M3P15 Algebraic Number Theory

Lectured by Dr Ana Caraiani
Typeset by David Kurniadi Angdinata

Spring 2019

Contents

0 Motivation and overview **3**

1 Rings **5**

2 Integral domains **7**

3 Unique factorisation domains **8**

4 Principal ideal domains **9**

5 Euclidean domains **9**

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 0.1. *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 0.2. 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 $i = 1, \dots, r$. If every $p \equiv 1 \mod 4$ is of the form $p = a^2 + b^2$, then we understand the general case,

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

Theorem 0.3. *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 0.4 (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 0.5 (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 0.6 (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 0.7 (Euclid's lemma)**.** *If $p \in \mathbb{Z}$ is prime, then*

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

Proof of Theorem 0.4.

- 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. $n = p_2 \dots p_n = q_2 \dots q_?$ Euclid's lemma gives $p_1 \mid q_1$, up to reordering, so $p_1 = \pm q_1$, and continue.

□

Lecture 2
Monday
14/01/19

1 Rings

Definition 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 1.2.

- $\mathbb{Z}^\times = \{\pm 1\}$.
- $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$.
- $\mathbb{Z}\left[\sqrt{2}\right]^\times \supseteq \{\pm 1, \epsilon^n\}$, 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 1.3. 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 $ax \in I$.

A fact is that 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 1.4. *R/I has ring structure induced by*

$$\begin{aligned}(a+I)+(b+I) &= (a+b)+I,\\ (a+I)\cdot(b+I) &= (a\cdot b)+I,\end{aligned}$$

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 1.5 (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 1.6. 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 $Ker\left(\phi\right) = I$, then result follows from Theorem 1.5. Such a ϕ would have to satisfy
$$\phi\left(4-\sqrt{5}\right) = 0, \qquad \phi\left(11\right) = 0.$$
$\phi\left(\sqrt{5}\right) = \phi\left(4\right) = 4 \mod 11.$
$$\begin{array}{cccc} \phi : & \mathbb{Z} \oplus \mathbb{Z}\left[\sqrt{5}\right] & \to & \dfrac{\mathbb{Z}}{11\mathbb{Z}} \\ & \sqrt{5} & \mapsto & 4 \end{array}.$$
Still have to check that
$$16 = \phi\left(5\right)^2 = \phi\left(\sqrt{5}^2\right) = \phi\left(5\right) = 5 \mod 11.$$
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 $\langle 9, 4-\sqrt{5}\rangle = R$.

Definition 1.7.

- If I, J are ideals in a ring R, we say that I **divides** J if $J \subseteq I$.
- We can form ideals
$$\begin{aligned} I \cap J &= \left\{r \mid r \in I,\ r \in J\right\}, \\ I + J &= \left\{r + s \mid r \in I,\ s \in J\right\}, \\ I \cdot J &= \left\{\sum_{i=1}^{n} r_i s_i \;\middle|\; r_i \in I,\ s_i \in J,\ i = 1, \dots, n\right\}. \end{aligned}$$
- I, J are said to be **relatively prime** if $I + J = R$.

Theorem 1.8 (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 1.9. If $R = \mathbb{Z}$, all ideals are principal and Theorem 1.8 specialises to usual Chinese remainder theorem.

Proof. Find surjective ring homomorphism
$$\begin{array}{ccc} R & \to & \dfrac{R}{I} \times \dfrac{R}{J} \\ r & \mapsto & \left(r \mod I, r \mod J\right) \end{array},$$
with kernel $I \cdot J$. ∎

Definition 1.10. A ring R is **Noetherian** if it satisfies the **ascending chain condition** on ideals, that is any infinite sequence of ideals
$$I_1 \subseteq I_2 \subseteq \dots$$
stabilises.

Example 1.11. $\mathbb{Z}$ and $\mathbb{Z}\left[x\right]$ are Noetherian. $\mathbb{Z}\left[x_1, x_2, \dots\right]$ is not Noetherian.

Lecture 3
Tuesday
15/01/19

2 Integral domains

Definition 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 2.2.

- $\mathbb{Z}$ 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 2.3. 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 2.4. *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 2.5. 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 $R^\times$, and
- 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 2.6. 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 2.7. If $a \in R \setminus \{0\}$ is irreducible, a does not have to be prime.

Example 2.8. $\mathbb{Z}\left[\sqrt{-5}\right] = \left\{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\right\}$ 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
$$N : \begin{array}{ccc} \mathbb{Z}\left[\sqrt{-5}\right] & \to & \mathbb{Z}_{\geq 0} \\ a + \sqrt{-5}b & \mapsto & \left(a + \sqrt{-5}b\right)\left(a - \sqrt{-5}b\right) = a^2 + 5b^2 \end{array},$$
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.

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

Example 3.2. $\mathbb{Z}$, but not $\mathbb{Z}\left[\sqrt{-5}\right]$.

Lemma 3.3. *If R is a UFD, then $p \in R \setminus \{0\}$ is irreducible gives p is prime.*

Proof. Exercise. □

Theorem 3.4. *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*
$$\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \dots$$
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 3.5. *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 $a = u \cdot p_1 \cdot \dots \cdot p_{d(a)}$ and $b = v \cdot q_1 \cdot \dots \cdot q_{d(b)}$. $a \mid b$ gives $b = a \cdot c$ for $c \in R \setminus \{0\}$. Let $c = w \cdot r_1 \cdot \dots \cdot r_{d(c)}$.
$$v \cdot q_1 \cdot \dots \cdot q_{d(b)} = u \cdot w \cdot p_1 \cdot \dots \cdot p_{d(a)} \cdot r_1 \cdot \dots \cdot r_{d(c)}.$$
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 3.4.

$\implies$ Assume R is a UFD. Irreducibles are prime. Let
$$\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \dots \qquad \implies \qquad \dots \mid a_2 \mid a_1 \qquad \implies \qquad d(a_1) \geq \dots \geq 0.$$
This sequence stabilises after finitely many steps. There exists n such that
$$d(a_n) = d(a_{n+1}) = \dots \qquad \implies \qquad a_n \sim a_{n+1} \sim \dots \qquad \implies \qquad \langle a_n \rangle = \langle a_{n+1} \rangle = \dots.$$

$\impliedby$ 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,
$$\langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \dots.$$
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
$$a = u \cdot p_1 \cdot \dots \cdot p_r = v \cdot q_1 \cdot \dots \cdot q_s.$$
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 3.6. $\mathbb{Z}\left[\sqrt{-5}\right]$ is not a UFD because 2 is irreducible but not prime.

4 Principal ideal domains

Definition 4.1. An ID R is a **principal ideal domain (PID)** if every ideal of R is principal.

Example 4.2.

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

Theorem 4.3. *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.

$\square$

Remark 4.4.

- $\mathbb{Z}\left[\sqrt{-5}\right]$ is not a PID. Follows from Theorem 4.3 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.

5 Euclidean domains

Definition 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
  - $\phi(r) < \phi(b)$, or
  - $r = 0$.
- 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 5.2. *A Euclidean domain is a principal ideal domain.*

Example 5.3. $\mathbb{Z}$ with Euclidean norm $b \mapsto |b|$.