Contents

Part I

Linear Algebra

Part II

Field Theory

Part III

Ring Theory

Chapter 1

Anatomy of Rings

1.1 Rings and Objects

1.2 Operations

* polynomial * quotient * kartesian product

1.3 Properties

* noether * artinian * local

1.4 Types

1.4.1 Integral Domains

Definition 1. An integral domain A is a nonzero commutative ring that meets one of the following equivalent conditions.

1. The product of any two nonzero elements of A is nonzero, i.e. if $a \in A \setminus \{0\}$ and $b \in A \setminus \{0\}$, then $ab \neq 0$.
2. The only zero divisor in A is 0, i.e. $\mathrm{ZD}(A) = \{0\}$.
3. The zero ideal (0) is a prime ideal in A.

Proposition 2. If A is a nonzero ring, then $A \times A$ is not an integral domain.

Proposition 3. Let A be a ring, and $\mathfrak{p} \subset A$ an ideal. $\mathfrak{p}$ is prime if and only if $A/\mathfrak{p}$ is an integral domain.

Example 3.1. The quotient of an integral domain by an arbitary ideal need not be an integral domain.

Proposition 4. If A is an integral domain, then $A[X_1, \ldots, X_n]$ for all $n \in \mathbb{N}$ is an integral domain.

Example 4.1. An integral domain need not be Noetherian and Noetherian rings need not be an integral domain.

Example 4.2. An integral domain need not be Artinian and Artinian rings need not be an integral domain.

Proposition 5. An integral domain is Artinian if and only if it is a field.

Example 5.1. An integral domain need not be local and a local ring need not be an integral domain.

1.4.2 Integrally Closed Domains

1.4.3 Unique Factorization Domains

Proposition 6. If A is a unique factorization domain, then $A[X_1, \ldots, X_n]$ for all $n \in \mathbb{N}$ is a unique factorization domain.

1.5 Appendix: Integrally Closed Domains

Example 6.1. $\mathbb{Q}[X,Y]/(Y^2 - X^3)$ is an integral domain, but it is not integrally closed.

Proof. Denote $A = \mathbb{Q}[X,Y]/(Y^2 - X^3)$. A is an integral domain, because A is a quotient of a polynomial ring with coefficients in an integral domain $\mathbb{Q}$.

Now, to show that A is not integrally closed, consider

$$p(X,Y) := \frac{Y}{X} \in \mathrm{Frac}(A).$$

If $p \in A$, then there are $f, g \in \mathbb{Q}[X,Y]$ with

$$Y = Xf(X,Y) + g(X,Y)(Y^2 - X^3)$$

□

1.6 Appendix: Unique Factorization Domain

Example 6.2. $\mathbb{Z}[\sqrt{-5}]$ is not a unique factorization domain.

Proof. □

1.7 Appendix: Principal Ideal Domain

1.8 Appendix: Euclidean Domain

Example 6.3. Let $A = \mathbb{Z}[i]$, then A is an Euclidean domain.

Proof. First, we define the Euclidean function to be

$$\phi : A \setminus \{0\} \longrightarrow \mathbb{N}_0, \quad x = a + ib \mapsto \phi(x) := a^2 + b^2$$

for some $a, b \in \mathbb{Z}$. Let $\alpha = a + ib \in \mathbb{Z}[i]$ and $\beta = c + id \in \mathbb{Z}[i]$ with $a, b, c, d \in \mathbb{Z}$. Consider

$$\frac{\alpha}{\beta} = \frac{a+ib}{c+id} = \frac{a+ib}{c+id} \cdot \frac{c-id}{c-id} = \underbrace{\frac{ac+bd}{c^2+d^2}}_{=:\lambda} + i \underbrace{\frac{bc-ad}{c^2+d^2}}_{=:\mu}.$$

Define $n \in \mathbb{Z}$ to be the integer closest to λ and $m \in \mathbb{Z}$ to be the integer closest to μ. Now, set $q := n + im$ and $r := x - yq$. Then,

$$\phi(r) = \phi(x - yq) = \phi\left(\frac{x}{y} - q\right)\phi(y) = \phi\left(\lambda + i\mu - n + im\right)\phi(y) = \phi\left(\lambda - n + i(\mu - m)\right)\phi(y).$$

Because of the construction, it is

$$|\lambda - n| < \frac{1}{2} \quad \text{and} \quad |\mu - m| < \frac{1}{2},$$

hence

$$\phi(\lambda - n + i(\mu - m)) < \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2}$$

and thus

$$\phi(r) = \phi(\lambda - n + i(\mu - m))\phi(y) < \phi(y)$$

as desired. For a given $x, y \in \mathbb{Z}[i]$, we found $q, r \in \mathbb{Z}[i]$ such that $x = yq + r$ with either $r = 0$ or $\phi(r) < \phi(y)$, therefore $\mathbb{Z}[i]$ is an Euclidean domain. □

Example 6.4. $\mathbb{Z}[\sqrt{3}]$ is an Euclidean domain with the Euclidean function

$$\phi : \mathbb{Z}[\sqrt{3}] \longrightarrow \mathbb{N}_0, \quad a + b\sqrt{3} \mapsto |a^2 - 3b^2|$$

where $a, b \in \mathbb{Z}$ are integers.

Example 6.5. $\mathbb{Z}[\sqrt{-2}]$ is an Euclidean domain.

Proof. Define the Euclidean function to be

$$\phi : \mathbb{Z}[\sqrt{-2}] \setminus \{0\} \longrightarrow \mathbb{N}_0, \quad a + ib \mapsto a^2 + 2b^2$$

for some $a, b \in \mathbb{Z}$. Let $x = a + b\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$ and $y = c + d\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$ where $a, b, c, d \in \mathbb{Z}$ are integers. Consider

$$\frac{x}{y} = \frac{a+b\sqrt{-2}}{c+d\sqrt{-2}} = \frac{a+b\sqrt{-2}}{c+d\sqrt{-2}} \cdot \frac{c-d\sqrt{-2}}{c-d\sqrt{-2}} = \underbrace{\frac{ac+2bd}{c^2+2d^2}}_{=:\lambda} + \underbrace{\left(\frac{bd-ad}{c^2+2d^2}\right)}_{=:\mu}\sqrt{-2}.$$

Define $n \in \mathbb{Z}$ to be the integer closest to λ and $m \in \mathbb{Z}$ to be the integer closest μ. Now set $q := n + m\sqrt{-2}$ and $r := x - yq$. Then,

$$\begin{aligned}\phi(r) &= \phi(x - yq) \\ &= \phi\left(\frac{x}{y} - q\right)\phi(y) \\ &= \phi(\lambda + \mu\sqrt{-2} - n - m\sqrt{-2})\phi(y) \\ &= \phi(\lambda - n + (\mu - m)\sqrt{-2})\phi(y).\end{aligned}$$

Because of the construction, it is

$$|\lambda - n| < \frac{1}{2} \quad \text{and} \quad |\mu - m| < \frac{1}{2},$$

hence

$$\phi(\lambda - n + (\mu - m)\sqrt{-2}) < \left(\frac{1}{2}\right)^2 + 2\left(\frac{1}{2}\right)^2 = \frac{3}{4}$$

and thus

$$\phi(r) = \phi(\lambda - n + i(\mu - m))\phi(y) < \phi(y)$$

as desired. For a given $x, y \in \mathbb{Z}[i]$, we found $q, r \in \mathbb{Z}[i]$ such that $x = yq + r$ with either $r = 0$ or $\phi(r) < \phi(y)$, therefore $\mathbb{Z}[i]$ is an Euclidean domain. □

Example 6.6. Let $A = \mathbb{Z}[\alpha]$ where

$$\alpha = \frac{1 + \sqrt{-7}}{2}$$

then A is an Euclidean domain.

Proof. □

https://math.stackexchange.com/questions/998716/proof-that-mathbbz-left-frac1-sqrt-192-right-is-a-pid

Example 6.7. Let $K = \mathbb{Q}(\sqrt{-19})$, then the ring of integers of K consisting of

$$\frac{a + b\sqrt{-19}}{2},$$

where $a, b \in \mathbb{Z}$ are integers both even or both odd, is a principal ideal domain that is not Euclidean.

Part IV

Number Theory

Chapter 2

Ring of Integers

Example 6.8. Let $d \in \mathbb{Z}$ square-free, and let $K = \mathbb{Q}(\sqrt{d})$. The ring of integers of K is $\mathcal{O}_K = \mathbb{Z}[\alpha]$ where

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

Proof. By definition, the ring of integers is

$$\mathcal{O}_K = \left\{ a + b\sqrt{d} \in K \mid a, b \in \mathbb{Q},\, p(a + b\sqrt{d}) = 0 \right\},$$

where $p \in \mathbb{Z}[X]$ is a monic polynomial with coefficients in $\mathbb{Z}$. Consider $a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ with $a, b \in \mathbb{Q}$ and $b \neq 0$. The minimal polynomial of $a + b\sqrt{d}$ is of degree 2. It is

$$(a + b\sqrt{d})^2 = 2ab\sqrt{d} + a^2 + b^2 d.$$

In the first step, we want to cancel $\sqrt{d}$ from $2ab\sqrt{d}$ by adding a suitable multiple of $a + b\sqrt{d}$, i.e. if $n \in \mathbb{Z}$, then

$$2ab\sqrt{d} + n(a + b\sqrt{d}) \in \mathbb{Q}.$$

Choose $n := -2a$, then

$$2ab\sqrt{d} - 2a(a + b\sqrt{d}) = -2a^2.$$

Going back, we have

$$(a + b\sqrt{d})^2 - 2a(a + b\sqrt{d}) = -a^2 + b^2 d,$$

thus, it is

$$(a + b\sqrt{d})^2 - 2a(a + b\sqrt{d}) + a^2 - b^2 d = 0.$$

This gives us the minimal polynomial of $a + b\sqrt{d}$ is $m(X) = X^2 - 2aX + a^2 - b^2 d$. However, a, b where in $\mathbb{Q}$, but $-2a$ and $a^2 - b^2 d$ must lie in $\mathbb{Z}$ in order for $a + b\sqrt{d}$ to be in the ring of integers $\mathcal{O}_K$.

Firstly, if $2a$ is odd, then we may write $2a = 2k + 1$ for some $k \in \mathbb{Z}$, and we have

$$a^2 - b^2 d = \frac{(2a)^2 - 4b^2 d}{4} = \frac{4k^2 + 4k + 1 - 4b^2 d}{4}.$$

In the equation above, b cannot be an integer, so it must be $2b = 2i + 1$, and it is

$$= \frac{4k^2 + 4k + 1 - (2b)^2 d}{4} = \frac{4k^2 + 4k + 1 - (2i+1)^2 d}{4} = \frac{4k^2 + 4k + 1 - 4i^2 d - 4id - d}{4}$$

Not done, but something like this. □

Example 6.9.

Chapter 3

The Trace, the Norm, and the Discriminant

Definition 7. A prime number $p \in \mathbb{N}$ is said to be ramified in an algebraic number field K if the prime ideal factorization

$$(p) = p\mathcal{O}_K = \mathfrak{p}_r^{e_1} \cdots \mathfrak{p}_r^{e_r}$$

has some e_i greater than 1. If every e_i equals 1 for $1 \leq i \leq r$, we say p is unramified in K.

Example 7.1. In $\mathbb{Z}[i]$, 2 ramifies because $(1+i)^2 = (2)$, and it is the only prime to do so.

Theorem 8. For an algebraic number field K, the primes which ramify are those dividing the integer $\mathrm{disc}_{\mathbb{Z}}(\mathcal{O}_K)$. In particular, only finitely many primes ramify.

Chapter 4

Dedekind Domain

Chapter 5

The Ideal Class Group

Definition 9 (Fractional Ideals)**.** Let R be a integral domain with fraction field F. A fractional ideal is a nonzero R-submodule $\mathcal{A} \subseteq F$ such that $d\mathcal{A} \subseteq R$ for some nonzero $d \in A$.

Remark. We say integral ideals of R and simply mean ideals of R to distinguish them from fractional ideals which are, despite its name and similarities, not true ideals.

Definition 10 (Equivalence of Fractional Ideals)**.** Let R be a integral domain. Two fractional ideals $\mathcal{A}$ and $\mathcal{B}$ of R are said to be equivalent if there exist α and β in R such that

$$(\alpha)\mathcal{A} = (\beta)\mathcal{B}.$$

In this case, we write $\mathcal{A} \sim \mathcal{B}$ or simply $\mathcal{A} = \mathcal{B}$.

Proposition 11. The relation defined above $\mathcal{A} \sim \mathcal{B}$ is indeed a equivalence relation.

Proof. Let $\mathcal{A}$ and $\mathcal{B}$ be two fractional ideals of an integral domain R. We show that the relation $\mathcal{A} \sim \mathcal{B}$ as defined above is a equivalence relation.

1. **Reflexivity.** Trivially, $(\alpha)\mathcal{A} = (\alpha)\mathcal{A}$ for any $\alpha \in R$, and we have $\mathcal{A} \sim \mathcal{A}$.

2. **Symmetry.** If $\mathcal{A} \sim \mathcal{B}$, then $(\alpha)\mathcal{A} = (\beta)\mathcal{B}$, and again it is trivial that $(\beta)\mathcal{B} = (\alpha)\mathcal{A}$, hence $\mathcal{B} \sim \mathcal{A}$.

3. **Transitivity.** Let $\mathcal{A} \sim \mathcal{B}$ and $\mathcal{B} \sim \mathcal{C}$ hold. There are $\alpha, \beta, \gamma, \theta \in R$ such that

   $$(\alpha)\mathcal{A} = (\beta)\mathcal{B} \quad \text{and} \quad (\gamma)\mathcal{B} = (\theta)\mathcal{C}.$$

   Multiplying both sides of both equalities by (γ) and (β) respectively yields

   $$(\gamma)(\alpha)\mathcal{A} = (\gamma)(\beta)\mathcal{B} \quad \text{and} \quad (\beta)(\gamma)\mathcal{B} = (\beta)(\theta)\mathcal{C}.$$

   Therefore, we have that $(\alpha\gamma)\mathcal{A} = (\beta\theta)\mathcal{C}$ or in other words $\mathcal{A} \sim \mathcal{C}$.

□

Definition 12. Let K be an algebraic number field. The equivalence classes of ideals of R form a group called the ideal class group of K or just class group of K, and write it as $\mathrm{Cl}(K)$.

Theorem 13. Let K be an algebraic number field.

1. The ideal class group is indeed an abelian group with ideal multiplication as its operation. $[(1)] = [R]$ is the identity element and
2. Each ideal class has an integral ideal representant.
3. The ideal class group is trivial, i.e. $\mathrm{Cl}(K) = [(1)]$, if and only if all fractional ideals in K are principal, which is equivalent to $\mathcal{O}_K$ being a principal ideal domain.
4. The ideal class group of K is finite.

Remark.
1. For some integral domains not all fractional ideals are invertible, so not all ideal classes are invertible. In other words, the ideal classes need not be a group for arbitary integral domains.
2. For Dedekind domains fractional ideals are invertible, so the ideal classes form a group, but they need not be finite.
3. For a Dedekind domain R, the group $\mathrm{Cl}(R)$ is trivial if and only if R is a principal domain which is equivalent to R being a unique factorization domain, so $\mathrm{Cl}(R)$ is a measure of how far R is from having unique factorization of elements.
4. Every abelian group is isomorphic to the ideal class group of some Dedekind domain.
5. It is believed that every finite abelian group is isomorphic to the ideal class group of some algebraic number field, but this is unsolved.
6. If R is Dedekind, $\mathrm{Cl}(R)$ can be regarded as a quotient Group
$$\mathrm{Cl}(R) = \{\text{ fractional } R\text{-ideals }\} / \{\text{ principal fractional } R\text{-ideals }\}$$
7. If all fractional ideal of an integral domain is invertible, then it is a Dedekind domain.

Definition 14. The Kronecker Bound (or Hurwitz bound?)
$$C = \prod_{\sigma : K \to \mathbb{C}} \sum_{i=1}^{n} |\sigma(e_i)|$$

Theorem 15. The ideal classes of $\mathcal{O}_K$ are

1. represented by ideals in $\mathcal{O}_K$ with norm at most C
2. generated as a group by prime ideals $\mathfrak{p}$ with norm at most C.

Theorem 16. Let K be an algebraic number field of degree n, Δ_K be the discriminant of $K/\mathbb{Q}$, and $2r_2 = n - r_1$ be the number of complex embeddings where r_1 is the number of real embeddings. Then every class in the ideal class group of K contains an integral ideal of norm not exceeding Minowski's bound

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

Moreover, the ideal class group is generated by the prime ideals with the norm not exceeding this bound.

5.1 Appendix: Computation of Some Ideal Class Groups

$K = \mathbb{Q}(\sqrt{2})$	$M_K \approx 1.41$	$\mathrm{Cl}(K) \cong Z_1$
$K = \mathbb{Q}(\sqrt{3})$	$M_K \approx 1.73$	$\mathrm{Cl}(K) \cong Z_1$
$K = \mathbb{Q}(\sqrt{5})$	$M_K \approx 1.12$	$\mathrm{Cl}(K) \cong Z_1$
$K = \mathbb{Q}(\sqrt{6})$	$M_K \approx 2.45$	$\mathrm{Cl}(K) \cong Z_1$
$K = \mathbb{Q}(\sqrt{7})$	$M_K \approx 2.65$	$\mathrm{Cl}(K) \cong Z_1$
$K = \mathbb{Q}(\sqrt{10})$	$M_K \approx 3.16$	$\mathrm{Cl}(K) \cong Z_2$
$K = \mathbb{Q}(\sqrt{11})$	$M_K \approx 3.32$	$\mathrm{Cl}(K) \cong Z_1$
$K = \mathbb{Q}(\sqrt{13})$	$M_K \approx 1.80$	$\mathrm{Cl}(K) \cong Z_1$
$K = \mathbb{Q}(\sqrt{14})$	$M_K \approx 3.74$	$\mathrm{Cl}(K) \cong Z_1$
cell4	cell5	cell6
cell7	cell8	cell9

$K = \mathbb{Q}(i) \quad M_K \approx 1.27 \quad \mathrm{Cl}(K) \cong Z_1$

$K = \mathbb{Q}(\sqrt[3]{2}) \quad M_K \approx 1.41 \quad \mathrm{Cl}(K) \cong Z_1$ |

Remark. If $d \in \mathbb{Z}$ is not a square-free integer, i.e. there is an integer $a \in \mathbb{Z}$ with $a^2 \cdot b = d$ for some intger $b \in \mathbb{Z}$, then

$$\mathbb{Q}\left(\sqrt{d}\right) = \mathbb{Q}\left(a\sqrt{b}\right) = \mathbb{Q}\left(\sqrt{b}\right).$$

Thus, if the algebraic number field is of the form $\mathbb{Q}(\sqrt{d})$, then we will only consider the cases where d is square-free.

Remark. If the Minkowski bound is less than 2, the ideal class group is generated by just one element, the identity, and every (fractional and integral) ideals are equivalent to (1). In such a case, the ideal class group is trivial, i.e. it is isomorphic to the cyclic group of order 1.
There are algebraic number fields with a Minkowski bound not less than 2 that have trivial ideal class groups, e.g. $\mathbb{Q}(\sqrt{6})$. In other words, a Minkowski bound of 2 or more does not guarantee that the algebraic number field has a trivial ideal class group.

Example 16.1. Let $K = \mathbb{Q}(\sqrt{6})$. Then, $M_K \approx 2.45$ and $\mathrm{Cl}(K) \cong Z_1$.

Proof. 6 is congruent to 2 modular 4, thus the discriminant is $\Delta_K = 4 \cdot 6$. There are $r_2 = 0$ complex embeddings and the degree of the algebraic number field K is 2. Then, the Minkowski bound is

$$M_K = \sqrt{4 \cdot 6} \left(\frac{4}{\pi}\right)^0 \frac{2}{4} = \sqrt{6} \approx 2.45.$$

Hence, the ideal (2) is of interest. It is

$$X^2 - 6 \equiv X^2 \mod 2.$$

Thus, $(2) = (2, \sqrt{6})^2$ where $(2, \sqrt{6})$ is a prime ideal in $\mathcal{O}_K$.

We want to show that $(2, \sqrt{6})$ is principal. If there is a common divisor x of 2 and $\sqrt{6}$, then its norm must divide $\mathrm{N}(2) = 4$ and $\mathrm{N}(\sqrt{6}) = -6$. Hence $\mathrm{N}(x) = \pm 2$. This is the same as solving the equation $a^2 - 6b^2 = \pm 2$ for integers. A solution is $a = 2$ and $b = 1$, and indeed $2 + \sqrt{6}$ is a common divisor because $(2+\sqrt{6})(-2+\sqrt{6}) = 2$ and $(2+\sqrt{6})(3-\sqrt{6}) = 6-2\sqrt{6}+3\sqrt{6}-6 = \sqrt{6}$. Therefore, $(2, \sqrt{6}) = (2 + \sqrt{6})$ and the ideal class group is trivial. □

Example 16.2. Let $K = \mathbb{Q}(\sqrt{7})$. Then, $M_K \approx 2.65$ and $\mathrm{Cl}(K) \cong Z_1$.

Proof. We have $7 \equiv 3 \mod 4$, thus the discriminant is $\Delta_K = 4 \cdot 7$. There are $r_2 = 0$ complex embeddings and the degree of the algebraic number field K is $n = 2$. This gives us the Minkowski bound

$$M_K = \sqrt{4 \cdot 7} \left(\frac{4}{\pi}\right)^0 \frac{2}{4} = \sqrt{7} \approx 2.65.$$

We find the prime factorization of the ideal (2). It is

$$X^2 - 7 \equiv X^2 - 1 \equiv X^2 + 1 \equiv (X+1)^2 \mod 2.$$

Thus, $(2) = \mathfrak{p}_2^2$ for some prime ideal $\mathfrak{p}_2$ in $\mathcal{O}_K$. Because (2) is equivalent to the identity (1) in the ideal class group, we know $\mathfrak{p}_2$ has an order not more than 2.

Here, we will use the fact that 2 has a factorization in $\mathcal{O}_K$ namely $2 = (3+\sqrt{7})(3-\sqrt{7})$. It is

$$\frac{3+\sqrt{7}}{3-\sqrt{7}} = \frac{(3+\sqrt{7})^2}{2} = 8 + 3\sqrt{7}.$$

Now, $8 + 3\sqrt{7}$ is a unit because of $(8+3\sqrt{7})(8-3\sqrt{7}) = 1$, thus $3+\sqrt{7}$ and $3-\sqrt{7}$ generate the same ideal. We had $(2) = \mathfrak{p}_2^2$, therefore $\mathfrak{p}_2 = (8+3\sqrt{7})$ which is principal. Hence, $\mathfrak{p}_2 \sim (1)$ and the ideal class group $\mathrm{Cl}(K)$ is isomorphic to the cyclic group of order 1. □

Example 16.3. Let $K = \mathbb{Q}(\sqrt{10})$. Then, the Minkowski bound is $M_K \approx 3.16$ and the ideal class group is $\mathrm{Cl}(K) \cong Z_2$.

Proof. It is $10 \equiv 2 \mod 4$, so the discriminant of K is $\Delta_K = 4 \cdot 10$. There are $r_2 = 0$ complex embeddings, and the degree of the algebraic number field is $n = 2$. This gives us the Minkowski bound of

$$M_K = \sqrt{4 \cdot 10} \left(\frac{4}{\pi}\right)^0 \frac{2}{4} = \sqrt{10} \approx 3.16.$$

Hence there are two ideals to analyse (2) and (3). It is

$$\begin{aligned} X^2 - 10 &\equiv X^2 \mod 2 \\ X^2 - 10 \equiv X^2 - 1 &= (X+1)(X-1) \mod 3. \end{aligned}$$

This gives us the factorizations $(2) = \mathfrak{p}_2^2$ and $(3) = \mathfrak{p}_3\mathfrak{p}_3'$ for some prime ideals $\mathfrak{p}_2$, $\mathfrak{p}_3$, and $\mathfrak{p}_3'$. If $\mathfrak{p}_2$ was principal, then $\mathfrak{p}_2 = (a + b\sqrt{10})$ for some integers $a, b \in \mathbb{Z}$. The norm of $\mathfrak{p}_2$ is 2 because $4 = \mathrm{N}((2)) = (\mathrm{N}(\mathfrak{p}_2))^2$, therefore we would have

$$\begin{aligned} a^2 - 10b^2 &= \pm 2 \\ \iff a^2 &= \pm 2 \mod 5. \end{aligned}$$

It is easy to verify that no such integer a exists, and hence $\mathfrak{p}_2$ is principal.

Now, consider $\mathfrak{p}_2\mathfrak{p}_3$. Taking the norm gives $\mathrm{N}(\mathfrak{p}_2\mathfrak{p}_3) = 6$ and since $\mathrm{N}(2+\sqrt{10}) = -6\mathrm{m}$ we have $\mathrm{p}_2\mathrm{p}_3$ is principal. This also means $\mathrm{p}_2 \sim \mathrm{p}_3$, so $\mathrm{Cl}(\mathbb{Q}(\sqrt{10})) \cong Z_2$. □

Example 16.4. Let $K = \mathbb{Q}(\sqrt{11})$.

Proof. We have $11 \equiv 3 \mod 4$. This gives us the discriminant of K which is $\Delta_K = 4 \cdot 11$. There are $r_2 = 0$ complex embeddings, and the degree of the algebraic number field is $n = 2$. Thus, the Minkowski bound is

$$M_K = \sqrt{4 \cdot 11} \left(\frac{4}{\pi}\right)^0 \frac{2}{4} = \sqrt{11} \approx 3.32.$$

The two ideals to investigate are therefore (2) and (3). It is

$$\begin{aligned} X^2 - 11 \equiv X^2 - 1 \equiv (X+1)(X-1) \mod 2 \\ X^2 - 11 \equiv X^2 - 2 \mod 3. \end{aligned}$$

$X^2 - 2 \mod 3$ is irreducible, therefore (3) is prime. On the other hand, we have a factorization $(2) = \mathfrak{p}_2\mathfrak{p}_2'$ for some prime ideals $\mathfrak{p}_2$ and $\mathfrak{p}_2'$ of $\mathcal{O}_K$. But they are principal as $\mathfrak{p}_2 = (3 + \sqrt{11})$ (because of the norm). Hence, $\mathrm{Cl}(K) \cong Z_1$. □

Example 16.5. Let $K = \mathbb{Q}(\sqrt{14})$. Then, the Minkowski bound is $M_K \approx 3.74$ and the ideal class group is $\mathrm{Cl}(K) \cong Z_1$.

Proof. It is $14 \equiv 2 \mod 4$. Then, the discriminant of K is $\Delta_K = 4 \cdot 14$. There are $r_2 = 0$ complex embeddings, and the degree of the algebraic number field is $n = 2$. This gives us the Minkowski bound of

$$M_K = \sqrt{4 \cdot 14} \left(\frac{2}{\pi}\right)^0 \frac{2}{4} = \sqrt{14} \approx 3.74.$$

We investigate (2) and (3).

$$\begin{aligned} X^2 - 14 \equiv X^2 \mod 2 \\ X^2 - 14 \equiv X^2 - 2 \mod 3. \end{aligned}$$

$X^2 - 2 \mod 3$ is irreducible, hence (3) is already prime. Using the norm, we get that $(2) = \mathfrak{p}_2^2$ with $\mathfrak{p}_2 = (4 + \sqrt{14})$, so $\mathfrak{p}$ is also principal. Therefore the ideal class group is trivial. □

Example 16.6. Let $K = \mathbb{Q}(\sqrt{82})$.

Proof. Since $82 \equiv 2 \mod 4$, the discriminant of K is $\Delta_K = 4 \cdot 82$. There are $r_2 = 0$ complex embeddings and the degree of K is $n = 2$. The Minkowski bound is therefore

$$M_K = \sqrt{4 \cdot 82} \left(\frac{4}{\pi}\right)^0 \frac{2}{4} = \sqrt{82} \approx 9.06.$$

Hence the ideals of interest are (2), (3), (5), and (7). It is

$$\begin{aligned} X^2 - 82 \equiv X^2 \mod 2 \\ X^2 - 82 \equiv X^2 - 1 \equiv (X+1)(X-1) \mod 3 \\ X^2 - 82 \equiv X^2 + 3 \mod 5 \\ X^2 - 82 \equiv X^2 + 2 \mod 7. \end{aligned}$$

I'm not exactly sure why, but $X^2 + 3 \mod 5$ and $X^2 + 2 \mod 7$ are irreducible, so (5) and (7) are already prime and principal.

On the other hand, we have the factorization $(2) = \mathfrak{p}_2^2$ and $(3) = \mathfrak{p}_3\mathfrak{p}_3'$ for some prime ideals $\mathfrak{p}_2$, $\mathfrak{p}_3$ and $\mathfrak{p}_3'$. We immediately have the relation $\mathfrak{p}_2^{-1} \sim \mathfrak{p}_2$ and $\mathfrak{p}_3^{-1} \sim \mathfrak{p}_3'$.

Now, we show that $\mathfrak{p}_2$ is nonprincipal. Suppose it isn't, then $\mathfrak{p}_2 = (a+b\sqrt{82})$ for some $a, b \in \mathbb{Z}$. Since $\mathfrak{p}_2^2$ is principal, we have

$$u\left(a+b\sqrt{82}\right)^2 = 2$$

for some unit $u \in \mathcal{O}_K$. If we take the norms, then □

Example 16.7. Let $K = \mathbb{Q}(\sqrt{-14})$. Then, the Minkowski bound is $M_K \approx 4.76$, and the ideal class group is $\mathrm{Cl}(K) \cong Z_4$.

Proof. Firstly, $-14 \equiv 2 \mod 4$, so the absolute discriminant of K is $|\Delta_K| = 4 \cdot 14$. There are $r_2 = 1$ complex embeddings, and the degree of the algebraic number field K is $n = 2$. Therefore, the Minkowski bound is given by

$$M_K = \sqrt{4 \cdot 14}\left(\frac{4}{\pi}\right)^1 \frac{2}{4} = \frac{4\sqrt{14}}{\pi} \approx 4.76.$$

Thus, the ideals of interest are (2) and (3). Reducing the minimal polynomial of $\sqrt{-14}$ modulo 2 and 3 yields

$$\begin{aligned} X^2 + 14 &\equiv X^2 \mod 2 \\ X^2 + 14 \equiv X^2 + 2 &\equiv (X+1)(X-1) \mod 3. \end{aligned}$$

Hence, we have $(2) = \mathfrak{p}_2^2$ and $(3) = \mathfrak{p}_3\mathfrak{p}_3'$ for some prime ideals $\mathfrak{p}_2$, $\mathfrak{p}_3$, and $\mathfrak{p}_3'$. Suppose $\mathfrak{p}_2$ is not principal, then $\mathfrak{p}_2 = (a+b\sqrt{-14})$, and since $4 = \mathrm{N}((2)) = (\mathrm{N}(\mathfrak{p}_2))^2$ we have $2 = \mathrm{N}(\mathfrak{p}_2) = a^2 + 14b^2$, but this is impossible. Thus, $\mathfrak{p}_2$ is not principal.

On the other hand, we have $\mathrm{N}(\mathfrak{p}_3) = \mathrm{N}(\mathfrak{p}_3') = 3$ because again $9 = \mathrm{N}((3)) = \mathrm{N}(\mathfrak{p}_3)\mathrm{N}(\mathfrak{p}_3')$. Consider $(2+\sqrt{-14})$. Because $\mathrm{N}(2+\sqrt{-14}) = 18$, $\mathfrak{p}_3$ or $\mathfrak{p}_3'$ divides $(2+\sqrt{-14})$, but not both because then (3) would divide $(2+\sqrt{-14})$ which it doesn't. So $(2+\sqrt{-14}) = \mathfrak{p}_2\mathfrak{p}_3^2$ and it is $\mathfrak{p}_3^2 \sim \mathfrak{p}_2^{-1} \sim \mathfrak{p}_2$. □

Example 16.8. Let $K = \mathbb{Q}(\sqrt{-30})$. Then, the Minkowski bound is $M_K \approx$, and the ideal class group is $\mathrm{Cl}(K) \cong Z_2 \times Z_2$.

Proof. It is $-30 \equiv 2 \mod 4$, thus the absolute discriminant of K is $|\Delta_K| = 4 \cdot 30$. There are $r_2 = 1$ complex embeddings, and the degree of the algebraic number field K is $n = 2$. Therefore, the Minkowski bound is given by

$$M_K = \sqrt{4 \cdot 30}\left(\frac{4}{\pi}\right)^1 \frac{2}{4} = \frac{4\sqrt{30}}{\pi} \approx 6.97.$$

The ideals of our interest are (2), (3), and (5). Reducing the minimal polynomial of $\sqrt{-30}$ yields

$$\begin{aligned} X^2 + 30 &\equiv X^2 \mod 2 \\ X^2 + 30 &\equiv X^2 \mod 3 \\ X^2 + 30 &\equiv X^2 \mod 5. \end{aligned}$$

Write $(2) = \mathfrak{p}_2^2$, $(3) = \mathfrak{p}_3^2$, and $(5) = \mathfrak{p}_5^2$ for some prime ideals $\mathfrak{p}_2$, $\mathfrak{p}_3$, and $\mathfrak{p}_5$ in $\mathcal{O}_K$. We know that $\mathfrak{p}_2$, $\mathfrak{p}_3$, and $\mathfrak{p}_5$ are nonprincipal ideals. □

Example 16.9. Let $K = \mathbb{Q}(\sqrt{-65})$. Then, the Minkowski bound is $M_K \approx$, and the ideal class group is $\mathrm{Cl}(K) \cong Z_2 \times Z_4$.

Proof. We have $-65 \equiv 3 \mod 4$, thus the absolute discriminant of K is $|\Delta_K| = 4 \cdot 65$. There are $r_2 = 1$ complex embeddings, and the degree of the algebraic number field K is $n = 2$. Therefore, the Minkowski bound is given by

$$M_K = \sqrt{4 \cdot 65} \left(\frac{4}{\pi}\right) \frac{2}{4} = 10.27.$$

Thus, the ideals of interest are (2), (3), (5), and (7). Reducing the minimal polynomial of $\sqrt{-65}$ modulo 2, 3, 5, and 7 yields

$$\begin{aligned} X^2 + 65 \equiv X^2 + 1 \equiv (X+1)^2 \mod 2 \\ X^2 + 65 \equiv X^2 + 2 \equiv (X+1)(X-1) \mod 3 \\ X^2 + 65 \equiv X^2 \mod 5 \\ X^2 + 65 \equiv X^2 + 2 \mod 7. \end{aligned}$$

Firstly, $X^2 + 2 \mod 7$ is irreducible, so (7) is prime. Write $(2) = \mathfrak{p}_2^2$ and $(5) = \mathfrak{p}_5^2$. Since there are no integer solution for neither $2 = N(\mathfrak{p}_2) = a^2 + 65b^2$ nor $5 = N(\mathfrak{p}_5) = a^2 + 65b^2$, the prime ideals $\mathfrak{p}_2$ and $\mathfrak{p}_5$ are not principal. □

Chapter 6

Fundamental Units

Definition 17. 1. An (additive) subgroup Λ of $\mathbb{R}^m$ is called discrete if any bounded subset of $\mathbb{R}^m$ contains only finitely many elements of Λ.

2. Let $\{\gamma_1, \ldots, \gamma_r\}$ be linearly independent set of vectors of $\mathbb{R}^m$ (so that $r \leq m$). The additive subgroup of $\mathbb{R}^m$ generated by $\gamma_1, \ldots, \gamma_r$ is called lattice of dimension r, generated by $\gamma_1, \ldots, \gamma_r$.

Theorem 18. Any discrete subgroup Λ of $\mathbb{R}^m$ for $m \in \mathbb{N}$ is a lattice.

Proof. If $m = 0$, then the discrete subgroup of $\mathbb{R}^0$ is $\Lambda = \{0\}$, which is a lattice of dimension 0.
Let $m = 1$. □