mathfrak{p}} = \{\overline{a} \mid a \in \mathfrak{p}\} \subsetneq \mathcal{O}_K$$
is also a prime ideal, and
$$\mathfrak{p} \cdot \overline{\mathfrak{p}} = Nm(\mathfrak{p}) = Nm(\overline{\mathfrak{p}}),$$
so there exist at most two prime ideals with a given norm. Thus $Cl(K)$ is finite.

Example. Trivial class groups.

Example. $Cl\left(\mathbb{Q}\left(\sqrt{-5}\right)\right) \cong \mathbb{Z}/2\mathbb{Z}$.

Example. What is $Cl\left(\mathbb{Q}\left(\sqrt{-10}\right)\right)$?

- Minkowski bound is
$$\frac{2\sqrt{40}}{\pi} = \frac{4\sqrt{10}}{\pi} = \sqrt{\frac{160}{\pi^2}} < \sqrt{\frac{160}{9}} < \sqrt{18} < 5,$$
so every ideal class in $Cl\left(\mathbb{Q}\left(\sqrt{-10}\right)\right)$ contains a representative with norm at most four. Have to understand ideals $\mathfrak{p}$ such that $Nm(\mathfrak{p}) = p \in \mathbb{Z}$, for p a prime number. Remark that in general, only need to consider, and factor, primes $p < \lambda(K)$ and such that p is ramified or split in K.
- We want to factor $2, 3$ in K.
  - $2 \mid Disc(K) = 40$, so 2 ramifies. Then $2 = \mathfrak{p}^2$ for some $\mathfrak{p} \subsetneq \mathcal{O}_K$ prime ideal of norm two. Let
  $$\mathfrak{p} = d\left(a\mathbb{Z} + \left(-b + \sqrt{-10}\right)\mathbb{Z}\right), \qquad a, b, d \in \mathbb{Z}, \qquad a \mid Nm_{K/\mathbb{Q}}\left(-b + \sqrt{-10}\right)$$
  in standard form. $2 \in \mathfrak{p}$, so $ad \mid 2$.
    - $a = d = 1$ implies that $\mathcal{O}_K \neq \mathfrak{p}$.
    - $d = 2$ and $a = 1$ implies that $\langle 2 \rangle \neq \mathfrak{p}$.
    - $d = 1$ and $a = 2$ implies that $2 \mid Nm_{K/\mathbb{Q}}\left(-b + \sqrt{-10}\right) = b^2 + 10$, so $b \equiv 0 \mod 2$. Take $b = 0$.

    In general, get congruence condition $b \equiv 0 \mod a$ in the ramified case or $b = \pm c \mod a$ for $a \nmid c$ in the split case. Thus
    $$\mathfrak{p} = 2\mathbb{Z} + \sqrt{-10}\mathbb{Z} = \left\langle 2, \sqrt{-10} \right\rangle, \qquad \mathfrak{p}^2 = \left\langle 4, 2\sqrt{-10}, -10 \right\rangle = \langle 2 \rangle.$$
  - $3 \nmid Disc(K) = 40$ and $x^2 + 10 \equiv 0 \mod 3$ has no solutions, so 3 is inert.
- Check whether $\mathfrak{p} = \left\langle 2, \sqrt{-10} \right\rangle$ is principal or not. If $\mathfrak{p} = \langle \alpha \rangle$ for $\alpha = a + b\sqrt{-10}$,
$$2 = Nm_{K/\mathbb{Q}}(\alpha) = a^2 + 10b^2$$
has no solutions with $a, b \in \mathbb{Z}$, so $\mathfrak{p}$ is not principal, and $\mathfrak{p}^2 = \langle 2 \rangle$ is principal.

Thus $Cl\left(\mathbb{Q}\left(\sqrt{-10}\right)\right) \cong \mathbb{Z}/2\mathbb{Z}$.

Example. What is $Cl\left(\mathbb{Q}\left(\sqrt{-21}\right)\right)$?

- Minkowski bound is
$$\lambda(K) = \frac{2\sqrt{84}}{\pi} = \sqrt{\frac{336}{\pi^2}} < 6.$$
- We want to factor $2, 3, 5$ in K.
  - $2 \mid Disc(K)$, so 2 ramifies, and
$$\left\langle 2, 1+\sqrt{-21}\right\rangle^2 = \left\langle 4, 2\sqrt{-21}, 2\right\rangle = \langle 2\rangle.$$
Let $\mathfrak{p}_2 = \left\langle 2, 1+\sqrt{-21}\right\rangle$. Then
$$2 = Nm(\mathfrak{p}_2) = a^2 + 21b^2$$
has no solutions with $a, b \in \mathbb{Z}$, so $\mathfrak{p}_2$ is not principal.
  - $3 \mid Disc(K)$, so 3 ramifies, and
$$\left\langle 3, \sqrt{-21}\right\rangle^2 = \left\langle 9, 3\sqrt{-21}, -21\right\rangle = \langle 3\rangle.$$
Let $\mathfrak{p}_3 = \left\langle 3, \sqrt{-21}\right\rangle$. Then
$$3 = Nm(\mathfrak{p}_3) = a^2 + 21b^2$$
has no solutions with $a, b \in \mathbb{Z}$, so $\mathfrak{p}_3$ is not principal.
  - 5 splits, since $x^2 + 21 \equiv 0 \mod 5$ has solutions $x \equiv \pm 2 \mod 5$. Then
$$\langle 5\rangle = \mathfrak{p}_5 \cdot \overline{\mathfrak{p}_5},$$
for $\mathfrak{p}_5 = \left\langle 5, -b+\sqrt{-21}\right\rangle$ and $5 \mid b^2 + 21$, so $b = \pm 2$. Then
$$5 = Nm(\mathfrak{p}_5) = a^2 + 21b^2$$
has no solutions with $a, b \in \mathbb{Z}$, so $\mathfrak{p}_5$ is not principal.
- Compute
$$\mathfrak{p}_2 \cdot \mathfrak{p}_3 = \left\langle 2, 1+\sqrt{-21}\right\rangle \left\langle 3, \sqrt{-21}\right\rangle = \left\langle 6, 3\left(1+\sqrt{-21}\right), 2\sqrt{-21}, \sqrt{-21}-21\right\rangle = \left\langle 6, 3+\sqrt{-21}\right\rangle,$$
and
$$\mathfrak{p}_2 \cdot \mathfrak{p}_3 \cdot \left\langle \frac{3-\sqrt{-21}}{6}\right\rangle = \left\langle 3-\sqrt{-21}, 5\right\rangle = \left\langle 5, -2+\sqrt{-21}\right\rangle = \mathfrak{p}_5.$$

Thus $Cl\left(\mathbb{Q}\left(\sqrt{-21}\right)\right) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is the Klein four group.

Example. $Cl\left(\mathbb{Q}\left(\sqrt{-23}\right)\right) \cong \mathbb{Z}/3\mathbb{Z}$.

4.8 Solving Diophantine equations

Lecture 28
Friday
15/03/19

The goal is solving Diophantine equations, an application of the class group. **Mordell's equation** is $x^2 + n = y^3$ for $n \in \mathbb{Z}$ given.

Theorem 4.8.1. *For any $n \in \mathbb{Z}$, the equation $x^2 + n = y^3$ has only finitely many solutions with $x, y \in \mathbb{Z}$.*

Example. $x^2 + 1 = y^3$ has solution $(0, 1)$. Use $\mathbb{Q}(i)$ is a UFD or a PID or a Euclidean domain.

Example. $x^2 + 2 = y^3$ has solutions $(\pm 5, 3)$. Use $\mathbb{Q}\left(\sqrt{-2}\right)$ is a UFD or a PID or a Euclidean domain.

Example. $x^2 + 5 = y^3$. $\mathbb{Q}\left(\sqrt{-5}\right)$ is not a UFD, since $Cl\left(\mathbb{Q}\left(\sqrt{-5}\right)\right) = \mathbb{Z}/2\mathbb{Z}$. $x^2 \equiv 0, 1, 4 \mod 8$, so $x^2 + 5 \equiv 5, 6, 1 \mod 8$, but if $2 \mid y$, then $8 \mid y^3$, so $x^2 + 5 \equiv 0 \mod 8$, a contradiction, so $2 \nmid y$ and y is odd.

$$\left(x + \sqrt{-5}\right)\left(x - \sqrt{-5}\right) = y^3$$

is the factorisation in $\mathbb{Z}\left[\sqrt{-5}\right]$. Are the ideals $\left\langle x + \sqrt{-5}\right\rangle$ and $\left\langle x - \sqrt{-5}\right\rangle$ relatively prime? If $\mathfrak{p} \subsetneq \mathbb{Z}\left[\sqrt{-5}\right]$ is a prime ideal such that $\mathfrak{p} \mid \left\langle x + \sqrt{-5}\right\rangle$ and $\mathfrak{p} \mid \left\langle x - \sqrt{-5}\right\rangle$, then $\mathfrak{p} \mid 2x$, $\mathfrak{p} \mid 2\sqrt{-5}$, and $Nm(\mathfrak{p}) \mid y^3$, so $Nm(\mathfrak{p}) \mid \gcd\left(20, y^3\right) = \gcd\left(5, y^3\right)$, which is either one or five.

- Assume $Nm(\mathfrak{p}) = 5$. $Nm(\mathfrak{p}) \mid y^3$ and $Nm(\mathfrak{p}) \mid x^2$, so $5 \mid x$ and $5 \mid y$, so $5 = y^3 - x^3$ is a multiple of 25, which has no solutions, a contradiction.
- $Nm(\mathfrak{p}) = 1$ and $\mathfrak{p}$ is prime is a contradiction.

Then $\left\langle x + \sqrt{-5}\right\rangle$ and $\left\langle x - \sqrt{-5}\right\rangle$ are relatively prime ideals, so there exist $I, J \subseteq \mathbb{Z}\left[\sqrt{-5}\right]$ ideals such that

$$\left\langle x + \sqrt{-5}\right\rangle = I^3, \qquad \left\langle x - \sqrt{-5}\right\rangle = J^3,$$

using unique factorisation into prime ideals. Are I, J principal ideals? Recall $Cl\left(\mathbb{Q}\left(\sqrt{-5}\right)\right) = \mathbb{Z}/2\mathbb{Z}$. Assume I is not principal, so $I = \langle a\rangle \cdot \left\langle 2, 1 + \sqrt{-5}\right\rangle$ for $a \in \mathbb{Q}\left(\sqrt{-5}\right)^\times$, but then

$$I^3 = \left\langle a^3\right\rangle \cdot \langle 2\rangle \cdot \left\langle 2, 1 + \sqrt{-5}\right\rangle = \left\langle 2a^3\right\rangle \cdot \left\langle 2, 1 + \sqrt{-5}\right\rangle,$$

which is not a principal ideal, so I was principal to begin with. Key idea is that $3 \nmid \#Cl\left(\mathbb{Q}\left(\sqrt{-5}\right)\right)$. The argument does not work if $3 \mid \#Cl(K)$ for K a quadratic field. Similarly, J is a principal ideal. Can I say $x + \sqrt{-5} = \left(a + b\sqrt{-5}\right)^3$ for $a, b \in \mathbb{Z}$? In general, only up to units in $\mathbb{Z}\left[\sqrt{-5}\right]$, and $\mathbb{Z}\left[\sqrt{-5}\right]^\times = \{\pm 1\}$ are cubes. So, indeed, we have

$$x + \sqrt{-5} = \left(a + b\sqrt{-5}\right)^3, \qquad x - \sqrt{-5} = \left(a - b\sqrt{-5}\right)^3, \qquad a, b \in \mathbb{Z}.$$

Then

$$x + \sqrt{-5} = a^3 + 3a^2b\sqrt{-5} - 15ab^2 - 5b^3\sqrt{-5},$$

so get Diophantine equation $3a^2b - 5b^3 = 1$ for $a, b \in \mathbb{Z}$, so $b\left(3a^2 - 5b^2\right) = 1$, so $b = \pm 1$.

- $b = 1$ implies that $3a^2 = 6$, which has no solution.
- $b = -1$ implies that $3a^2 = 4$, which has no solution.

Example. $x^2 + 11 = y^3$. We factor this as

$$\left(x + \sqrt{-11}\right)\left(x - \sqrt{-11}\right) = y^3.$$

The relevant number field for this equation is $\mathbb{Q}\left(\sqrt{-11}\right)$, which is a principal ideal domain. We had seen earlier in the course that it is even a Euclidean domain. One can also prove that the class group is trivial by considering the Minkowski bound

$$\lambda(K) = \frac{2\sqrt{11}}{\pi} < 3.$$

This means we only need to understand how to factor 2 and since $-11 \equiv 5 \mod 8$, we know that 2 must stay inert, so it does not give rise to any non-principal ideal. We prove as before that y must be odd and that the ideals $\left\langle x + \sqrt{-11}\right\rangle$ and $\left\langle x - \sqrt{-11}\right\rangle$ are relatively prime. Using unique factorisation, also noting that the units ± 1 are both cubes, we deduce that

$$x + \sqrt{-11} = \frac{\left(a + b\sqrt{-11}\right)^3}{8}, \qquad x - \sqrt{-11} = \frac{\left(a - b\sqrt{-11}\right)^3}{8}, \qquad a, b \in \mathbb{Z}$$

must have the same parity. We obtain the Diophantine equation $8 = 3a^2b - 11b^3$. This has solutions $(a, b) = (\pm 1, 1)$ and $(a, b) = (\pm 4, 2)$. These give the solutions $(x, y) = (\pm 4, 3)$ and $(x, y) = (\pm 15, 58)$.

Example. $x^2 - 7 = y^3$.

$$x^2 - 7 = \left(x + \sqrt{7}\right)\left(x - \sqrt{7}\right) = y^3$$

in $K = \mathbb{Q}\left(\sqrt{7}\right)$, a real quadratic field. Claim $Cl(K) = 1$. Minkowski bound is

$$\lambda(K) = \sqrt{7} < 3,$$

that is at most 2, and 2 ramifies, since $2 \mid 28 = Disc(K)$, and

$$\langle 2\rangle = \left\langle 2, 1 + \sqrt{7}\right\rangle^2 = \left\langle 3 + \sqrt{7}\right\rangle^2,$$

so K is a PID. $x + \sqrt{7} = u \cdot \left(a + b\sqrt{7}\right)^3$ for $u \in \mathbb{Z}\left[\sqrt{7}\right]^\times$. Problem is

$$\mathbb{Z}\left[\sqrt{7}\right]^\times = \left\{\pm\epsilon^k \mid k \in \mathbb{Z}\right\} \cong \{\pm 1\} \times \qquad \mathbb{Z}, \epsilon = 8 + \sqrt{7} \cdot 3$$

such that

$$Nm(\epsilon) = \left(8 + \sqrt{7} \cdot 3\right)\left(8 - \sqrt{7} \cdot 3\right) = 64 - 63 = 1.$$

The following is an elementary solution.

$$x^2 + 1 = y^3 + 8 = (y + 2)\left(y^2 - 2y + 4\right) = (y + 2)\left((y - 1)^2 + 3\right).$$

y is odd and $y - 1$ is even, so

$$x^2 + 1 = (y + 2)(4k + 3), \qquad k \in \mathbb{Z}.$$

Then there exists $p \equiv 3 \mod 4$ prime such that $p \mid x^2 + 1$ but -1 is not a square mod p if $p \equiv 3 \mod 4$, since $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = -1$, a contradiction. Thus $x^2 - 7 = y^3$ has no solutions with $x, y \in \mathbb{Z}$.

Remark. $x^2 + n = y^3$ with $n > 0$, if $3 \nmid \#Cl\left(\mathbb{Q}\left(\sqrt{-n}\right)\right)$, then the equation has at most two pairs of solutions $(\pm x, y)$.

4.9 Fundamental units

Lecture 29
Monday
18/03/19

The goal is to discuss the group of units $\mathcal{O}_K^\times$ when K is a real quadratic field. If K is imaginary quadratic, then

$$\mathcal{O}_K^\times = \begin{cases} \mathbb{Z}/4\mathbb{Z} & K = \mathbb{Q}(i) \\ \mathbb{Z}/6\mathbb{Z} & K = \mathbb{Q}(\omega) \\ \mathbb{Z}/2\mathbb{Z} & \text{otherwise} \end{cases}.$$

Theorem 4.9.1. *If K is real quadratic, then*

$$\mathcal{O}_K^\times \cong \{\pm 1\} \times \mathbb{Z}$$
$$\pm\epsilon^k \hookleftarrow (\pm 1, k),$$

*with $\epsilon \in \mathcal{O}_K^\times$ a **fundamental unit**, that is the smallest element of $\mathcal{O}_K^\times$ such that $\epsilon > 1$.*

In general, $Nm_{K/\mathbb{Q}}(\epsilon) = \pm 1$. To find $\mathcal{O}_K^\times$, we will look at solutions to **Pell's equation** $x^2 - dy^2 = \pm 1$, where $K = \mathbb{Q}\left(\sqrt{d}\right)$ for $d > 0$ square-free and $\epsilon = x + \sqrt{d} \cdot y$.

Example. Let $K = \mathbb{Q}\left(\sqrt{5}\right)$. Then $x^2 - 5y^2 = -1$ has solution $(x, y) = (\pm 2, \pm 1)$, since $2 + \sqrt{5}$ has

$$Nm_{K/\mathbb{Q}}\left(2 + \sqrt{5}\right) = \left(2 + \sqrt{5}\right)\left(2 - \sqrt{5}\right) = -1.$$

Lemma 4.9.2. *Let $\epsilon \in \mathcal{O}_K^\times$ be such that $\epsilon > 1$ and ϵ is the smallest element of $\mathcal{O}_K^\times$ with this property. Then any $\epsilon' \in \mathcal{O}_K^\times$ satisfies $\epsilon' = \pm\epsilon^k$ for some $k \in \mathbb{Z}$.*

Proof. Let

$$[\epsilon, \infty) = \left[\epsilon, \epsilon^2\right) \cup \left[\epsilon^2, \epsilon^3\right) \cup \dots.$$

Then $\epsilon' \in \mathbb{R}^\times \setminus \{\pm 1\}$, so one of $\epsilon', -\epsilon', 1/\epsilon', -1/\epsilon'$ is greater than one. If either of these is $\pm\epsilon^k$, for $k \in \mathbb{Z}$, then ϵ' is of this form as well. We may assume $\epsilon' > 1$, so $\epsilon' > \epsilon$, so $\epsilon' \in \left[\epsilon^k, \epsilon^{k+1}\right)$ for some $k \in \mathbb{Z}_{\geq 1}$. Then $\epsilon'/\epsilon^k \in \mathcal{O}_K^\times$ and $\epsilon'/\epsilon^k \in [1, \epsilon)$. This gives a contradiction unless $\epsilon'/\epsilon^k = 1$, so $\epsilon' = \epsilon^k$. □

4.10 Continued fractions

The goal is to understand solutions to Pell's equation $x^2 - dy^2 = \pm 1$. If (x, y) is a solution for $x, y > 0$ then $x/y \in \mathbb{Q}$ is close to $\sqrt{d} \in \mathbb{R} \setminus \mathbb{Q}$. In fact it is the best rational approximation to $\sqrt{d}$. The theory of **continued fractions** gives a way of constructing such rational approximations for $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Let $a_0 = \lfloor \alpha \rfloor \in \mathbb{Z}$. If $a_0 = \alpha$ terminate here. If not, then $\alpha - a_0 \in (0, 1)$, so

$$a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1} \in \mathbb{Q}, \qquad a_1 = \left\lfloor \frac{1}{\alpha - a_0} \right\rfloor \in \mathbb{Z}_{\geq 1}.$$

If $a_1 = 1/(\alpha - a_0)$ terminate here. If not, then $1/(\alpha - a_0) - a_1 \in (0, 1)$, so

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2}} = a_0 + \frac{1}{\frac{a_1 a_2 + 1}{a_2}} = \frac{a_0 a_1 a_2 + a_0 + a_2}{a_1 a_2 + 1} \in \mathbb{Q}, \qquad a_2 = \left\lfloor \frac{1}{\frac{1}{\alpha - a_0} - a_1} \right\rfloor.$$

Let

$$[a_0; a_1, \dots, a_n] = a_0 + \frac{1}{a_1 + \frac{1}{\dots + \frac{1}{a_n}}} \in \mathbb{Q}.$$

Then $[a_0; a_1, \dots, a_n] \to \alpha$ when $n \to \infty$.

Lemma 4.10.1. *The continued fraction expansion of $\alpha \in \mathbb{R}$ terminates if and only if $\alpha \in \mathbb{Q}$. If $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ the continued fraction expansion is $[a_0; a_1, \dots]$, where $a_0 \in \mathbb{Z}$ and $a_1, a_2, \dots \in \mathbb{Z}_{\geq 1}$. Then*

$$a_0 + \frac{1}{a_1 + \frac{1}{\dots}}$$

converges to α.

Example.

$$\frac{1+\sqrt{5}}{2} = 1 + \frac{\sqrt{5}-1}{2} = 1 + \frac{1}{\frac{2}{\sqrt{5}-1}} = 1 + \frac{1}{\frac{2\left(1+\sqrt{5}\right)}{4}} = 1 + \frac{1}{\frac{1+\sqrt{5}}{2}} = 1 + \frac{1}{1+\frac{1}{\cdots}} = [1;1,1,\dots] = \left[\overline{1}\right]$$

is **purely periodic**.

$$\sqrt{7} = 2 + \left(\sqrt{7}-2\right) = 2 + \frac{1}{\frac{\sqrt{7}+2}{3}} = 2 + \frac{1}{1+\frac{\sqrt{7}-1}{3}} = \cdots = [2;1,1,1,4,1,1,1,4,\dots] = \left[2;\overline{1,1,1,4}\right]$$

is **periodic**.

Theorem 4.10.2. *The continued fraction expansion of an element $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ is periodic if and only if α is a quadratic number, that is $\alpha \in \mathbb{Q}\left(\sqrt{d}\right)$, for $d > 0$ square-free.*

Lecture 30
Tuesday
19/03/19

Definition 4.10.3. Let $[a_0; a_1, a_2, \dots]$. The **i-th convergent** is the truncated expansion

$$[a_0; a_1, \dots, a_i] = a_0 + \frac{1}{a_1 + \frac{1}{\cdots + \frac{1}{a_i}}}.$$

Definition 4.10.4. Let $\{p_i\}_{i=-2}^{\infty}$ and $\{q_i\}_{i=-2}^{\infty}$ be the sequences defined by

$$p_{-2} = 0, \qquad p_{-1} = 1, \qquad p_{i+1} = a_{i+1}p_i + p_{i-1}, \qquad q_{-2} = 1, \qquad q_{-1} = 0, \qquad q_{i+1} = a_{i+1}q_i + q_{i-1},$$

so $p_0 = a_0, p_1 = a_1a_0 + 1, q_0 = 1, q_1 = a_1$.

Lemma 4.10.5. *We have*

$$\frac{p_i}{q_i} = [a_0; a_1, \dots, a_i].$$

Proof. $[a_0] = a_0 = p_0/q_0$ and $[a_0; a_1] = a_0 + 1/a_1 = (a_0a_1 + 1)/a_1 = p_1/q_1$. Proof by induction on i. The key idea is to apply the $(i-1)$-st step to

$$[a_0; a_1, \dots, a_i] = \left[a_0; a_1, \dots, a_{i-1} + \frac{1}{a_i}\right],$$

the $(i-1)$-st convergent. □

Proposition 4.10.6. *The i-th convergent p_i/q_i satisfy the following.*

1. $p_iq_{i-1} - q_ip_{i-1} = (-1)^{i-1}$. *In particular,* $\gcd(p_i, q_i) = 1$ *and also*

$$\left|\frac{p_i}{q_i} - \frac{p_{i-1}}{q_{i-1}}\right| = \frac{1}{q_iq_{i-1}} = \left|\frac{p_iq_{i-1} - p_{i-1}q_i}{q_iq_{i-1}}\right| = \left|\frac{1}{q_iq_{i-1}}\right|.$$

2. *If $x = [a_0; a_1, \dots] \in \mathbb{R} \setminus \mathbb{Q}$ and $p_i/q_i = [a_0; a_1, \dots, a_i]$ then $p_i/q_i < x$ for i even and $p_i/q_i > x$ for i odd. In particular,*

$$\frac{p_i}{q_i} < x < \frac{p_{i-1}}{q_{i-1}},$$

for i even, so

$$\left|x - \frac{p_i}{q_i}\right| < \left|\frac{p_{i-1}}{q_{i-1}} - \frac{p_i}{q_i}\right| = \frac{1}{q_iq_{i-1}} < \frac{1}{(i-1)^2}$$

because $q_i \geq i$.

Corollary 4.10.7. $[a_0; a_1, \ldots, a_i] \to x$ *as* $i \to \infty$.

In other words

$$x = [a_0; a_1, \ldots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots}}$$

makes sense.

Proof of Proposition 4.10.6. By induction on i.

1. Use $i-1$ case and recurrence for $\{p_i\}_i$ and $\{q_i\}_i$.
2. $[a_1; a_2, \ldots, a_i]$ is the $(i-1)$-st convergent to $1/(x - a_0)$. If i is even and $i-1$ is odd, by induction hypothesis

$$[a_1; a_2, \ldots, a_i] > \frac{1}{x - a_0} \qquad \iff \qquad x > a_0 + \frac{1}{[a_1; a_2, \ldots, a_i]} = [a_0; a_1, \ldots, a_i].$$

Similarly i is odd and $i-1$ is even.

□

In conclusion, $p_i/q_i \to x$ as $i \to \infty$ and

$$\left| \frac{p_i}{q_i} - x \right| < \frac{1}{q_i q_{i+1}} < \frac{1}{q_i^2}.$$

Theorem 4.10.8 (Best rational approximation)**.** *If* $r, s \in \mathbb{Z}$ *such that* $0 < |s| \leq q_i$ *then*

$$\left| x - \frac{r}{s} \right| \geq \left| x - \frac{p_i}{q_i} \right|,$$

with equality only if $r/s = p_i/q_i$.

4.11 Pell's equation

If $d = 0$ is square-free, then $\sqrt{d} = [a_0; \overline{a_1, \ldots, a_m}]$ is periodic, but not purely periodic. $\left\lfloor \sqrt{d} \right\rfloor + \sqrt{d}$ is purely periodic.

Theorem 4.11.1. *The solutions to Pell's equation* $x^2 - dy^2 = \pm 1$ *are the* (p_n, q_n) *with* $n = km - 1$ *for* $k \in \mathbb{Z}_{\geq 1}$ *and moreover*

$$p_n^2 - dq_n^2 = (-1)^{km}.$$

In particular $x^2 - dy^2 = -1$ *has a solution if and only if* m *is odd.*

Example.

- Let $\mathbb{Q}(\sqrt{7}) \supseteq \mathbb{Z}[\sqrt{7}]$. Then $\sqrt{7} = [2, \overline{1, 1, 1, 4}]$ has period length four. $x^2 - 7y^2 = -1$ has no solutions. $x^2 - 7y^2 = 1$ has solutions (p_{4k-1}, q_{4k-1}). Fundamental solution is (p_3, q_3).

$$2 + \cfrac{1}{1 + \frac{1}{2}} = 2 + \frac{1}{\frac{3}{2}} = 2 + \frac{2}{3} = \frac{8}{3},$$

so $(p_3, q_3) = (8, 3)$. Thus $8 + \sqrt{7} \cdot 3$ is the fundamental unit, so $\mathbb{Z}[\sqrt{7}]^\times = \{\pm 1\} \times \{\epsilon^k \mid k \in \mathbb{Z}\}$, where $\epsilon = 8 + \sqrt{7} \cdot 3$.

- Let $\mathbb{Q}(\sqrt{13}) \supseteq \mathbb{Z}\left[\frac{1+\sqrt{13}}{2}\right]$. What is $\mathbb{Z}\left[\frac{1+\sqrt{13}}{2}\right]^\times$? $\sqrt{13} = [3; \overline{1, 1, 1, 1, 6}]$ has period length five. $x^2 - 13y^2 = -1$ has solutions (p_4, q_4).

$$3 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \frac{1}{1}}}} = \frac{18}{5},$$

so $(p_4, q_4) = (18, 5)$. Thus $18 + \sqrt{13} \cdot 5$ is a fundamental unit.

A Fermat's last theorem

Lecture 31
Friday
22/03/19

A.1 History

The following theorem is conjectured by Fermat and proved by Taylor-Wiles.

Theorem A.1.1. *$x^n + y^n = z^n$ has no non-trivial solutions if $n \geq 3$.*

Initial idea is that it is enough to consider case $n = 4$ and $n = p$ for p odd prime.

Theorem A.1.2 (Fermat)**.** *$x^4 + y^4 = z^4$ has no non-trivial solutions.*

Proof. Use infinite descent argument. Assume a solution (x, y, z) and construct a solution (x', y', z') that is smaller for some measure. □

Theorem A.1.3 (Euler)**.** *$x^3 + y^3 = z^3$ has no non-trivial solutions.*

Proof. Use factorisation $(x + y)(x + \omega y)\left(x + \omega^2 y\right) = z^3$ in the Eisenstein integers $\mathbb{Z}[\omega]$, where $\omega^3 = 1$ is the primitive cube of unity, which is a unique factorisation domain.

- Find common prime factors of $\langle x + y\rangle, \langle x + \omega y\rangle, \left\langle x + \omega^2 y\right\rangle$.
- Use unique factorisation to show that $\langle x + y\rangle = I^3 \cdot \gcd\left(\langle x + y\rangle, \langle x + \omega y\rangle, \left\langle x + \omega^2 y\right\rangle\right)$.

Then use infinite descent. □

More generally, $x^p + y^p = z^p$ factors as $\prod_{i=0}^{p-1}\left(x + \zeta_p^i y\right) = z^p$, for ζ_p a primitive p-th root of unity, in the ring of integers $\mathcal{O}_K \subseteq K$ of a **cyclotomic field** $K = \mathbb{Q}(\zeta_p)/\mathbb{Q}$, an extension of degree $p - 1$. Can try to adopt strategy from $p = 3$ to general p. Problem is that there is no reason to believe $\mathcal{O}_K$ is a UFD or a PID, so there is no reason to expect $Cl(K) = 1$. If $p \nmid \#Cl(K)$, the same idea works. Such p are called **regular**.

Theorem A.1.4 (Kummer)**.** *$x^p + y^p = z^p$ has no non-trivial solutions if p is regular.*

Example. If $\gcd\left(x - \zeta_p^i y, x + \zeta_p^j y\right) = 1$ for $i \neq j$, then $x + \zeta_p^i y = u_i \alpha_i^p$ for $i = 0, \ldots, p - 1$.

Problem is that there exist infinitely many primes such that $p \mid \#Cl(\mathbb{Q}(\zeta_p))$, such as $p = 37$.

A.2 Class field theory

Let $K/\mathbb{Q}$ be a number field. Then $Cl(K) = I/P$ is a finite abelian group, where I is all the non-zero fractional ideals of K and P is all the non-zero principal ideals of K. If L/K is a finite field extension, the **Galois group** $Gal(L/K)$ is the group of field automorphisms of L that are identity on K.

Example. Let $L = \mathbb{Q}\left(\sqrt{d}\right)$ be a quadratic field and $K = \mathbb{Q}$. Then $Gal(L/K) = \mathbb{Z}/2\mathbb{Z} = \{1, \tau\}$ is generated by $\tau : \sqrt{d} \mapsto -\sqrt{d}$.

There exists a finite extension L/K **unramified everywhere**. All prime ideals $\mathfrak{p} \subsetneq \mathcal{O}_K$ of K either split or stay inert in L, so $\mathfrak{p} = \mathfrak{p}_1 \cdot \cdots \cdot \mathfrak{p}_g$ for some $g \in \mathbb{Z}$ and prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_g \subsetneq \mathcal{O}_L$ all distinct, and L/K is unramified at **infinite places**. Moreover $Gal(L/K)$ is abelian. Then L is the **Hilbert class field** of K, the biggest finite abelian extension of K which is unramified everywhere.

Theorem A.2.1. *$Cl(K) \cong Gal(L/K)$.*

Example. Let $Cl(K) \cong \mathbb{Z}/4\mathbb{Z}$.

- There exists a quadratic extension L_1/K unramified everywhere with $Gal(L_1/K) \cong \mathbb{Z}/2\mathbb{Z}$.
- There exists a quadratic extension L_2/L_1 unramified everywhere with $Gal(L_2/L_1) \cong \mathbb{Z}/2\mathbb{Z}$.

Then L_2 is the Hilbert class field of K.

Can generalise this picture to ideals $\mathfrak{m} \subseteq \mathcal{O}_K$. The **ray class group** of **conductor** $\mathfrak{m}$ is $I^{\mathfrak{m}}/P^{\mathfrak{m}}$, where $I^{\mathfrak{m}}$ is all the non-zero fractional ideals prime to $\mathfrak{m}$ and $P^{\mathfrak{m}}$ is all the ideals generated by $a \equiv 1 \mod \mathfrak{m}$.

Theorem A.2.2. *There exists a* ***ray class field*** L/K.

Can understand $Gal\left(\overline{K}/K\right)^{ab}$. Let

$$Gal\left(\overline{K}/K\right) = \varprojlim_{L/K \text{ finite}} Gal\left(L/K\right)$$

be the **absolute Galois group** of K. Can describe $Gal\left(\overline{K}/K\right)^{ab}$, the maximal abelian quotient of $Gal\left(\overline{K}/K\right)$, in terms of generalisations of $Cl\left(K\right)$, the **idele class group** I_K.

Theorem A.2.3 (Global Artin reciprocity)**.** $I_K/Nm_{L/K}\left(I_L\right) \cong Gal\left(\overline{K}/K\right)^{ab}$.

This is interesting for $K = \mathbb{Q}$.

A.3 Modular forms and elliptic curves

If $Gal\left(L/K\right)$ is not abelian, need to understand n-dimensional representations of $Gal\left(L/K\right)$.

Example. $Gal\left(L/K\right) \cong S_3$ has 2-dimensional irreducible representations $\rho : S_3 \to GL_2\left(\mathbb{C}\right)$, so

$$Gal\left(\overline{K}/K\right) \twoheadrightarrow Gal\left(L/K\right) \cong S_3 \xrightarrow{\rho} GL_2\left(\mathbb{C}\right).$$

The $n = 2$ case is related to **modular forms**, holomorphic functions f on $\mathcal{H} = \{z \in \mathbb{C} \mid \Im\left(z\right) > 0\}$ satisfying certain symmetries. $SL_2\left(\mathbb{Z}\right)$ acts on $\mathcal{H}$ by

$$\begin{array}{rcl} SL_2\left(\mathbb{Z}\right) \curvearrowright \mathcal{H} & \longrightarrow & \mathcal{H} \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix}\left(z\right) & \longmapsto & \dfrac{az+b}{cz+d}, \end{array} \qquad a,b,c,d \in \mathbb{Z}, \qquad ad - bc = 1,$$

so

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} : z \mapsto z, \qquad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} : z \mapsto z+1, \qquad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} : z \mapsto -\frac{1}{z}.$$

Expanding $f\left(z\right) = f\left(z+1\right)$ in Fourier series,

$$f\left(z\right) = q + a_2 q^2 + a_3 q^3 + \ldots, \qquad q = e^{2\pi i z}.$$

Example. $f\left(z\right) = q\prod_{n=1}^{\infty}\left(1-q^n\right)^2\left(1-q^{11n}\right)^2$ is a modular form.

On the other hand, **elliptic curves**, smooth projective curves $E/\mathbb{Q}$ of genus one, have a **group law** over $\mathbb{Q}$. Let $E\left[p\right]$ be the p**-torsion points**, where

$$0 = \left[p\right]\left(x_0, y_0\right) = \left(x_0, y_0\right) +_E \cdots +_E \left(x_0, y_0\right).$$

Then $Gal\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ acts on $E\left[p\right]$ to give $\left(x_0, y_0\right)$ for algebraic numbers $x_0, y_0 \in \overline{\mathbb{Q}}$, and $E\left[p^n\right] \cong \left(\mathbb{Z}/p^n\mathbb{Z}\right)^2$.

Example. $y^2 + y = x^3 - x^2$ is an elliptic curve.

A.4 From Artin reciprocity to modularity

If L be the Hilbert class field of K, then a one-dimensional reciprocity is

$$Gal\left(L/K\right) \cong Cl\left(K\right).$$

If E is an elliptic curve and a_p is the Fourier coefficient to a modular form for some prime p, a two-dimensional reciprocity is

$$p - \#\left\{\text{solutions to } E \mod p\right\} = a_p.$$

This was the key to the proof of Fermat's last theorem.