DEDEKIND RINGS AND IDEAL CLASS GROUP

Seminar on Commutative Algebra

Yassin Mousa

Abstract

This paper refers to the 10th talk in the seminar on Commutative Algebra supervised by Prof. Dr. Moritz Kerz and Dr. Florian Strunk at the University of Regensburg in WS 2016/2017. In the following we will introduce Dedekind domains and the ideal class group and very roughly discuss some applications in algebraic number theory and algebraic geometry.

On the 1st March 1847 Gabriel Lamé took the stage during the proceedings of the Paris academy and the Prussian academy in Berlin and excitedly announced that he found a proof of Fermat's Last Theorem.

Let us very roughly discuss his ideas. It obviously suffices to proof the impossibility of the diophantine equation

$$x^n + y^n = z^n \text{ for } n > 2$$

in the cases were n is either 4 or an odd prime number. Fermat himself proved the case $n = 4$ and proofs for the cases $n = 3, 5, 7$ were also known in 1847 (compare [1, Ch. 1.6 p. 10-14]. These proofs all depended on some algebraic factorization. Lamé's basic idea was to introduce complex numbers to decompose $x^n + y^n$ completely into n linear factors, since with ζ_n a primitive n-th root of unity, the Fermat equation translates to

$$y^n = \prod_{i=1}^{n} (z - \zeta_n^{i-1} x).$$

This is an equation in the integral closure $\mathcal{O}_K$ of $\mathbb{Z}$ in the cyclotomic field $K = \mathbb{Q}(\zeta_n)$. We call $\mathcal{O}_K$ the ring of *algebraic integers* in K. Lamé asserted that the ring $\mathcal{O}_K$ is always factorial and therefore thought he had proven Fermat's Last Theorem.

Liouville took the floor after Lamé. He expressed strong concers on Lamé's claim that unique factorization into primes holds true in the range of complex numbers. Nevertheless, Cauchy thought that there was some likelihood that Lamé would succeed and in the following weeks Cauchy puplished several papers in which he attempted to fill out the gap in Lamé's proof. Finally, after several eventful weeks on May 24, Liouville read into the proceedings a letter from Kummer, that eventually ended the discussion. Kummer confirmed Liouville's doubts about the proof. Three years earlier he had already published results in which he had demonstrated the failure of unique factorization in cases where Lamé had been asserting it was valid. An example that the ring of algebraic integers of a number field in general is not necessary factorial is given by the ring $\mathbb{Z}[\sqrt{-5}]$, which is the ring of algebraic integers of the number field $\mathbb{Q}(\sqrt{-5})$. A non-unique factorization is given by

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

However, in his letter Kummer also indicated that it was possible to save the theory of factorization by introducing a new kind of complex numbers which he called *ideal complex numbers*. Reduced to the above example his fabulous idea was to introduce four *ideal prime numbers* $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4$ sucht that

$$2 = \mathfrak{p}_1\mathfrak{p}_2, \quad 3 = \mathfrak{p}_3\mathfrak{p}_4, \quad (1 + \sqrt{-5}) = \mathfrak{p}_1\mathfrak{p}_3, \quad (1 - \sqrt{-5}) = \mathfrak{p}_2\mathfrak{p}_4.$$

Then the above equation read as

$$6 = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$$

and uniqueness is saved. The problem is, that it is by no means clear, how one can realize Kummer's idea. At least it is not possible to understand *ideal numbers* as elements of a ring extension. Kummer himself described *ideal numbers* as elements of an abelian group and he was able to contribute interesting results on Fermat's Last Theorem.

A much more elegant and beneficial realization is due to Dedekind's ideal theory. Whatever an ideal number $\mathfrak{a}$ should be defined to be, it ought to be linked to the algebraic integers $a \in \mathcal{O}_K$ by a divisibility relation satisfying the following rules

$$\mathfrak{a} \mid a \text{ and } \mathfrak{a} \mid b \Rightarrow \mathfrak{a} \mid a \pm b; \quad \mathfrak{a} \mid a \Rightarrow \mathfrak{a} \mid \lambda a$$

for all elements $a, b, \lambda \in \mathcal{O}_K$. Moreover an ideal number should be determined by the totality of its divisors in $\mathcal{O}_K$. In view of the rules of divisibility, this set is an ideal in $\mathcal{O}_K$. Accordingly *ideal numbers* can be interpreted as the ideals of the ring $\mathcal{O}_K$ and this is the reason, why Dedekind introduced ideals in the first place (See [2, p.117 and p.424 f.]). The divisibility relation $\mathfrak{a} \mid a$ can simply be defined by the inclusion $a \in \mathfrak{a}$ and the divisibility relation $\mathfrak{a} \mid \mathfrak{b}$ by $\mathfrak{b} \subseteq \mathfrak{a}$. In oder to show that those heuristically thoughts really do work out, we need to verify that unique factorization into prime ideals holds

true for the ring $\mathcal{O}_K$. The latter was proven by Dedekind (Compare [2]). (For more details see [3, p.17ff.], [2, p. 19 f., p.112 ff.] and [1, Ch. 4 S. 76 ff.]) We will gain a better understanding of rings with this property by the following

Theorem 1. *For an integral domain R the following conditions are equivalent*

1.) *Every non-zero ideal of R is invertible;*

2.) *R is Noetherian, normal and has dimension at most 1;*

3.) *Every ideal $\mathfrak{a} \subseteq R$ is a finite product of prime ideals (where $\mathfrak{a} = R$ occurs as the empty product).*

Moreover if one of these conditions is satisfied, then the factorization of a non-zero ideal into prime ideals is always unique.

Proof. Assume that every non-zero ideal of R is invertible. Since every invertible ideal is finitely generated, we deduce that R is Noetherian. Then [4, Cor. 14.7] implies that every prime ideal $\mathfrak{p}$ has height one and $R_\mathfrak{p}$ is regular. We know from [4, Cor. 13.6 (b)] that every regular local ring is normal. Since normal is a local property, we derive that R is normal.

Next we assume that R is Noetherian, normal and has dimension at most 1. Then for any non-zero prime ideal $\mathfrak{p}$ the local ring $R_\mathfrak{p}$ is Noetherian and normal. Further, the prime indeals in $R_\mathfrak{p}$ are in one to one correspondence with the prime ideals in R, which lie in $\mathfrak{p}$. Thus $R_\mathfrak{p}$ has dimension at most 1 and therefore is either a field or a discrete valuation ring. Accordingly, $R_\mathfrak{p}$ is locally factorial for all prime ideals $\mathfrak{p}$ and from [4, Thm. 14.8 (a)] we conclude that every height-one prime ideal of R is invertible.

We will use Noetherian Induction to show 3.). Let Σ denote the set of all ideals of R which can not be expressed as a finite product of prime ideals. This set is partially ordered by the inclusion. If Σ is non-empty, then Σ has a maximal element $\mathfrak{a}$, since R is Noetherian. Let $\mathfrak{m}$ be a maximal ideal of R which contains $\mathfrak{a}$. Since $\mathfrak{m} \neq 0$ and R has dimension at most 1, we derive that $\mathfrak{m}$ is a height-one prime ideal, whence it is invertible. Then [4, Lem. 14.9] yields $\mathfrak{a} \subsetneq \mathfrak{a} \cdot \mathfrak{m}^{-1} \subseteq R$. By the maximality of $\mathfrak{a}$, we conclude that $\mathfrak{a} \cdot \mathfrak{m}^{-1}$ is a finite product of prime ideals. But then the same is true for $\mathfrak{a}$. Hence, Σ must be empty.

We now assume that every ideal is a finit product of prime ideals. We will show 1.) in two steps. First we will prove that every invertible prime ideal is maximal and from this fact we will conclude that every non-zero prime ideal is invertible.

So let $\mathfrak{p} \subset R$ be an invertible prime ideal. Assume that there exists an element $a \in R \setminus \mathfrak{p}$, such that $\mathfrak{p} + (a) \neq R$. We find

$$\mathfrak{p} + (a) = \prod_{i=1}^{n} \mathfrak{p}_i \quad \text{and} \quad \mathfrak{p} + (a^2) = \prod_{j=1}^{m} \mathfrak{q}_j$$

with prime ideals $\mathfrak{p}_i$ and $\mathfrak{q}_j$. Computing modulo $\mathfrak{p}$ we derive

$$(\bar{a}) = \prod_{i=1}^{n} \mathfrak{p}_i/\mathfrak{p} \quad \text{and} \quad (\bar{a}^2) = \prod_{j=1}^{m} \mathfrak{q}_j/\mathfrak{p}.$$

Using the isomorphism theorems for residues of modules, we conclude that the ideals $\mathfrak{p}_i/\mathfrak{p}$ and $\mathfrak{q}_j/\mathfrak{p}$ are prime ideals. Next [4, Thm. 14.10] implies that $m = 2n$ and, after renumbering,

$$\mathfrak{q}_{2i}/\mathfrak{p} = \mathfrak{q}_{2i-1}/\mathfrak{p} = \mathfrak{p}_i/\mathfrak{p}.$$

Since $\mathfrak{p}$ is contained in every $\mathfrak{p}_i$ and every $\mathfrak{q}_j$, we find that $\mathfrak{q}_{2i} = \mathfrak{q}_{2i-1} = \mathfrak{p}_i$. Consequently,

$$(\mathfrak{p} + (a))^2 = \mathfrak{p} + (a^2).$$

Further,

$$\mathfrak{p} \subseteq \mathfrak{p} + (a^2) = (\mathfrak{p} + (a))^2 \subseteq \mathfrak{p}^2 + (a).$$

This says that for every element $x \in \mathfrak{p}$ we find elements $y \in \mathfrak{p}^2$ and $z \in R$ with $x = y + za$. Since $za = x - y$ is an element of $\mathfrak{p}$ and a is not, we find that z is an element of $\mathfrak{p}$, i.e

$$\mathfrak{p} \subseteq \mathfrak{p}^2 + \mathfrak{p}(a).$$

Thus,

$$\mathfrak{p} = \mathfrak{p}^2 + \mathfrak{p}(a).$$

Multiplying with $\mathfrak{p}^{-1}$ gives

$$\mathfrak{p} + (a) = R,$$

which contradicts the choice of a.

Now let $\mathfrak{q} \subset R$ be an arbitrary non-zero prime ideal and $a \in \mathfrak{q}$ be non-zero.We have

$$(a) = \prod_{i=1}^{n} \mathfrak{q}_i \subseteq \mathfrak{q}$$

with some prime ideals $\mathfrak{q}_i$. Since (a) is invertible, the same is true for the $\mathfrak{q}_i$'s. Moreover $\mathfrak{q}$ is prime and therefore contains at least one of the $\mathfrak{q}_i$'s, say $\mathfrak{q}_j \subseteq \mathfrak{q}$. By what we have shown before, we know that $\mathfrak{q}_j$ is maximal, whence $\mathfrak{q}_j = \mathfrak{q}$, so $\mathfrak{q}$ is invertible. Alluding to this fact every ideal is a finite product of invertible prime ideals and therefore invertible.

By [4, Thm. 14.10] such a decomposition is always unique. ■

Definition 2. *We call an integral domain R a Dedekind domain if it satisfies one of the properties from the theorem.*

From the theorem we derive some elementary examples for Dedekind domains

Examples. 1.) Every *principal ideal domain* is a Dedekind domain.

2.) If R is a *discrete valuation ring*, then R is a local ring and every ideal can be expressed as a finite power of the maximal ideal. Therefore R is a Dedekind domain.

3.) Let R be a Dedekind domain and $S \subseteq R \setminus 0$ be a multiplicative closed subset. Then $S^{-1}R$ is Noetherian and normal and of dimension at most 1, so $S^{-1}R$ is a Dedekind domain.

We have the following local caracterisation of a Dedekind domain:

Proposition 4. *Let R be a Noetherian integral domain that is not a field. Then the following are equivalent:*

1.) R is a Dedekind domain.

2.) $R_\mathfrak{p}$ is a discrete valuation ring for every prime ideal $\mathfrak{p}$.

3.) $R_\mathfrak{m}$ is a discrete valuation ring for every maximal ideal $\mathfrak{m}$.

Proof. Let R be a Dedekind domain, then for all non-zero prime ideals $\mathfrak{p}$, we find that $R_\mathfrak{p}$ is a Noetherian, normal, local integral domain of dimension 1, whence a discrete valuation ring (See [5, Prop. 9.2]).

Vice versa assume that $R_\mathfrak{m}$ is a discrete valuation ring for every maximal ideal $\mathfrak{m}$. Let $\mathfrak{a}$ be an arbitrary non-zero fractional ideal of R and $\mathfrak{m}$ an arbitrary maximal ideal. Then $\mathfrak{a}$ is finitely generated and $\mathfrak{a}_\mathfrak{m}$ is invertible. Now let $\mathfrak{b} := \mathfrak{a}(R : \mathfrak{a})$. Since $\mathfrak{a}$ is finitely generated, we find that $(R : \mathfrak{a})_\mathfrak{m} = (R_\mathfrak{m} : \mathfrak{a}_\mathfrak{m})$ (Compare [5, Cor. 3.15]), thus $b_\mathfrak{m} = \mathfrak{a}_\mathfrak{m}(R_\mathfrak{m} : \mathfrak{a}_\mathfrak{m})$. Further,

$$(R_\mathfrak{m} : \mathfrak{a}_\mathfrak{m}) = \mathfrak{a}_\mathfrak{m}^{-1}\mathfrak{a}_\mathfrak{m}(R_\mathfrak{m} : \mathfrak{a}_\mathfrak{m}) \subseteq \mathfrak{a}_\mathfrak{m}^{-1}.$$

This yields $\mathfrak{a}_\mathfrak{m}(R_\mathfrak{m} : \mathfrak{a}_\mathfrak{m}) \subseteq R_\mathfrak{m}$, whence $b_\mathfrak{m} = R_\mathfrak{m}$. Alluding to this fact we find that $\mathfrak{b} \cap (R \setminus \mathfrak{m})$ is non empty for every maximal ideal $\mathfrak{m}$, so $\mathfrak{b}$ contains a unit and is therefore equal to R and we arrive that R is a Dedekind domain. ■

Proposition 5. *The ring of integers in an algebraic number field K is a Dedekind domain.*

Proof. We will show that $\mathcal{O}_K$ is Noetherian and normal and has dimension at most one. We will use without a proof that $\mathcal{O}_K$ admits an *integral basis*, wich says that $\mathcal{O}_K$ is a finitely generated free $\mathbb{Z}$-module (See [3, Ch. I, Prop. 2.10]). As a consequence we derive that $\mathcal{O}_K$ is Noetherian. Furthermore it is clear that $\mathcal{O}_K$ is normal, so it remains to show that $\mathcal{O}_K$ has dimension at most one. Let $\mathfrak{p} \subset \mathcal{O}_K$ be an arbitrary non-zero prime

ideal and let x be a non-zero element of $\mathfrak{p}$. Since x is integral over $\mathbb{Z}$, it satisfies an equation of the form

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0 \text{ with certain } a_i \in \mathbb{Z}.$$

Using that $\mathcal{O}_K$ is an integral domain, we can assume without loss of generality that a_n is non-zero. Hence, $\mathfrak{q} := \mathbb{Z} \cap \mathfrak{p}$ is a non-zero prime ideal of $\mathbb{Z}$, so $\mathfrak{q}$ is a maximal ideal. Then $\mathcal{O}_K/\mathfrak{p}$ is integral over $\mathbb{Z}/\mathfrak{q}$ (by [5, Prop. 5.6]). Therefore $\mathcal{O}_K/\mathfrak{p}$ is a field if and only if $\mathbb{Z}/\mathfrak{q}$ is a field (by [5, Prop. 5.7]), so $\mathfrak{p}$ is maximal. ■

Proposition 6. *Let R be a Dedekind domain. Every non-zero fractional ideal $\mathfrak{a}$ can uniquely be written in the form*

$$\mathfrak{a} = \prod_{\substack{\mathfrak{p} \\ \text{prime ideal}}} \mathfrak{p}^{\nu_\mathfrak{p}(\mathfrak{a})},$$

where the $\nu_\mathfrak{p}(\mathfrak{a})$ are integers such that, for given $\mathfrak{a}$, the integers $\nu_\mathfrak{p}(\mathfrak{a}) \neq 0$ are finite in number. Furthermore, $\mathfrak{a}$ lies in R if and only if all $\nu_\mathfrak{p}(\mathfrak{a})$ are non-negative. Let $\mathfrak{b}$ be another fractional ideal. In order that $\mathfrak{a} \subseteq \mathfrak{b}$, it is necessary and sufficient that $\nu_\mathfrak{p}(\mathfrak{a}) \geqslant \nu_\mathfrak{p}(\mathfrak{b})$ for all prime ideals $\mathfrak{p}$. Moreover, we have the following relations:

i.) $\nu_\mathfrak{p}(\mathfrak{ab}) = \nu_\mathfrak{p}(\mathfrak{a}) + \nu_\mathfrak{p}(\mathfrak{b})$;

ii.) $\nu_\mathfrak{p}(\mathfrak{a} + \mathfrak{b}) = \min(\nu_\mathfrak{p}(\mathfrak{a}), \nu_\mathfrak{p}(\mathfrak{b}))$;

iii.) $\nu_\mathfrak{p}(\mathfrak{a} \cap \mathfrak{b}) = \max(\nu_\mathfrak{p}(\mathfrak{a}), \nu_\mathfrak{p}(\mathfrak{b}))$.

Proof. Let $\mathfrak{a}$ be a fractional ideal. We find an element $d \in R$, such that $\mathfrak{a}\dot{(}d)$ is an ideal. Then we can factor $\mathfrak{a}(d)$ and (d) into prime ideals. Hence, $\mathfrak{a}$ can be written in the above form. Uniqueness can be easily deduced from the uniqueness of the factorization into prime ideals.

If all the $\nu_\mathfrak{p}(\mathfrak{a})$'s are non-negative, then $\mathfrak{a}$ is an ideal. Vice versa let $\mathfrak{q}$ be a prime ideal with $\nu_\mathfrak{q}(\mathfrak{a}) < 0$. In the proof of proposition 4 we saw that $(R : \mathfrak{q}^{-1}) = \mathfrak{q}$. Since R has dimension at most one, we deduce that $\mathfrak{a}$ can not be contained in R.

Let $\mathfrak{b}$ be another fractional ideal. The relation *i.)* is clear. Further, $\mathfrak{a}$ is contained in $\mathfrak{b}$ if and only if $\mathfrak{ab}^{-1}$ is contained in R. Thus *i.)* implies that for $\mathfrak{a} \subseteq \mathfrak{b}$, it is necessary and sufficient that $\nu_\mathfrak{p}(\mathfrak{a}) \geqslant \nu_\mathfrak{p}(\mathfrak{b})$ for all prime ideals $\mathfrak{p}$. We conclude that $\prod \mathfrak{p}^{\min(\nu_\mathfrak{p}(\mathfrak{a}),\nu_\mathfrak{p}(\mathfrak{b}))}$ is the smallest fractional ideal which contains $\mathfrak{a}$ and $\mathfrak{b}$ and $\prod \mathfrak{p}^{\max(\nu_\mathfrak{p}(\mathfrak{a}),\nu_\mathfrak{p}(\mathfrak{b}))}$ is the largest fractional ideal, which is contained in $\mathfrak{a}$ and $\mathfrak{b}$, so the relation *ii.)* and *iii.)* hold true. ■

Lemma 7. *Let R be a Dedekind domain and let $\{\mathfrak{p}_i\}$ $(i \in I)$ be a finite family of prime ideals. Then for given integers e_i we find an element a in the quotient field K of R such that $\nu_{\mathfrak{p}_i}(a) = e_i$ for all $i \in I$.*

Proof. We can assume with out loss of generality that the e_i are non-negative. We have $\mathfrak{p}_i \nsubseteq \mathfrak{p}_i^2$ and $\mathfrak{p}_i \nsubseteq \mathfrak{p}_j$ if $j \neq i$. By the Prime Avoidance Lemma ([4, Lem. 7.7]) we find an element $a_i \in \mathfrak{p}_i$ wich is neither contained in $\mathfrak{p}_i^2$ nor in $\mathfrak{p}_j$ if $j \neq i$. Then $\nu_{\mathfrak{p}_j}(a_i)$ vanishes if $i \neq j$ and $\nu_{\mathfrak{p}_i}(a_i)$ equals one. Hence, $\prod a_i^{e_i}$ has the desired property. ∎

Proposition 8. *Let R be a Dedekind domain. Then every ideal is generated by at most two elements.*

Proof. Let $\mathfrak{a} \subset R$ be an ideal. Let

$$\mathfrak{a} = \prod_{\substack{\mathfrak{p} \\ \text{prime ideal}}} \mathfrak{p}^{\nu_{\mathfrak{p}}(\mathfrak{a})}$$

be the factorization into prime ideals. Let $x \in \mathfrak{a}$ be non-zero. Then $\nu_{\mathfrak{p}}(\mathfrak{a}) \leqslant \nu_{\mathfrak{p}}(x)$ for all prime ideals $\mathfrak{p}$. By Lemma 7 we find an element $y \in R$ such that for all prime ideals $\mathfrak{p}$ we have

i.) $\nu_{\mathfrak{p}}(y) = \nu_{\mathfrak{p}}(\mathfrak{a})$ if $\nu_{\mathfrak{p}}(\mathfrak{a})$ is non-zero,

ii.) $\nu_{\mathfrak{p}}(y) = 0$ if $\nu_{\mathfrak{p}}(x)$ is non-zero and $\nu_{\mathfrak{p}}(\mathfrak{a})$ vanishes.

Proposition 6 implies that $(x, y) = \mathfrak{a}$. ∎

Let us now revisit the ring $\mathbb{Z}[\sqrt{-5}]$ of algebraic integers of the number field $\mathbb{Q}(\sqrt{-5})$. We gave an example of a non-unique factorization:

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

We know that (6) uniquely factorizes into prime ideals. But how do the associated prime ideals look like? If $\mathfrak{p}$ is a prime ideal that belongs to (6), then $\mathfrak{p}$ nececarly contains two of the factors $2, 3$ and $1 \pm \sqrt{-5}$. Having in mind that every ideal in a Dedekind domain ist generated by at most two elements it is easy to find the following factorizations

$$\begin{aligned}
(2) &= (2, 1 + \sqrt{-5})^2, \\
(3) &= (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}), \\
(1 + \sqrt{-5}) &= (2, 1 + \sqrt{-5})(3, 1 + \sqrt{-5}), \\
(1 - \sqrt{-5}) &= (2, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}).
\end{aligned}$$

To see that $(2, 1 + \sqrt{-5})$ and $(3, 1 \pm \sqrt{-5})$ are prime ideals, we observe that they are the kernels of the ring homomorphisms

$$\begin{aligned}
\mathbb{Z}[\sqrt{-5}] &\longrightarrow \mathbb{F}_2 \\
a + b\sqrt{-5} &\longmapsto a + b \bmod 2
\end{aligned}$$

and

$$\begin{aligned}\mathbb{Z}[\sqrt{-5}] &\longrightarrow \mathbb{F}_3\\ a + b\sqrt{-5} &\longmapsto a \mp b \bmod 3,\end{aligned}$$

respectively. Therefore we obtain the unique factorization

$$(6) = (2, 1 + \sqrt{-5})^2(3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}).$$

Proposition 9. *Let R be a Dedekind domain. Then R is factorial, if and only if R is a principal ideal domain.*

Proof. If R is a principal ideal domain, then it is clear that R is factorial.

Vice versa let R be factorial. Let $\mathfrak{p} \subset R$ be an arbitrary non-zero prime ideal and let $x \in \mathfrak{p}$ be non-zero. Let p be a prime factor of x. Since R has dimension at most 1, we find $(p) = \mathfrak{p}$. Consequently, R is a principal ideal domain. ■

Let R be a Dedekind domain with quotient field K. Then the non-zero fractional ideals of R form an abelian group with respect to multiplication. This group is called the *group of ideals*; we deonte it by I_K. Since every ideal in R has an unique factorization into prime ideals, we find that I_K is the free group generated by the non-zero prime ideals of R. We have a group homomorphism

$$\begin{aligned}\phi : K^\times &\longrightarrow I_K\\ u &\longmapsto (u).\end{aligned}$$

The image P_K of ϕ is the group of *principal fractional ideals*. The quotient

$$Cl_K := I_K/P_K$$

is called *ideal class group*. The kernel of ϕ is the group of units $R^\times$, thus we haven an exact sequence,

$$1 \longrightarrow R^\times \longrightarrow K^\times \longrightarrow I_K \longrightarrow Cl_K \longrightarrow 1.$$

One of the most central results in algebraic number theory says that the ideal class group of an algebraic number field is always finite. For a proof see Neukirch [3, Ch. I, Thm. 6.3] Its order is called the *class number*. We can re-write proposition 9 and derive that $\mathcal{O}_K$ is factorial if and only if the class number equals one. So the Cl_K can be viewed as quantifying the extent to which a Dedekind domain fails to be factorial Another, classical result from algebraic number theory relates to the group of units of $\mathcal{O}_K$. *Dirichlet's unit theorem* predicts that $\mathcal{O}_K^\times$ is the direct product of a finite cyclic group and a free

abelian group of finite rank. Compare with Neukirch [3, Ch. I, Thm. 7.4].

Another important class of Dedekind domains comes from algebraic geometry. Let (E, O) be an elliptic curve over an algebraically closed field K. The coordinate ring $k[E]$ of E is a Dedekind domain. Recall that we can associate to every point $P \in E$ a maximal ideal

$$\mathfrak{m}_P := \{f \in K[E] \mid f(P) = 0\}$$

of $K[E]$. We have a natural map

$$\begin{aligned} \phi : E &\longrightarrow Cl \\ P &\longmapsto [\mathfrak{m}_P], \end{aligned}$$

from the elliptic curve to the ideal class group of the coordinate ring, that is an isomorphism of groups. For a proof see [4, Ch. 14.3].

References

[1] H. M. Edwards, *Fermat's Last Theorem. A Genetic Introduction to Algebraic Number Theory*. Graduate Texts in Mathematics, Springer, 1977.

[2] Robert Fricke, Emmy Noether, Öystein Ore, *Richard Dedekind. Gesammelte mathematische Werke*, vol. 3. Friedr. Vieweg & Sohn Akt.-Ges., 1932.

[3] J. Neukirch, *Algebraische Zahlentheorie*. Springer, 2007.

[4] G. Kemper, *A Course in Commutative Algebra*. Springer, 2009.

[5] M. F. Atiyah, Frs, I. G. MacDonald, *Introduction to Commutative Algebra*. Addison-Wesley Series in Mathematics, Addision-Wesley Publishing Company, Inc., 1969.

[6] Oscar Zariski, Pierre Samuel, *Commutative Algebra Volume I*. D. Van Nostrand Company, Inc., 1965.