M3P15 Algebraic Number Theory

Lectured by Dr Ana Caraiani
Typeset by David Kurniadi Angdinata

Spring 2019

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 $p_i \mid mn$ gives $p_i \mid m$ 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 $a, b \in \mathbb{Z}$, $b \neq 0$, 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 $a, b \in \mathbb{Z}$, $ab \neq 0$. 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*

$$p \mid ab, \qquad a, b \in \mathbb{Z} \qquad \implies \qquad p \mid a \text{ or } p \mid b.$$

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 gives $p_1 \mid q_1$, 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 $x, y \in I$ gives $x + y \in I$, 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

$$\begin{array}{ccc} R & \to & \dfrac{R}{I} \\ a & \mapsto & a + I \end{array}.$$

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

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

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

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*

$$\begin{array}{ccc} \dfrac{R}{Ker\,(\phi)} & \to & \phi\,(R) \subset S \\ r + Ker\,(\phi) & \mapsto & \phi\,(r) \end{array},$$

for $r \in R$.

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

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

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

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

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

$$\begin{array}{rcl} R & \to & \dfrac{R}{I} \times \dfrac{R}{J} \\ r & \mapsto & (r \mod I, r \mod J) \end{array},$$

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 $a, b \in R$ gives $a = 0$ 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 $ab \in \mathfrak{p}$ gives $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. $(a + \mathfrak{p})(b + \mathfrak{p}) = 0$ in $R/\mathfrak{p}$ gives $a + \mathfrak{p} = 0$, 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. $a \mid b$ gives there exists c such that $ac = b$ and $b \mid a$ gives there exists d such that $bd = a$ for $c, d \in R$. $acd = bd = a$ if and only if $a(cd - 1) = 0$. R is an ID gives $a = 0$ 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 $b, c \in R$ then either b or c is in $R^\times$.
- We say $a \in R$ is **prime** if
  - a is not a unit, and
  - $a \mid bc$ gives $a \mid b$ 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.

Proof. Let $b, c \in R$ be such that $a = bc$, so $b \mid a$ and $c \mid a$. Because a is prime, $a = bc$ gives $a \mid b$ or $a \mid c$. Say $a \mid b$ happens. There exists $d \in R^\times$ such that $a = bd$. $a = bc$ gives $b(d - c) = 0$. $b \neq 0$, 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 $\alpha, \beta \in \mathbb{Z}\left[\sqrt{-5}\right]$. Goal is that α or β is a unit. We will use

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

  which is multiplicative. $N(2) = 4 = N(\alpha)N(\beta)$. If $N(\alpha) = 1$, then α is a unit. $N(\alpha) = N(\beta) = 2$ gives $a^2 + 5b^2 = 2$, 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 gives 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 $b = v \cdot q_1 \cdot \cdots \cdot q_{d(b)}$. $a \mid b$ gives $b = a \cdot c$ 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 gives $d(b) = d(a) + d(c)$, 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

$$\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \ldots \qquad \Longrightarrow \qquad \cdots \mid a_2 \mid a_1 \qquad \Longrightarrow \qquad d(a_1) \geq \cdots \geq 0.$$

This sequence stabilises after finitely many steps. There exists n such that

$$d(a_n) = d(a_{n+1}) = \ldots \qquad \Longrightarrow \qquad a_n \sim a_{n+1} \sim \ldots \qquad \Longrightarrow \qquad \langle a_n \rangle = \langle a_{n+1} \rangle = \ldots.$$

$\Longleftarrow$ 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, $a_2 = b$. $a = bc$ for c not a unit gives $\langle a \rangle \subsetneq \langle b \rangle$. 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 irreducible gives 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 $x + y \in \langle a_m \rangle$ gives $x + y \in I$. Otherwise $y \in \langle a_n \rangle$, so $x + y \in \langle a_n \rangle$ gives $x + y \in I$. 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 unique factorisation domain.*

Lecture 5
Monday
21/01/19

Proof. Let $I \subseteq R$ be an ideal. Assume $I \neq \langle 0 \rangle$ 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 $b \in I \setminus \langle a \rangle$. Apply property of ϕ to b and a, $b = qa + r$. $r \neq 0$, otherwise $a \mid b$ gives $b \in \langle a \rangle$. $r = b - qa \in I$ but $\phi(r) < \phi(a)$, a contradiction. □

Example.

- $\mathbb{Z}$, with Euclidean norm
$$\begin{array}{ccc} \mathbb{Z} \setminus \{0\} & \to & \mathbb{Z}_{\geq 1} \\ n & \mapsto & |n| \end{array}.$$
- Gaussian integers. $\mathbb{Z}[i]$, with Euclidean norm given by restriction to $\mathbb{Z}[i] \subset \mathbb{C}$ of complex absolute value
$$\begin{array}{ccc} \mathbb{Z}^2 \setminus \{(0,0)\} & \to & \mathbb{Z}_{\geq 1} \\ a + ib & \mapsto & (a+ib)(a-ib) = a^2 + b^2 \end{array}.$$
- 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
$$\begin{array}{ccc} \mathbb{Z}^2 \setminus \{(0,0)\} & \to & \mathbb{Z}_{\geq 1} \\ a + b\omega & \mapsto & a^2 - ab + b^2 \end{array}.$$

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

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

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 $N(1) = 1$. $uv = 1$ gives $N(u) \cdot N(v) = 1$, so $N(u) \geq 1$ and $N(v) \geq 1$ gives $N(u) = N(v) = 1$. □

$N(u) = u \cdot \overline{u} = 1$. $u = a + bi \in \mathbb{Z}[i]^\times$ 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 $\alpha, \beta \in \mathbb{Z}[i]$, $\beta \neq 0$, 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. $\lambda = \beta(\alpha/\beta - \kappa)$ gives $N(\lambda) < N(\beta)$. □

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 $N(a+bi) \mid N(p) = p^2$ gives $N(a+bi) = p = a^2 + b^2$, which cannot happen. This is an **inert** prime.

Lecture 6
Tuesday
22/01/19

Quadratic reciprocity gives 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 $2 \mid y$ gives $8 \mid y^3$. But $x^3 + 1 \equiv 1, 2, 5 \mod 8$ gives $\gcd(x+i, x-i) = 1$, so

$$\begin{cases} x + i = uz^3 = (uz)^3 \\ x - i = \overline{uz}^3 = (\overline{uz})^3 \end{cases},$$

for $u \in \{\pm 1, \pm i\}$.

$$x - i = (a+bi)^3 = a^3 - b^3 i + 3a^2 bi - 3ab^2,$$

for some $a, b \in \mathbb{Z}$. 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*

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

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 Summary of 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 $\mathcal{O}_7, \mathcal{O}_{11} \subset \mathbb{Q}\left(\sqrt{-7}\right)$ 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.

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

  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 Structure theorem for finitely generated abelian groups

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

$$m_1, m_2 \in M \qquad \Longrightarrow \qquad m_1 + m_2 \in M,$$

- an action of R on M,

$$\begin{array}{rcl} R \times M & \to & M \\ (r, m) & \mapsto & rm \end{array}$$

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 Weak structure theorem

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

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

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'. □

2.3 Strong structure theorem

Theorem 2.3.1 (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 2.3.2. *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 2.3.2, 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 2.3.1 gives

$$M = e_1\mathbb{Z} \oplus \cdots \oplus e_n\mathbb{Z}, \qquad M' = a_1 e_1 \mathbb{Z} \oplus \cdots \oplus a_q e_q \mathbb{Z},$$

where $a_{q+1} = \cdots = a_n = 0$. 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 2.3.3. *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 2.3.4. *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 $J \in S'$ gives $I = J$, 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 2.3.4 were not true, would set

$$I_1 \subsetneq I_2 \subsetneq \dots,$$

with $I_i \in S$, a contradiction. □

Lemma 2.3.5. *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 2.3.4, 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 2.3.3 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 2.3.1. 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 $n - 1$.
- Let $N' = M' \cap N$ be a submodule, where

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

- 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 $(a_2 e_2, \dots, a_q e_q)$ and $a_2 \mid \dots \mid a_q$. $M' \twoheadrightarrow p(M') = a_1\mathbb{Z}$ 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 $x = a_1 e_1$, where

$$e_1 = e_1' + \frac{p_2(x)}{a_1} e_2 + \dots + \frac{p_n(x)}{a_1} e_n,$$

  and $p_2(x)/a_1, \dots, p_n(x)/a_1 \in \mathbb{Z}$.
- Left to prove that $a_1 \mid a_2$. Let $d = (a_1, a_2) = b_1 a_1 + b_2 a_2$. There exists $d : M \to \mathbb{Z}$ such that $d(x) = b_1 p_1(x) + b_2 p_2(x)$, 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

2.4 Torsion elements

Definition 2.4.1.

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

Proof. Use structure theorem.

$$M \cong \frac{\mathbb{Z}}{a_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{a_n\mathbb{Z}},$$

with $a_1, \ldots, a_n \in \mathbb{Z}$ satisfying $a_1 \mid \cdots \mid a_n$. 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. □

3 Ring of integers in number fields

3.1 Integral closure

Definition 3.1.1. An element $x \in \mathbb{C}$ is called

- an **algebraic number** if it satisfies an equation

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

  with all $a_i \in \mathbb{Q}$, and
- 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 3.1.2. 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

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

with $a_i \in A$ for $i = 0, \ldots, n-1$.

Theorem 3.1.3. *Let R be an integral domain and $A \subseteq R$ a subring. Then if $a, b \in R$ are integral over A, so are $a + b, a - b, ab$.*

Lemma 3.1.4. *Let R be an integral domain. 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 gives

$$M^n + a_{n-1}M^{n-1} + \cdots + a_0 I_n = 0_n \in R^n \qquad \Longrightarrow \qquad M^n v + a_{n-1}M^{n-1}v + \cdots + a_0 I_n v = 0_n \in R^n.$$

Since $Mv = x \cdot v$, we get

$$x^n \cdot v + a_{n-1}x^{n-1} \cdot v + \cdots + a_0 \cdot v = 0_n \in R^n \qquad \Longrightarrow \qquad \left(x^n + a_{n-1}x^{n-1} + \cdots + a_0\right) \cdot v = 0_n \in R^n.$$

$v \neq 0$ gives

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0 \in R,$$

so x is a root of P. □

Proof of Theorem 3.1.3. Let $x = a + b$. 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 $b^{m-1}, \ldots, 1$.

$$(a+b) \cdot a^i b^j = a^{i+1}b^j + a^i b^{j+1},$$

for $i = 0, \ldots, n-1$ and $j = 0, \ldots, m-1$. 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 3.1.4 gives 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 3.1.5. *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 3.1.6.

- Let R be an integral domain 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.

- $\mathbb{Z}$ and $\mathbb{Z}[\omega]$ are integrally closed.
- $\mathbb{Z}[x]$ is 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 3.1.7. *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

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0, \tag{4}$$

for $a_{n-1}, \ldots, a_0 \in R$. 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. Multiply (4) by b^n,

$$a^n + a_{n-1}a^{n-1}b + \cdots + a_0 b^n = 0 \qquad \Longrightarrow \qquad b\left(a_{n-1}a^{n-1}b + \cdots + a_0\right) = -a^n,$$

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 3.1.8. *Let $R \subset S$ be an inclusion of integral domains. 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 $\mathbb{Z}[i], \mathbb{Z}[\omega], \mathbb{Z}\left[\sqrt{-5}\right]$.

3.2 Number 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 3.2.1. *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 $\alpha, \beta \in \mathbb{Q}$.

$$x = \frac{\alpha \pm \sqrt{\alpha^2 + 4\beta}}{2}.$$

$d = \alpha^2 + 4\beta \in \mathbb{Q}$, 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 3.2.2. *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

$$x = a + b\sqrt{d} \mapsto \overline{x} = a - b\sqrt{d}.$$

$x, \overline{x}$ 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 $4b^2 d \in \mathbb{Z}$ gives $2b \in \mathbb{Z}$, 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

3.3 Trace and norm

Lecture 14
Monday
11/02/19

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

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

Then

$$Tr: \begin{array}{ccc} K & \to & \mathbb{Q} \\ \alpha & \mapsto & \alpha + \overline{\alpha} \end{array}, \qquad Nm: \begin{array}{ccc} K & \to & \mathbb{Q} \\ \alpha & \mapsto & \alpha \cdot \overline{\alpha} \end{array},$$

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 2. 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 3.3.1. *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

$$\sigma: \begin{array}{ccc} K & \to & \mathbb{C} \\ x & \mapsto & \sigma(x) = \alpha \end{array},$$

where $\sigma|_F = id_F$. 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 3.3.1.

Let $x \in K$. Think of

$$\begin{array}{ccc} K & \to & K \\ y & \mapsto & x \cdot y \end{array}$$

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

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

for all $x \in K$.

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

$$\begin{array}{ccc} K & \to & \mathbb{C} \\ x & \mapsto & \alpha \end{array}$$

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 3.3.3. $Tr : K \to F$ 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 3.3.4. *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 3.3.5. *Let K, F, S, R as in Theorem 3.3.4. 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 3.3.4. 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 $x \in S$ gives $P(t) \in R[t]$, so $\sigma(x) \in T$. The coefficients of $char_{K/F}(x)$ are symmetric polynomials in the $\sigma(x)$,

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

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 3.3.6. *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 $Nm : \mathcal{O}_K \to \mathbb{Z}$.*

3.4 Bilinear forms

Definition 3.4.1. Let V be a finite dimensional $\mathbb{Q}$-vector space. A function

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

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 $V = \mathbb{Q}$.
$$\begin{array}{ccc} V \times V & \to & \mathbb{Q} \\ (v, w) & \mapsto & 0 \end{array}$$
is symmetric and bilinear.
- Let $V = \mathbb{Q}^2$.
$$\begin{array}{ccc} V \times V & \to & \mathbb{Q} \\ (v, w) & \mapsto & \langle v, w \rangle = v \cdot w = v \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} w^t \end{array}$$
is the inner product, which is non-degenerate.
- Let $K/\mathbb{Q}$ be quadratic.
$$\begin{array}{rccc} Tr_{K/\mathbb{Q}}(,) : & K \times K & \to & \mathbb{Q} \\ & (x, y) & \mapsto & Tr_{K/\mathbb{Q}}(x \cdot y) \in \mathbb{Q} \end{array}$$
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 $x, y \in \mathbb{Z}[i]$ gives $Tr_{\mathbb{Q}(i)/\mathbb{Q}}(x, y) \in \mathbb{Z}$.

3.5 Lattices

Lecture 16
Friday
15/02/19

Definition 3.5.1. 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 3.5.2. *Let $M \subseteq V$ be a lattice. If $e_1, \ldots, e_n$ is a $\mathbb{Z}$-basis for M then $e_1, \ldots, e_n$ is a $\mathbb{Q}$-basis for V.*

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

$$a_1' e_1 + \cdots + a_n' e_n = 0,$$

where $a_1', \ldots, a_n' \in \mathbb{Z}$, 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 3.5.3. *$M^V \subseteq V$ 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

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

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

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

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

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

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

  $$w = a_1 e_1^V + \cdots + a_n e_n^V = 0,$$

  where $a_i \in \mathbb{Z} \subseteq \mathbb{Q}$, 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 $v \in M$. $v \in M$ gives

  $$v = b_1 e_1 + \cdots + b_n e_n,$$

  where $b_i \in \mathbb{Z}$, so $\left\langle v, e_i^V \right\rangle = b_i \in \mathbb{Z}$.

- For all $w \in M^V \subseteq V$,

  $$w = c_1 e_1^V + \cdots + c_n e_n^V,$$

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

□

3.6 Main result

Theorem 3.6.1. *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. Idea is

1. find lattice $M \subseteq \mathcal{O}_K$, and
2. show $M^V \supseteq \mathcal{O}_K$, 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.

   $$e_i^n + \alpha_1 e_i^{n-1} + \cdots + \alpha_{n-1} = 0,$$

   for $\alpha_1, \ldots, \alpha_{n-1} \in \mathbb{Q}$. Multiply equation by n-th power A^n of denominators of α_i. Let $e_i' = Ae_i$, so

   $$(Ae_i)^n + (A\alpha_1)(Ae_i)^{n-1} + \cdots + (A^n\alpha_{n-1}) = 0,$$

   for $A\alpha_1, \ldots, A^n\alpha_{n-1} \in \mathbb{Z}$. 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 3.5.3. 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 $Tr_{K/\mathbb{Q}}|_{\mathcal{O}_K}: \mathcal{O}_K \to \mathbb{Z} \subset \mathbb{Q}$.

□