ALGEBRAIC NUMBER THEORY

FRANZ LEMMERMEYER

1. Algebraic Integers

Let A be a subring of a commutative ring R. An element $x \in R$ is integral over A if there exist $a_0, \ldots, a_{n-1} \in A$ such that $x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$.

Example. Take $A = \mathbb{Z}$ and $R = \mathbb{A}$, the field of algebraic numbers. Then $x \in \mathbb{A}$ is integral over $\mathbb{Z}$ if there exist integers $a_0, \ldots, a_{n-1}$ such that $x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$. These elements are called algebraic integers.

Theorem 1.1. *With the notation as above, the following are equivalent:*

(1) *x is integral over A;*
(2) *the ring $A[x]$ is a finitely generated A-module;*
(3) *there exists a subring B of R, finitely generated as an A-module, such that $A[x] \subseteq B$.*

Let A be a subring of R; we say that R is integral over A if every $x \in R$ is integral over A.

Lemma 1.2. *Let R be integral over A, and let $\theta : R \longrightarrow S$ be a ring epimorphism. Then S is integral over $\theta(A)$.*

Theorem 1.3. *Let R be a domain, integral over some subring A. If $\mathfrak{a}$ is an ideal in R, then $\mathfrak{a} \cap A \neq \varnothing$.*

If every element of R which is integral over A belongs to A, then A is said to be integrally closed in R.

If A is an integral domain with quotient field K, and if A is integrally closed in K, then we say that A is integrally closed.

Proposition 1.4. *Let A be a subring of R and let $x_1, \ldots, x_n \in R$. If x_1 is integral over A, x_2 integral over $A[x_1]$, etc. then $A[x_1, \ldots, x_n]$ is a finitely generated A-module.*

Integrality is transitive:

Proposition 1.5. *Let $A \subseteq B \subseteq C$ be rings. If C is integral over B and B is integral over A, then C is integral over A.*

Proposition 1.6. *Let A be subring of R, and let B be the set of all elements $x \in R$ that are integral over A. Then B is a subring of R, integrally closed in R, and integral over A.*

This ring B is called the integral closure of A in R.

Proposition 1.7. *Let R be a domain integrally closed over A. Then R is a field if and only if A is a field.*

Corollary 1.8. *Let R be integral over A and let $\mathfrak p$ be a prime ideal in R. Then $\mathfrak p$ is a maximal ideal of R if and only if $\mathfrak p \cap A$ is a maximal ideal of A.*

Theorem 1.9. *Let A be an integrally closed domain with quotient field K. Let L be an algebraic extension of K. If $x \in L$ is integral over A, then its minimal polynomial over K is an element of $A[T]$. All conjugates of x over K are also integral over A. If B is the integral closure of A in L, then $B \cap K = A$.*

Proposition 1.10. *Let A be an integrally closed domain with quotient field K, and let L/K be an algebraic extension. Let B denote the integral closure of A in L. Then every element of L has the form b/a, where $b \in B$ and $a \in A \setminus \{0\}$.*

Proposition 1.11. *Every UFD is integrally closed.*

In particular, PIDs are integrally closed.

For a number field K, let $\mathbb{Z}_K$ denote the ring of algebraic integers in K. We know that $\mathbb{Z}_K$ is integrally closed, and that $\mathbb{Z}_K \cap \mathbb{Q} = \mathbb{Z}$. We also know that if $\alpha \in \mathbb{Z}_K$, then $\operatorname{Tr} \alpha$ and $N\alpha$ are integers.

Proposition 1.12. *Let A be a domain satisfying the ascending chain condition for principal ideals: any increasing chain $Aa_1 \subseteq Aa_2 \subseteq \ldots \subseteq Aa_n \subseteq \ldots$ of principal ideals of A becomes stationary, i.e. there is an $n \in \mathbb{N}$ such that $Aa_n = Aa_{n+1} = \ldots$. Then every nonunit $a \in A$ can be written as a product of irreducible elements.*

Proposition 1.13. *Let A be a domain in which every element is a product of irreducible elements. Then the following statements are equivalent:*

1. *if $p_1 \cdots p_r = q_1 \cdots q_s$ are factorizations into irreducible elements, then $s = r$ and the q_i can be reindexed in such a way that $p_i = u_i q_i$ for suitable units $u_i \in R$.*
2. *if p is irreducible and $p \mid ab$ for $a, b \in A$, then $p \mid a$ or $p \mid b$*

The second condition can be expressed by saying that irreducibles are prime. Note that, in my book, an irreducible element $a \in R$ is an element with the property that if $a = rs$ for $r, s \in R$, then r or s is a unit (i.e. there are only trivial factorizations of a); an element $p \in R$ is called prime if $p \mid ab$ for any $a, b \in R$ always implies that $p \mid a$ or $p \mid b$.

Proposition 1.14. *An algebraic integer is a unit if and only if it has norm ± 1.*

2. Algebraic Preliminaries

In the following, all rings are commutative and have a unit. For a squarefree integer $m \in \mathbb{Z}\backslash\{0,1\}$ the set $k = \mathbb{Q}(\sqrt{m}\,) = \{a+b\sqrt{m} : a, b \in \mathbb{Q}\}$ forms a field called a *quadratic number field.* We say that k is real or complex quadratic according as $m > 0$ or $m < 0$.

The element $\alpha = a + b\sqrt{m} \in k$ is a root of the quadratic polynomial $P_\alpha(x) = x^2 - 2ax + a^2 - mb^2 \in \mathbb{Q}[x]$; its second root $\alpha' = a - b\sqrt{m}$ is called the *conjugate* of α. We also define

$$\begin{array}{lclll} \mathrm{N}\,\alpha & = & \alpha\alpha' & = a^2 - mb^2 & \text{the } \textit{norm} \text{ of } \alpha, \\ \mathrm{Tr}\,\alpha & = & \alpha + \alpha' & = 2a & \text{the } \textit{trace} \text{ of } \alpha, \text{ and} \\ \mathrm{disc}(\alpha) & = & (\alpha - \alpha')^2 & = 4mb^2 & \text{the } \textit{discriminant} \text{ of } \alpha. \end{array}$$

The basic properties of norm and trace are

Proposition 2.1. *For all $\alpha, \beta \in k$ we have $N(\alpha\beta) = N\alpha\, N\beta$ and $\mathrm{Tr}(\alpha+\beta) = \mathrm{Tr}\,\alpha + \mathrm{Tr}\,\beta$. Moreover $N\alpha = 0$ if and only if $\alpha = 0$, $\mathrm{Tr}\,\alpha = 0$ if and only if $\alpha \in \mathbb{Q}\sqrt{m}$, and $\mathrm{disc}(\alpha) = 0$ if and only if $\alpha \in \mathbb{Q}$.*

Proof. Left as an exercise. □

The map $\sigma : k \longrightarrow k : \alpha \longmapsto \sigma(\alpha) := \alpha'$ is called the *nontrivial automorphism* of $k/\mathbb{Q}$.

Exercise. The map $\sigma : k \longrightarrow k$ is a ring homomorphism, i.e., we have $\sigma(\alpha+\beta) = \sigma(\alpha) + \sigma(\beta)$ and $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$ for all $\alpha, \beta \in k$. Show that $\alpha \in k$ is rational if and only if $\alpha = \sigma(\alpha)$.

Since $\sigma \circ \sigma = \mathrm{id}$ (the identity map), $\{\mathrm{id}, \sigma\}$ is a group of order 2 called the *Galois group*[1] of $k/\mathbb{Q}$ and denoted by $\mathrm{Gal}(k/\mathbb{Q})$.

Let $k \subseteq K$ be fields; then K may be viewed as a k-vector space: the vectors are the elements from K (they form an additive group), the scalars are the elements of k, and the scalar multiplication is the restriction of the usual multiplication in K. The dimension $\dim_k K$ of K as a k-vector space is called the *degree* of K/k and is denoted by $(K : k)$.

Clearly $\mathbb{Q}(\sqrt{m}\,)$ has degree 2 over $\mathbb{Q}$: a basis is given by$\{1, \sqrt{m}\}$ since every element of K can be written uniquely as a $\mathbb{Q}$-linear combination of 1 and $\sqrt{m}$.

[1] Évariste Galois (1811–1832), a French mathematician killed in a duel at the age of 20.

3. Integers of Quadratic Fields

Let $K = \mathbb{Q}(\sqrt{m}\,)$ be a quadratic extension with m squarefree. Elements of K have the form $a + b\sqrt{m}$ with $a, b \in \mathbb{Q}$. The conjugate of $a + b\sqrt{m}$ is $a - b\sqrt{m}$.

Lemma 3.1. *We have $a+b\sqrt{m} \in \mathbb{Z}_K$ if and only if $u = 2a$ and $v = 2b$ are integers with $u^2 - mv^2 \equiv 0 \bmod 4$.*

Proposition 3.2. *We have*

$$\mathbb{Z}_K = \begin{cases} \{a + b\sqrt{m} : a, b \in \mathbb{Z}\} & \text{if } m \equiv 2, 3 \bmod 4, \\ \{\frac{a+b\sqrt{m}}{2} : a \equiv b \bmod 2\} & \text{if } m \equiv 1 \bmod 4 \end{cases}$$

Corollary 3.3. *The ring $\mathbb{Z}_K$ of integers in a quadratic number field K is a free abelian group. If $m \equiv 2, 3 \bmod 4$, then $\{1, \sqrt{m}\}$ is a basis of $\mathbb{Z}_K$; if $m \equiv 1 \bmod 4$, then $\{1, \frac{1+\sqrt{m}}{2}\}$ is a basis of $\mathbb{Z}_K$.*

Exercise. Consider the rings

$$\mathbb{Z}[\sqrt{5}\,] \subset \mathbb{Z}[\tfrac{1+\sqrt{5}}{2}] \subset \mathbb{Z}[\tfrac{1}{2}, \sqrt{5}\,] \subset \mathbb{Q}(\sqrt{5}\,).$$

Show that

- $\mathbb{Z}[\sqrt{5}\,]$ and $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ are integral over $\mathbb{Z}$.
- $\mathbb{Z}[\frac{1}{2}, \sqrt{5}\,]$ is not integral over $\mathbb{Z}$, but is integral over $\mathbb{Z}[\frac{1}{2}]$.
- $\mathbb{Z}[\sqrt{5}\,]$ is not integrally closed.
- $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ and $\mathbb{Z}[\frac{1}{2}, \sqrt{5}\,]$ are integrally closed.

Actually, more is true. Call a subring of $K = \mathbb{Q}(\sqrt{5}\,)$ an order if it contains $\mathbb{Z}$ and has K as its quotient field. Then $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ is the maximal order that is integral over $\mathbb{Z}$, and the minimal order that is integrally closed.

4. Some History

Number Theory has a long history: already the Pythagoreans studied prime numbers and perfect numbers, and Pythagorean triples like $(3, 4, 5)$ are even older. The most outstanding number theorists in ancient times was Diophantus of Alexandria, who probably lived in the third century AD. His methods were closely studied by Fermat and led to his conjecture that the diophantine equation $x^n + y^n = z^n$ does not have a solution in natural numbers if $n > 2$. Fermat also came up with results and conjectures that were explained much later by algebraic number theory. His claim that primes $p \equiv 1, 9 \bmod 20$ can be written in the form $p = x^2 + 5y^2$ was studied and eventually proved by mathematicians such as Euler and Lagrange, and it is connected with the fact that the field $\mathbb{Q}(\sqrt{-5}\,)$ has class number 2 (in the language of binary quadratic forms: there are two nonequivalent quadratic forms of discriminant -20, namely $x^2 + 5y^2$ and $2x^2 + 2xy + 3y^2$).

Euler also introduced algebraic numbers in his proof that the diophantine equation $y^2 = x^3 - 2$ has $(x, y) = (3, 5)$ as its only solution in natural numbers by factoring the equation as $x^3 = (y + \sqrt{-2}\,)(y - \sqrt{-2}\,)$.

The work of Euler, Lagrange and Legendre on quadratic forms were formed into a beautiful (and, at the time, difficult and abstract) theory by Gauss in his Disquisitiones Arithmeticae published in 1801. One of the main results of Gauss was the first complete proof of the quadratic reciprocity law

$$\Big(\frac{p}{q}\Big)\Big(\frac{q}{p}\Big) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Gauss was working on a generalization of quadratic reciprocity to fourth powers for years until he realized that in order to formulate a proper reciprocity law for fourth powers, one had to work in the ring $\mathbb{Z}[\sqrt{-1}\,]$. There, the reciprocity law can be stated in the form

$$\Big[\frac{\pi}{\rho}\Big]\Big[\frac{\rho}{\pi}\Big] = (-1)^{\frac{N\pi-1}{4}\cdot\frac{N\rho-1}{4}}.$$

Here π and ρ are primes $\equiv 1 \bmod (2 + 2i)$ in $\mathbb{Z}[i]$, and N denotes the norm. Gauss published (parts of) these results only in 1828; ten years later Jacobi worked out simple proofs of the cubic and quartic reciprocity laws, but Eisenstein published them first in 1844. In an unpublished paper, Gauss also proved Fermat's Last Theorem for the exponent 3 using the fact that the ring $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}\,]$ is a UFD.

Dirichlet invented analytic number theory, and among other results proved a class number formula for the class number of binary quadratic forms, which we interpret nowadays as a class number formula for quadratic number fields. He also determined the rank of the unit group in rings of integers of algebraic number fields, widely generalizing the result that the Pell equation $X^2 - dY^2 = 1$ is solvable for nonsquare integers $d > 0$.

Eisenstein and Kummer then started working on a reciprocity law for p-th power residues, which lives in the ring $\mathbb{Z}[\zeta_p]$ of the field $\mathbb{Q}(\zeta_p)$ of p-th roots of unity. In order to cope with nonunique factorization, Kummer introduced ideal numbers. He succeded proving the reciprocity law for all regular primes, that is, primes with the property that p does not divide the order of the class group of $\mathbb{Q}(\zeta_p)$; Kummer showed that this can be checked by computing the first $p - 3$ Bernoulli numbers. He also saw that his methods could be applied to Fermat's Last Theorem, and with a lot of work he finally obtained proofs for all prime exponents below 100.

Algebraic number theory in the modern sense starts with Dedekind: he replaced Kummer's ideal numbers by ideals, realized the importance of integral closure, and proved that we have unique factorization into prime ideals in rings of integers in algebraic number fields. Together with Weber he developed the theory of function fields; the rational function field $\mathbb{F}_q(X)$ over finite fields had already been investigated by Gauss (unpublished), Serret and Dedekind, and its subring $\mathbb{F}_q[X]$ was known to have many properties analogous to the ring of integers. The analogy between function fields and number fields keeps inspiring number theorists to this day.

Hilbert finally translated all the results obtained so far by Gauss, Dirichlet, and Kummer into Dedekind's language; in some sense, his report from 1896 completed the classical era of algebraic number theory. About the same time, the axiomatization of mathematics began with the emergence of the concept of abstract groups and vector spaces. It took another 25 years until Emmy Noether finally came up with the axioms that guarantee that a ring admits unique factorization into prime ideals; such rings were called 'Dedekind rings' starting around 1950.

Hilbert also outlined a program for studying abelian extensions of number fields. His program was worked out by his student Furtwängler between 1900 and 1910 and generalized considerably by Takagi in 1920: class field theory was born. Takagi's results were streamlined by Hasse, and finally Artin completed class field theory by finding a simple formulation of the general reciprocity law in abelian extensions of number fields. Artin's reciprocity law is an isomorphism between a class group and a Galois group and, at first sight, seems to have nothing to do with the explicit reciprocity laws derived by Gauss, Jacobi, Eisenstein, and Kummer.

The generalization of reciprocity laws to nonabelian extensions is the content of Langlands' program; there has been some progress in recent years: the Langlands correspondence for GL_n over the field of p-adic numbers was proved in 1998 by Michael Harris and Richard Taylor, and Guy Henniart gave a second proof shortly afterwards. Laurent Lafforgue proved the Langlands correspondence for function fields and was awarded the Fields medal in 2002 for this result. The results of Wiles may be seen as a small step in the proof of the Langlands correspondence for number fields.

5. Ideals

What is an ideal? Recall that a subset I of a ring R is called a subring if I it is closed under the ring operations, that is, adding and multiplying elements of I again produces elements of I. This is similar to the concepts of subgroups or subspaces of vector spaces; what is different in the category of rings is that the quotient $R/I = \{r + I : r \in R\}$ in general is not a ring with respect to addition $(r + I) + (s + I) = r + s + I$ and multiplication $(r + I) \cdot (s + I) = rs + I$. In fact, this multiplication is in general not defined: if $r + I = r' + I$ and $s + I = s' + I$, i.e., if $a = r - r' \in I$ and $b = s - s' \in I$, then $r's' + I = (r - a)(s - b) + I = rs + (ab - rb - sa) + I$, and this is equal to the coset $rs + I$ only if $ab - rb - sa \in I$; since $a, b \in I$ implies that $ab \in I$, this is equivalent to $rb + sa \in I$. But for general subrings I of R this is not necessarily the case:

Exercise. Show that the set of upper triangular 2×2-matrices with coefficients in some ring R is a subring, but not an ideal of the ring of all 2×2-matrices.

In order to guarantee that $rb + sa \in I$ for $a, b \in I$ and $r, s \in R$ we have to demand that I be an ideal: this is a subring of R with the additional property that $ri \in I$ whenever $i \in I$ and $r \in R$ (we abbreviate this by writing $RI \subseteq I$).

Note that if I and J are ideals in R, then so are

$$\begin{aligned} I + J &= \{i + j : i \in I, j \in J\}, \\ IJ &= \{i_1 j_1 + \ldots + i_n j_n : i_1, \ldots, i_n \in I, j_1, \ldots, j_n \in J\}, \end{aligned}$$

as well as $I \cap J$. The index n in the product IJ is meant to indicate that we only form finite sums. If A and B are ideals in some ring R, we say that $B \mid A$ if $A = BC$ for some ideal C.

Exercise. Consider the space S of all sequences of rational numbers. This is a ring with respect to pointwise addition and multiplication: $(a_1, a_2, a_3, \ldots) + (b_1, b_2, b_3, \ldots) = (a_1 + b_1, a_2 + b_2, a_3 + b_3, \ldots)$ and $(a_1, a_2, a_3, \ldots) \cdot (b_1, b_2, b_3, \ldots) = (a_1 b_1, a_2 b_2, a_3 b_3, \ldots)$.

Show that the the following subsets of S actually are subrings:

(1) the set N of sequences converging to 0;
(2) the set D of sequences converging in $\mathbb{Q}$;
(3) the set C of Cauchy sequences;
(4) the set B of bounded sequences.

Observe that $N \subset D \subset C \subset B \subset S$. Determine which of these subrings are ideals in B (resp. C, D).

The difference between additive subgroups, subrings, and ideals is not visible in the ring $R = \mathbb{Z}$ of integers:

Exercise. Show that every subgroup A of $\mathbb{Z}$ is automatically a subring and even an ideal in $\mathbb{Z}$, and that there is an $a \in \mathbb{Z}$ such that $A = a\mathbb{Z}$.

We say that an nonzero ideal $I \neq R$ is

- irreducible if $I = AB$ for ideals A, B implies $A = R$ or $B = R$;
- a prime ideal if $AB \subseteq I$ for ideals A, B always implies $A \subseteq I$ or $B \subseteq I$;
- a maximal ideal if $I \subseteq J \subseteq R$ for an ideal J implies $J = I$ or $J = R$.

For principal ideals, this coincides with the usual usage of prime and irreducible elements: an ideal (a) is irreducible (prime) if and only if a is irreducible (prime). In fact, $(r) \mid (s)$ is equivalent to $r \mid s$.

Prime ideals and maximal ideals can be characterized as follows:

Proposition 5.1. *An ideal I is*

- *prime in R if and only if R/I is an integral domain;*
- *maximal in R if and only if R/I is a field.*

Proof. □

Note that an integral domain is a ring with 1 in which $0 \neq 1$; thus (1) is not prime since the null ring R/R only has one element.

It follows from this proposition that every maximal ideal is prime; the converse is not true in general. In fact, consider the ring $\mathbb{Z}[X]$ of polynomials with integral coefficients. Then $I = (X)$ is an ideal, and $R/I \simeq \mathbb{Z}$ is an integral domain but not a field, hence I is prime but not maximal.

An important result is

Theorem 5.2 (Chinese Remainder Theorem)**.** *If A and B are ideals in R with $A + B = R$, then $R/AB \simeq R/A \oplus R/B$.*

Proof. □

6. Ideal Arithmetic in Quadratic Number Fields

Let us first look at the ring $R = \mathbb{Z}[\sqrt{-2}\,]$. We have

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

Does this mean that R is not a UFD? It would if the elements in the factorizations (1) were irreducible, but, as a matter of fact, they are not: we have

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

It is now easy to see that the two seemingly different factorizations come from pairing up the factors in the prime factorization

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

Now consider the ring of integers $R = \mathbb{Z}[\sqrt{-5}\,]$ in the quadratic number field $\mathbb{Q}(\sqrt{-5}\,)$. Then

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

Can we decompose these factors further? No we cannot: they are irreducible. In fact, applying the norm to $1 + \sqrt{-5} = \alpha\beta$ for $\alpha, \beta \in R$ yields $6 = N\alpha N\beta$. Since norms from complex quadratic fields are nonnegative, the only possibilities for $N\alpha$ are

- $N\alpha = 1$: writing $\alpha = x + y\sqrt{-5}$, this means $x^2 + 5y^2 = 1$, hence $x = \pm 1$, $y = 0$ and $\alpha = \pm 1$.

- $N\alpha = 2$: this is impossible, since $x^2 + 5y^2 = 2$ does not have a solution in integers.
- $N\alpha = 3$: but then $N\beta = 2$, which is impossible.
- $N\alpha = 6$: this implies $N\beta = 1$, hence $\beta = \pm 1$.

Thus all factorizations of $1+\sqrt{-5}$ are trivial, that is, $1+\sqrt{-5}$ is irreducible. The same can be shown for the other elements in the factorization of 6 above.

Moreover, the elements are not associated: if $1+\sqrt{-5}$ and e.g. 2 would differ by a unit, then their quotient $\frac{1}{2}(1+\sqrt{-5}\,)$ would have to be an algebraic integer, which it is not.

Thus $\mathbb{Z}[\sqrt{-5}\,]$ is not a UFD, and the factorizations of 6 in (2) are genuinely different.

Kummer's great idea was to introduce "ideal numbers" (turned into ideals by Dedekind) which explain the different factorizations (2) in very much the same way as the prime factors of 2 and 3 explain (1).

Where do these ideals that save unique factorizations come from? In order to motivate their introduction, consider the following example of Dirichlet. The set of integers $S = \{1, 5, 9, 13, \ldots\}$ form a multiplicatively closed set. But they do not have unique factorization, as $9 \cdot 49 = 21 \cdot 21$ shows. What is "missing" is a common factor of 9 and 21 in S. Since it is not there, we introduce it as an 'ideal factor' $\gcd(9, 21)$. Then $9 = (9, 21)^2$, $49 = (49, 21)^2$, and $21 = (9, 21)(49, 21)$, and the nonunique factorization $9 \cdot 49 = 21 \cdot 21$ is explained by the ideal factorization $441 = (9, 21)^2(49, 21)^2$.

Now let us do the same in $\mathbb{Z}[\sqrt{-5}\,]$ by introducing the ideals $\mathfrak{p} = (2, 1+\sqrt{-5}\,)$, $\mathfrak{q} = (3, 1+\sqrt{-5}\,)$, and $\mathfrak{q}' = (3, 1+\sqrt{-5}\,)$ (note that $(2, 1-\sqrt{-5}\,) = \mathfrak{p}$). We find

$$\begin{aligned}\mathfrak{p}^2 &= (2\cdot 2, 2(1+\sqrt{-5}\,), 2(1+\sqrt{-5}\,), -4+2\sqrt{-5}\,)\\ &= (4, 2(1+\sqrt{-5}\,), -4+2\sqrt{-5}\,)\\ &= (2)(2, 1+\sqrt{-5}, -2+\sqrt{-5}\,);\end{aligned}$$

since the last ideal contains $\sqrt{-5} = 2 + (-2+\sqrt{-5}\,)$ and $1 = (1+\sqrt{-5}\,) - \sqrt{5}$, we conclude that $\mathfrak{p}^2 = (2)(1) = (2)$. Similarly, we get

$$\begin{aligned}\mathfrak{q}\mathfrak{q}' &= (9, 3(1+\sqrt{-5}\,), 3(1-\sqrt{-5}\,), 6)\\ &= (3)(3, 1+\sqrt{-5}, 1-\sqrt{-5}, 2)\\ &= (3)(1) = (3).\end{aligned}$$

and

$$\begin{aligned}\mathfrak{q}^2 &= (9, 3(1+\sqrt{-5}\,), (1+\sqrt{-5}\,)^2)\\ &= (2+\sqrt{-5}\,)(2-\sqrt{-5}, 1-\sqrt{-5}, -2)\\ &= (2+\sqrt{-5}\,).\end{aligned}$$

Thus the nonunique factorization (2) turns into the ideal equality

$$(6) = \mathfrak{p}^2\mathfrak{q}\mathfrak{q}',$$

from which the factorizations of principal ideals

$$(6) = (2)(3) \quad \text{and} \quad (6) = (1+\sqrt{-5}\,)(1-\sqrt{-5}\,)$$

follows by pairing the ideals $\mathfrak{p}$, $\mathfrak{q}$ and $\mathfrak{q}'$ in two different ways.

The first goal now is to prove that this is not accidental, and that factorization into prime ideals holds in any ring of integers of an algebraic number field. This can be shown in various degrees of abstraction. In the next section, we give a down and dirty way of doing this in quadratic number fields, and then give the general proof that the rings of integers in algebraic number fields are Dedekind rings.

As an exercise, study the factorization $6 = 2 \cdot 3 = -\sqrt{-6}^2$ in $\mathbb{Z}[\sqrt{-6}\,]$. A more difficult example is the factorization $6 = 2 \cdot 3 = (2+\sqrt{10}\,)(-2+\sqrt{10}\,)$. The reason why 6 occurs so often here is that it is the product of the two smallest primes; there are similar examples involving factorizations of 10 or 15 . . . .

Remark. The condition that we work in the ring of integers is important: the ring $R = \mathbb{Z}[\sqrt{-3}\,]$, which is not integrally closed, does not have unique factorizations into prime ideals, as we can see from the factorization $(2)(2) = (1+\sqrt{-3}\,)(1-\sqrt{-3}\,)$. The ideal (2) is irreducible. Moreover, we do not have $(2) = (1+\sqrt{-3}\,)$, since this would imply $\frac{1+\sqrt{-3}}{2} \in R$. In particular, this problem disappears over the integral closure $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ of R, since we clearly have $(2) = (1+\sqrt{-3}\,)$.

7. Unique Factorization into Prime Ideals

We want to show that every ideal in the ring $\mathbb{Z}_K$ of integers in a quadratic number field $K = \mathbb{Q}(\sqrt{d}\,)$ can be factored uniquely into prime ideals.

Norms of Ideals. Ideals in rings of integers may not always be principal (generated by one element), but they always can be generated by two elements. This is not true in general rings: the ideal (X_1, X_2, X_3) in the polynomial ring $\mathbb{Z}[X_1, X_2, X_3, X_4]$ cannot be generated by two elements.

In the following, $K = \mathbb{Q}(\sqrt{d}\,)$ is a quadratic number field, and $\{1, \omega\}$ is a basis of its ring of integers $\mathbb{Z}_K$.

Proposition 7.1. *Let $\mathfrak{a} \subset \mathbb{Z}_K$ be a $\mathbb{Z}$-module in $\mathbb{Z}_K$, that is an additive subgroup of $\mathbb{Z}_K$. Then there exist $m, n \in \mathbb{N}_0$ and $a \in \mathbb{Z}$ such that $\mathfrak{a} = n\mathbb{Z} \oplus (a + m\omega)\mathbb{Z}$.*

If $\mathfrak{a} \neq (0)$ is an ideal, then $m \mid n$, $m \mid a$ (hence $a = mb$ for some $b \in \mathbb{Z}$) and $n \mid m \cdot N(b + \omega)$. In particular, every ideal in $\mathbb{Z}_K$ is generated by at most two elements.

Proof. Consider the subgroup $H = \{s : r + s\omega \in \mathfrak{a}\}$ of $\mathbb{Z}$. Every subgroup of $\mathbb{Z}$ is automatically an ideal, hence H has the form $H = m\mathbb{Z}$ for some $m \geq 0$. By construction, there is an $a \in \mathbb{Z}$ such that $a + m\omega \in \mathfrak{a}$. Finally, $\mathfrak{a} \cap \mathbb{Z}$ is a subgroup of $\mathbb{Z}$, hence $\mathfrak{a} \cap \mathbb{Z} = n\mathbb{Z}$ for some $n \geq 0$.

We now claim that $\mathfrak{a} = n\mathbb{Z} \oplus (a + m\omega)\mathbb{Z}$. The inclusion $\supseteq$ is clear; assume therefore that $r + s\omega \in \mathfrak{a}$. Since $s \in H$ we have $s = um$ for some $u \in \mathbb{Z}$, and then $r - ua = r + s\omega - u(a + m\omega) \in \mathfrak{a} \cap \mathbb{Z}$, hence $r - ua = vn$. But then $r + s\omega = r - ua + u(a + m\omega) = vn + u(a + m\omega) \in n\mathbb{Z} \oplus (a + m\omega)\mathbb{Z}$.

Now assume in addition that $\mathfrak{a}$ is an ideal. Then $c \in \mathfrak{a} \cap \mathbb{Z}$ implies $c\omega \in \mathfrak{a}$, hence $c \in H$ by definition of H. This shows that $n\mathbb{Z} = \mathfrak{a} \cap \mathbb{Z} \subseteq H = m\mathbb{Z}$, hence $m \mid n$ (if the multiples of n are contained in the multiples of m, then m must divide n; this instance of “to divide means to contain” will reoccur frequently in the following).

In order to show that $m \mid a$ we observe that $\omega^2 = x + y\omega$ for suitable $x, y \in \mathbb{Z}$. Since $\mathfrak{a}$ is an ideal, $a + m\omega \in \mathfrak{a}$ implies $(a + m\omega)\omega = mx + (a + my)\omega \in \mathfrak{a}$, hence $a + my \in H$ by definition of H, and therefore $a + my$ is a multiple of m. This implies immediately that $m \mid a$, hence $a = mb$ for some $b \in \mathbb{Z}$.

In order to prove the last divisibility relation we put $\alpha = a + m\omega = m(b + \omega)$. Then $\alpha \in \mathfrak{a}$ implies $\alpha(b + \omega') \in \mathfrak{a}$. Since $\frac{1}{m}N\alpha = m(b + \omega)(b + \omega') \in \mathfrak{a} \cap \mathbb{Z}$, we conclude that $\frac{1}{m}N(b + \omega)$ is a multiple of n. □

Our next aim is the claim that the “norm” $\mathfrak{a}\mathfrak{a}'$ of an ideal (for an ideal $\mathfrak{a}$, the set $\mathfrak{a}' = \{\alpha' : \alpha \in \mathfrak{a}\}$ is an ideal called the conjugate of $\mathfrak{a}$) is generated by a natural number. For principal ideals $\mathfrak{a} = (\alpha)$ this is obvious in view of $(\alpha)(\alpha)' = (\alpha)(\alpha') = (\alpha\alpha') = (N\alpha) = (-N\alpha)$ klar.

Proposition 7.2. *Let $\mathfrak{a} \neq (0)$ be an ideal in $\mathbb{Z}_K$; then there is an $a \in \mathbb{N}$ such that $\mathfrak{a}\mathfrak{a}' = a\mathbb{Z}_K$.*

For the proof of Proposition 7.2 we use the following lemma due to Hurwitz:

Lemma 7.3. *Let $\alpha, \beta \in \mathbb{Z}_K$ and $m \in \mathbb{N}$. If $N\alpha$, $N\beta$ and $\operatorname{Tr}\alpha\beta'$ are divisible by m, then $m \mid \alpha\beta'$ and $m \mid \alpha'\beta$.*

Proof. Put $\gamma = \alpha\beta'/m$; then $\gamma' = \alpha'\beta/m$, and we know that $\gamma + \gamma' = (\operatorname{Tr}\alpha\beta')/m$ and $\gamma\gamma' = \frac{N\alpha}{m}\frac{N\beta}{m}$ are integers. But if the norm and the trace of some γ in a quadratic number field are integral, then we have $\gamma \in \mathbb{Z}_K$. □

Proof of Proposition 7.2. Using Proposition 7.1 we can write $\mathfrak{a} = (\alpha, \beta)$ for $\alpha, \beta \in \mathbb{Z}_K$. Then $\mathfrak{a}' = (\alpha', \beta')$ and therefore $\mathfrak{a}\mathfrak{a}' = (N\alpha, \alpha\beta', \alpha'\beta, N\beta)$. If we put $a = \gcd(N\alpha, N\beta, \operatorname{Tr}\alpha\beta')$ (in $\mathbb{Z}$), then Hurwitz's Lemma shows that $\frac{\alpha\beta'}{a}$ and $\frac{\alpha'\beta}{a}$ are integral; thus we get $\mathfrak{a}\mathfrak{a}' = (a)(\frac{N\alpha}{a}, \frac{N\beta}{a}, \frac{\alpha\beta'}{a}, \frac{\alpha'\beta}{a})$, where the last ideal lies in $\mathbb{Z}_K$. In order to prove $\mathfrak{a}\mathfrak{a}' = (a)$ it is therefore sufficient to show that $1 \in (\frac{N\alpha}{a}, \frac{N\beta}{a}, \frac{\alpha\beta'}{a}, \frac{\alpha'\beta}{a})$. But 1 is a $\mathbb{Z}$-linear combination of $\frac{N\alpha}{a}$, $\frac{N\beta}{a}$ and $\frac{\operatorname{Tr}\alpha\beta'}{a}$ (by the definition of a), hence in particular a $\mathbb{Z}_K$-linear combination of $\frac{N\alpha}{a}$, $\frac{N\beta}{a}$ and $\frac{\alpha\beta'}{a} + \frac{\alpha'\beta}{a}$. This proves the claim. □

The natural number a in Proposition 7.2 is called the norm of the ideal $\mathfrak{a}$; thus we have $\mathfrak{a}\mathfrak{a}' = (N\mathfrak{a})$. Since $(N\mathfrak{a}\mathfrak{b}) = (\mathfrak{a}\mathfrak{b})(\mathfrak{a}\mathfrak{b})' = (\mathfrak{a}\mathfrak{a}')(\mathfrak{b}\mathfrak{b}') = (N\mathfrak{a})(N\mathfrak{b})$, the ideal norm is multiplicative. Here are a few more useful properties:

- $N\mathfrak{a} = 1 \iff \mathfrak{a} = (1)$: if $N\mathfrak{a} = 1$, then $(1) = \mathfrak{a}\mathfrak{a}' \subseteq \mathfrak{a} \subseteq \mathbb{Z}_K = (1)$, and the converse is clear.
- $N\mathfrak{a} = 0 \iff \mathfrak{a} = (0)$: if $\mathfrak{a}\mathfrak{a}' = (0)$, then $N\alpha = \alpha\alpha' = 0$ for all $\alpha \in \mathfrak{a}$.
- if $\mathfrak{a} = n\mathbb{Z} + m(b + \omega)\mathbb{Z}$ as in Prop. 7.1, then $N\mathfrak{a} = mn$.

  In fact, let $\alpha = m(b + \omega)$; then $\mathfrak{a} = (n, \alpha)$, $\mathfrak{a}' = (n, \alpha')$ and $\mathfrak{a}\mathfrak{a}' = (n^2, mn(b+\omega'), mn(b+\omega), m^2N(b+\omega)) = (mn)(\frac{n}{m}, b+\omega, b+\omega', \frac{1}{n}N(b+\omega))$. By Proposition 7.1, the last ideal lies in Z_K, hence $(N\mathfrak{a}) = \mathfrak{a}\mathfrak{a}' \subseteq (mn)\mathbb{Z}_K = (mn)$ and therefore $mn \mid N\mathfrak{a}$.

  For the converse $N\mathfrak{a} \mid mn$ put $A = N\mathfrak{a}$; then $\mathfrak{a}\mathfrak{a}' = (A)$. Since $\alpha \in \mathfrak{a}$ and $n \in \mathfrak{a}'$, we have $n\alpha \in \mathfrak{a}\mathfrak{a}' = (A)$, hence $A \mid n\alpha = na + nm\omega$; since $\{1, \omega\}$ is an integral basis of $\mathbb{Z}_K$, this implies $A \mid na$ and $A \mid nm$.

Lemma 7.4. *The ideal $\mathfrak{a} = n\mathbb{Z} \oplus m(b + \omega)\mathbb{Z}$ has norm $N\mathfrak{a} = mn$.*

Proof. We have to show that $\mathfrak{a}\mathfrak{a}' = (mn)$. Writing $n = mc$ for some integer c we get

$$\begin{aligned}\mathfrak{a}\mathfrak{a}' &= (n, m(b + \omega))(n, m(b + \omega')) \\ &= (n^2, mn(b + \omega), mn(b + \omega'), m^2N(b + \omega)) \\ &= (mn)(c, b + \omega, b + \omega', \frac{1}{c}N(b + \omega)).\end{aligned}$$

The second ideal is integral because of Propositon 7.1. We want to show that it is the unit ideal. Note that the ideal must be generated by an integer since $\mathfrak{a}\mathfrak{a}' = (a)$. But the only integers dividing $b + \omega$ are ±1 since $\{1, \omega\}$ is an integral basis. □

In arbitrary rings R, the norm of an ideal $\mathfrak{a}$ is defined by $N\mathfrak{a} = \#R/\mathfrak{a}$. This agrees with our definition:

Proposition 7.5. *Let $\mathfrak{a} = n\mathbb{Z} + m(b + \omega)\mathbb{Z}$ be an ideal in $\mathbb{Z}_K$. Then*

$$S = \{r + s\omega : 0 \le r < n,\ 0 \le s < m\}$$

is a complete residue system modulo $\mathbb{Z}_K/\mathfrak{a}$.

Proof. We first show that every $x + y\omega \in \mathbb{Z}_K$ is congruent mod $\mathfrak{a}$ to an element of S. Write $y = mq + s$ for some $q \in \mathbb{Z}$ and $0 \le s < m$; then $x + y\omega - qm(b+\omega) = x' + s\omega$, hence $x + y\omega \equiv x' + s\omega \bmod \mathfrak{a}$. Now write $x' = nq' + r$ for $q' \in \mathbb{Z}$ and $0 \le r < n$; then $x' + s\omega \equiv r + s\omega \bmod \mathfrak{a}$.

Now we claim that the elements of S are pairwise incongruent modulo $\mathfrak{a}$. Assume that $r + s\omega \equiv r' + s'\omega \bmod \mathfrak{a}$ for $0 \le r, r' < n$ and $0 \le s, s' < m$; then $r - r' + (s - s')\omega \in \mathfrak{a}$ implies that $s - s' \in m\mathbb{Z}$ and $r - r' \in n\mathbb{Z}$, hence $r = r'$ and $s = s'$. □

The Cancellation Law. Now we turn to the proof of unique factorization for ideals. The idea behind the proof is the same as in the proof of unique factorization for numbers: from equality of two products, conclude that there must be two equal factors, and then cancel. Now cancelling a factor is the same as multiplying with its inverse; the problem is that we do not have an inverse for ideals.

In the ring $R = \mathbb{Z}/6\mathbb{Z}$ we have $(2)(3) = (2)(0)$, but cancelling (2) yields nonsense. Similar examples exist in all rings with zero divisors. Are there examples in integral domains? Yes, there are. Simple calculations show that $(a, b)^3 = (a^2, b^2)(a, b)$ in arbitrary commutative rings; whenever $(a^2, b^2) \ne (a, b)^2$, we have a counter example to the cancellation law. For an example, take $R = \mathbb{Z}[X, Y]$ and observe that $XY \in (X, Y)^2$, byt $XY \notin (X^2, Y^2)$.

In rings of integers of algebraic numbers, however, the cancellation law holds:

Proposition 7.6. *If $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ are nonzero ideals in $\mathbb{Z}_K$ with $\mathfrak{ab} = \mathfrak{ac}$, then $\mathfrak{b} = \mathfrak{c}$.*

Proof. The idea is to reduce the cancellation law for ideals to the one for numbers, or rather for principal ideals.

Thus assume first that $\mathfrak{a} = (\alpha)$ is principal. Then $\alpha\mathfrak{b} = \mathfrak{ab} = \mathfrak{ac} = \alpha\mathfrak{c}$. For every $\beta \in \mathfrak{b}$ we have $\alpha\beta \in \alpha\mathfrak{c}$, hence there is a $\gamma \in \mathfrak{c}$ such that $\alpha\beta = \alpha\gamma$. This shows $\beta = \gamma \in \mathfrak{c}$, hence $\mathfrak{b} \subseteq \mathfrak{c}$. By symmetry we conclude that $\mathfrak{b} = \mathfrak{c}$.

Now assume that $\mathfrak{a}$ is an arbitrary ideal. Then $\mathfrak{ab} = \mathfrak{ac}$ implies that $(\mathfrak{aa}')\mathfrak{b} = (\mathfrak{aa}')\mathfrak{c}$. Since $\mathfrak{aa}' = (N\mathfrak{a})$ is principal, the claim follows from the first part of the proof. □

This shows that the ideals in $\mathbb{Z}_K$ form a monoid with cancellation law, analogous to the natural numbers. Such objects can be made into a group by imitating the construction of $\mathbb{Z}$ from $\mathbb{N}$. Another solution is to put $\mathfrak{ab}^{-1} = \frac{1}{b}\mathfrak{ab}'$, where $b = N\mathfrak{b}$ and $\frac{1}{m}\mathfrak{a} = \{\frac{\alpha}{m} : \alpha \in \mathfrak{a}\}$. Such sets are called fractional ideals.

Divisibility of Ideals. We say that an ideal $\mathfrak{b}$ is divisible by an ideal $\mathfrak{a}$ if there is an ideal $\mathfrak{c}$ such that $\mathfrak{b} = \mathfrak{ac}$. Since $\mathfrak{c} \subseteq \mathbb{Z}_K$ we see $\mathfrak{b} = \mathfrak{ac} \subseteq \mathfrak{a}(1) = \mathfrak{a}$; this fact is often expressed by saying "to divide is to contain". As a matter of fact, the converse is also true:

Proposition 7.7. *If $\mathfrak{a}, \mathfrak{b}$ are nonzero ideals in $\mathbb{Z}_K$, then $\mathfrak{a} \supseteq \mathfrak{b}$ if and only if $\mathfrak{a} \mid \mathfrak{b}$.*

Proof. From $\mathfrak{a} \supseteq \mathfrak{b}$ we deduce $\mathfrak{ba}' \subseteq \mathfrak{aa}' = (a)$, where $a = N\mathfrak{a}$. Then $\mathfrak{c} = \frac{1}{a}\mathfrak{ba}'$ is an ideal because of $\frac{1}{a}\mathfrak{a}'\mathfrak{b} \subseteq \mathbb{Z}_K$ (the ideal axioms are easily checked) Now the claim follows from $\mathfrak{ac} = \frac{1}{a}\mathfrak{baa}' = \mathfrak{b}$. □

We know that maximal ideals are always prime, as it is known that $\mathfrak{a}$ is maximal in a ring R if and only if $R/\mathfrak{a}$ is a field, and it is prime if and only if $R/\mathfrak{a}$ is an integral domain.

In the rings of integers in algebraic number fields all three notions coincide; irreducible and maximal ideals are the same:

- irreducible ideals are maximal: if $\mathfrak{a}$ were not maximal, then there were an ideal $\mathfrak{b}$ with $\mathfrak{a} \subsetneq \mathfrak{b} \subsetneq (1)$; this implies $\mathfrak{b} \mid \mathfrak{a}$ with $\mathfrak{b} \ne (1), \mathfrak{a}$.
- maximal ideals are irreducible: for $\mathfrak{a} = \mathfrak{bc}$ implies $\mathfrak{a} \subsetneq \mathfrak{b} \subsetneq (1)$.

It remains to show that, in our rings, prime ideals are maximal; note that this is not true in general rings. In fact we have to use Proposition 7.7 in the proof.

Proposition 7.8. *In rings of integers of qadratic number fields, prime ideals are maximal.*

Proof. Assume that $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ and $\mathfrak{a} \nmid \mathfrak{b}$; then $\mathfrak{a} \mid \mathfrak{c}$, and since $\mathfrak{c} \mid \mathfrak{a}$ (to divide is to contain) we have $\mathfrak{a} = \mathfrak{c}$ and therefore $\mathfrak{b} = (1)$. □

Observe that from $\mathfrak{a} \mid \mathfrak{c}$ and $\mathfrak{c} \mid \mathfrak{a}$ we cannot conclude equality $\mathfrak{a} = \mathfrak{c}$: we do get $\mathfrak{a} = \mathfrak{c}\mathfrak{d}$ and $\mathfrak{c} = \mathfrak{a}\mathfrak{e}$, hence $\mathfrak{a} = \mathfrak{d}\mathfrak{e}\mathfrak{a}$. But without the cancellation law we cannot conclude that $\mathfrak{d}\mathfrak{e} = (1)$.

In $R = \mathbb{Z}[X]$, the ideal (X) is prime since $\mathbb{Z}[X]/(X) \simeq \mathbb{Z}$ is an integral domain; it is not maximal, since $\mathbb{Z}$ is not a field, and in fact we have $(X) \subset (2, X) \subset R$.

Now we can prove

Theorem 7.9. *Every nonzero ideal $\mathfrak{a}$ in the ring of integers $\mathbb{Z}_K$ of a quadratic number field K can be written uniquely (up to order) as a product of prime ideals.*

Proof. We start with showing the existence of a factorization into irreducible ideals. If $\mathfrak{a}$ is irreducible, we are done. If not, then $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$; if $\mathfrak{b}$ and $\mathfrak{c}$ are irreducible, we are done. If not, we keep on factoring. Since $N\mathfrak{a} = N\mathfrak{b}N\mathfrak{c}$ and $1 < N\mathfrak{b}$, $N\mathfrak{c} < N\mathfrak{a}$ etc. this process must terminate, since the norms are natural numbers and cannot decrease indefinitely.

Now we prove uniqueness. Assume that $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$ are two decompositions of $\mathfrak{a}$ into prime ideals. We claim that $r = s$ and that we can reorder the $\mathfrak{q}_i$ in such a way that we have $\mathfrak{p}_i = \mathfrak{q}_i$ for $1 \le i \le r$. Since $\mathfrak{p}_1$ is prime, it divides some $\mathfrak{q}_j$ on the right hand side, say $\mathfrak{p}_1 \mid \mathfrak{q}_1$. Since $\mathfrak{q}_1$ is irreducible, we must have equality $\mathfrak{p}_1 = \mathfrak{q}_1$, and the cancellation law yields $\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_s$. The claim now follows by induction. □

8. Decomposition of Primes

Now that we know that ideals in $\mathbb{Z}_K$ can be factored uniquely into prime ideals, we have to come up with a description of these prime ideals. For quadratic (and, as we will see, also for cyclotomic) fields this is not hard.

Lemma 8.1. *Let $\mathfrak{p}$ be a prime ideal; then there is a unique prime number p such that $\mathfrak{p} \mid (p)$.*

Proof. We have $\mathfrak{p} \mid \mathfrak{p}\mathfrak{p}' = (N\mathfrak{p})$; decomposing $N\mathfrak{p}$ in $\mathbb{Z}$ into prime factors and using the fact that $\mathfrak{p}$ is prime shows that $\mathfrak{p}$ divides (hence contains) some ideal (p) for prime p. If $\mathfrak{p}$ would divide (hence contain) prime ideals (p) and (q) for different primes p and q, it would also contain 1, since p and q are coprime: this implies, by Bezout, the existence of $x, y \in \mathbb{Z}$ with $px + qy = 1$. □

If p is the prime contained in $\mathfrak{p}$, then we say that the prime ideal $\mathfrak{p}$ lies above p. Since (p) has norm p^2, we find that $N\mathfrak{p}$ equals p oder p^2.

Lemma 8.2. *If $\mathfrak{p}$ is an ideal in $\mathbb{Z}_K$ with norm p, then it is prime.*

Proof. The ideal is clearly irreducible ($\mathfrak{p} = \mathfrak{a}\mathfrak{b}$ implies $p = N\mathfrak{p} = N\mathfrak{a} \cdot N\mathfrak{b}$), hence prime. □

For describing the prime ideals in quadratic number fields it is useful to have the notion of the discriminant. If $K = \mathbb{Q}(\sqrt{m}\,)$ with m squarefree, let $\{1, \omega\}$ denote an integral basis. We then define

$$\operatorname{disc} K = \left|\begin{smallmatrix} 1 & \omega \\ 1 & \omega' \end{smallmatrix}\right|^2 = (\omega - \omega')^2 = \begin{cases} m & \text{if } m \equiv \ \ 1 \mod 4, \\ 4m & \text{if } m \equiv 2, 3 \mod 4. \end{cases}$$

Theorem 8.3. *Let p be an odd prime, $K = \mathbb{Q}(\sqrt{m}\,)$ a quadratic number field, and $d = \operatorname{disc} K$ its discriminant.*

- *If $p \mid d$, then $p\mathbb{Z}_K = (p, \sqrt{m}\,)^2$; we say that p is ramified in K.*
- *If $(d/p) = +1$, then $p\mathbb{Z}_K = \mathfrak{p}\mathfrak{p}'$ for prime ideals $\mathfrak{p} \neq \mathfrak{p}'$; we say that p splits (completely) in K.*
- *If $(d/p) = -1$, then $p\mathbb{Z}_K$ is prime, and we say that p is inert in K.*

Proof. Assume first that $p \mid d$; since p is odd, we also have $p \mid m$. Now

$$(p, \sqrt{m}\,)^2 = (p^2, p\sqrt{m}, m) = (p)(p, \sqrt{m}, \tfrac{m}{p}) = (p),$$

since the ideal $(p, \sqrt{m}, \frac{m}{p})$ contains the coprime integers p and $\frac{m}{p}$, hence equals (1).

Next assume that $(d/p) = 1$; then $d \equiv x^2 \bmod p$ for some integer $x \in \mathbb{Z}$. Putting $\mathfrak{p} = (p, x + \sqrt{m}\,)$ we find

$$\begin{aligned} \mathfrak{p}\mathfrak{p}' &= (p^2, p(x + \sqrt{m}\,), p(x - \sqrt{m}\,), x^2 - m) \\ &= (p)(p, x + \sqrt{m}, x - \sqrt{m}, (x^2 - m)/p). \end{aligned}$$

Clearly $2\sqrt{m} = x + \sqrt{m} - (x - \sqrt{m}\,)$ and therefore $4m = (2\sqrt{m})^2$ are contained in the last ideal; since p and $4m$ are coprime, this ideal equals (1), and we have $\mathfrak{p}\mathfrak{p}' = (p)$. If we had $\mathfrak{p} = \mathfrak{p}'$, then it would follow that $4m \in \mathfrak{p}$ and $\mathfrak{p} = (1)$: contradiction.

Finally assume that $(d/p) = -1$. If there were an ideal $\mathfrak{p}$ of norm p, Proposition 7.1 would show that it has the form $\mathfrak{p} = (p, b+\omega)$ with $p \mid N(b+\omega)$. If $\omega = \sqrt{m}$, this means $b^2 - m \equiv 0 \bmod p$, hence $(d/p) = (4m/p) = (m/p) = +1$ in contradiction to our assumption. If $\omega = \frac{1}{2}(1+\sqrt{m}\,)$, then $(2b+1)^2 \equiv m \bmod p$, and this again is a contradiction. □

The description of all prime ideals above 2 is taken care of by the following

Exercise. Let $K = \mathbb{Q}(\sqrt{m}\,)$ be a quadratic number field, where m is squarefree.

- If $m \equiv 2 \bmod 4$ then $2\mathbb{Z}_K = (2, \sqrt{m}\,)^2$.
- If $m \equiv 3 \bmod 4$ then $2\mathbb{Z}_K = (2, 1+\sqrt{m}\,)^2$.
- If $m \equiv 1 \bmod 8$ then $2\mathbb{Z}_K = \mathfrak{a}\mathfrak{a}'$, where $\mathfrak{a} = (2, \frac{1+\sqrt{m}}{2}\,)$ and $\mathfrak{a} \neq \mathfrak{a}'$.
- If $m \equiv 5 \bmod 8$ then $2\mathbb{Z}_K$ is prime.

The two cases p odd and $p = 2$ can be subsumed into one by introducing the *Kronecker-Symbol* (d/p). This agrees with the Legendre symbol for odd primes p and is defined for $p = 2$ and $d \equiv 1 \bmod 4$ by $(d/2) = (-1)^{(d-1)/4}$; for $d \not\equiv 1 \bmod 4$ we put $(d/2) = 0$.

Now we will derive a few corollaries.

Proposition 8.4. *Assume that $\mathbb{Z}_K$ is a PID, where $K = \mathbb{Q}(\sqrt{m}\,)$. Then every prime p with $(d/p) = +1$ can be written in the form $\pm p = x^2 - my^2$ if $m \equiv 2, 3 \bmod 4$, and in the form $\pm 4p = x^2 - my^2$ if $m \equiv 1 \bmod 4$.*

Proof. Assume that $(d/p) = +1$; then p splits in K, hence $p = \mathfrak{p}\mathfrak{p}'$ for prime ideals $\mathfrak{p}$, $\mathfrak{p}'$ of norm p. Since $\mathbb{Z}_K$ is a PID, there is an $\alpha \in \mathbb{Z}_K$ such that $\mathfrak{p} = (\alpha)$. Taking the norm show that $(N\alpha) = (p)$ as ideals, hence $N\alpha = \pm p$. The claim now follows by writing $\alpha = x + y\omega$, where $\{1, \omega\}$ is the standard integral basis of $\mathbb{Z}_K$. □

If we could show that the rings of integers in $\mathbb{Q}(\sqrt{m}\,)$ for $m = -1$ and $m = -2$ were PIDs, this would imply

- $p \equiv 1 \bmod 4 \Longrightarrow p = x^2 + y^2$,
- $p \equiv 1, 3 \bmod 8 \Longrightarrow p = x^2 + 2y^2$,

and many similar results.

This stresses the importance of finding a method for determining when $\mathbb{Z}_K$ is a PID.

9. The Ideal Class Group

Definition. We have seen that the set of nonzero ideals in $\mathbb{Z}_K$ form a monoid with cancellation law. Such monoids can be made into groups by imitating the construction of $\mathbb{Z}$ from $\mathbb{N}$ (or that of $\mathbb{Q}$) from $\mathbb{Z}$); the group I_K of these fractional ideals contains the group $H_K = \{(\alpha) : \alpha \in K^\times\}$ of principal ideals as a subgroup, and the quotient group $\mathrm{Cl}(K) = I_K/H_K$ is called the class group of K. This group is trivial if and only if $\mathbb{Z}_K$ is a PID. The order $h(K)$ of $\mathrm{Cl}(K)$ is called the class number of K.

We can avoid this formal procedure by introducing fractional ideals as actual sets: write $\mathfrak{a}\mathfrak{b}^{-1} = \mathfrak{a}\mathfrak{b}'(\mathfrak{b}\mathfrak{b}')^{-1} = \frac{1}{b}\mathfrak{a}\mathfrak{b}$, where $b = N\mathfrak{b}$ denotes the norm of $\mathfrak{b}$, and define $\frac{1}{\alpha}\mathfrak{c} := \{\frac{\gamma}{\alpha} : \gamma \in \mathfrak{c}\}$. The set of nonzero fractional ideals forms a group with respect to multiplication; note that the inverse of the integral ideal $\mathfrak{a}$ is the fractional ideal $\mathfrak{a}^{-1} = \frac{1}{a}\mathfrak{a}'$ with $a = N\mathfrak{a}$.

In these notes, we choose a third possibility: we define an equivalence relation on the set of all integral ideals and then make the equivalence classes into a group.

To this end, let $\mathfrak{a}$ and $\mathfrak{b}$ be two ideals; they are called equivalent ($\mathfrak{a} \sim \mathfrak{b}$) if there exist $\alpha, \beta \in \mathbb{Z}_K$ such that $\alpha\mathfrak{a} = \beta\mathfrak{b}$. Checking the usual axioms (symmetry, reflexivity, transitivity) is left as an exercise.

On the set of equivalence classes of ideals we define a multiplication as follows: given classes c und d, we pick representatives $\mathfrak{a} \in c$ and $\mathfrak{b} \in d$, and then put $c \cdot d = [\mathfrak{a}\mathfrak{b}]$. This definition does not depend on the choice of representatives; the class of the unit ideal is the neutral element; and finally the fact that $\mathfrak{a}\mathfrak{a}' = (a)$ shows that $[\mathfrak{a}]^{-1} = [\mathfrak{a}']$.

Thus the ideal classes $[\mathfrak{a}]$ form an abelian group $\mathrm{Cl}(K)$. If this group is trivial, then every ideal is equivalent to (1), that is, every ideal is principal. Since the converse is also clear, we see that $\mathbb{Z}_K$ is a PID if and only if K has class number 1.

Consider e.g. the ring $R = \mathbb{Z}[\sqrt{-5}\,]$; here we have the classes $1 = [(1)]$ und $c = [\mathfrak{a}]$ mit $\mathfrak{a} = (2, 1 + \sqrt{-5}\,)$. We have $c^2 = 1$ since $\mathfrak{a}^2 = (2)$ ist $c^2 = 1$. Putting $\mathfrak{b} = (3, 1 + \sqrt{-5}\,)$ we find $\mathfrak{a} \sim \mathfrak{b}$: in fact, $\mathfrak{a}\mathfrak{b} = (1 + \sqrt{-5}\,)$ implies $\mathfrak{a}\mathfrak{b} \sim (1)$, hence $[\mathfrak{b}] = [\mathfrak{a}]^{-1} = [\mathfrak{a}]$. More calculations seem to suggest that there are only two classes, that is, the class number of R seems to be 2.

The goal of this section is to show that $\mathrm{Cl}(K)$ is finite and to give an algorithm for computing it. The finiteness of the class group is one of three important finiteness theorems in algebraic number theory:

- $\mathrm{Cl}(K)$ is finite;
- $E_K = \mathbb{Z}_K^\times$ is a finitely generated abelian group;
- given a $B > 0$, the set of number fields with discriminant $< B$ is finite.

Finiteness of the Class Number. We now show that every ideal class in $\mathrm{Cl}(k)$ contains an integral ideal with norm bounded by a constant depending only on k; this immediately implies the finiteness of the class number.

Let us call an ideal in $\mathbb{Z}_K$ primitive if it is not divisible by a rational integer $m > 1$. Clearly every ideal class is represented by a primitive ideal.

According to Proposition 7.1, every ideal $\mathfrak{a}$ has a $\mathbb{Z}$-basis of the form $\{n, m(b+\omega)\}$ with $m \mid n$; Thus $\mathfrak{a}$ is primitive if and only if $m = 1$. In other words: if $\mathfrak{a}$ is primitive, then there exist $n \in \mathbb{N}$ and $b \in \mathbb{Z}$ such that $\mathfrak{a} = n\mathbb{Z} \oplus (b+\omega)\mathbb{Z}$, and we have $N\mathfrak{a} = n$. Now we claim:

Theorem 9.1. *Let $m \in \mathbb{Z}$ be squarefree, $K = \mathbb{Q}(\sqrt{m}\,)$ a quadratic field with ring of integers $\mathcal{O}_K = \mathbb{Z}[\omega]$ and discriminant d. Define the Gauss bound*

$$\mu_K = \begin{cases} \sqrt{d/5}, & \text{if } d > 0, \\ \sqrt{-d/3}, & \text{if } d < 0. \end{cases}$$

Then every ideal class in $\mathrm{Cl}(K)$ contains an integral nonzero ideal with norm $\le \mu_K$; in particular, the number $h = \#\,\mathrm{Cl}(K)$ of ideal classes is finite.

The bounds are clearly best possible: for $d = 5$ and $d = -3$ they are sharp. If $\mu_K \le 2$, then every ideal class contains a nonzero integral ideal with norm < 2; but then the norm must be 1, hence every ideal class contains the unit ideal, and we deduce that $h = 1$ and that $\mathcal{O}_K$ is a PID. Theorem 9.1 says that this is true for $-12 \le d \le 20$, i.e. for $m \in \{-11, -7, -3, -2, -1, 2, 3, 5, 13, 17\}$.

Exercise. If $d \equiv 5 \bmod 8$, then (2) is inert, hence there are no ideals of norm 2 in $\mathcal{O}_K$. Show that this implies that the fields with $d = -19, 21, 29, 37$ have class numberl 1. Which fields do you get by demanding in addition that (3) be inert (that is, $d \equiv 2 \bmod 3$)?

Now consider $R = \mathbb{Z}[\sqrt{-5}\,]$, where $d = -20$; according to Theorem 9.1, every ideal class contains a nonzero ideal with norm $< \sqrt{20/3}$, hence ≤ 2. Since there are only two such ideals, namely the unit ideal (1) and the nonprincipal ideal $(2, 1+\sqrt{-5}\,)$, we deduce that R has class number 2.

Actually we can show more: we have seen that $\mathrm{Cl}(K)$ is generated by the classes of (1) and $\mathfrak{a} = (2, 1+\sqrt{-5}\,)$. Now let p be a prime with $(-20/p) = +1$; then $p\mathbb{Z}_K = \mathfrak{p}\mathfrak{p}'$ for some prime ideal $\mathfrak{p}$ with norm p. Then $\mathfrak{p}$ is either principal, say $\mathfrak{p} = (a + b\sqrt{-5}\,)$ and thus $p = a^2 + 5b^2$, or $\mathfrak{p} \sim \mathfrak{a}$, and then $\mathfrak{a}\mathfrak{p} = (C + d\sqrt{-5}\,)$ is principal. In the latter case we get $2p = C^2 + 5d^2$; since C and d are both odd, we can write $C = 2c + d$ for some $c \in \mathbb{Z}$ and find $2p = (2c+d)^2 + 5d^2 = 4c^2 + 4cd + 6d^2$, that is, $p = 2c^2 + 2cd + 3d^2$. In other words: if $(-5/p) = +1$, then $p = a^2 + 5b^2$ or $p = 2c^2 + 2cd + 3d^2$.

Since $p = a^2 + 5b^2 \equiv a^2 + b^2 \equiv 1 \bmod 4$, this can only happen if $p \equiv 1 \bmod 20$. Similarly, $p = 2c^2 + 2cd + 3d^2 \equiv 3 \bmod 4$, that is, $p \equiv 11, 19 \bmod 20$. We have proved:

Theorem 9.2. *Primes $p \equiv 1, 9 \bmod 20$ are represented by the quadratic form $x^2 + 5y^2$, whereas primes $p \equiv 11, 19 \bmod 20$ are represented by $2x^2 + 2xy + 3y^2$.*

An important consequence of Theorem 9.1 is the following observation:

Corollary 9.3. *Let $K = \mathbb{Q}(\sqrt{m}\,)$ be a quadratic number field with class number h, and assume that $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$ splits completely in $\mathcal{O}_K$. Then there exist $x, y \in \mathbb{N}$ such that $\pm 4p^h = x^2 - my^2$.*

Proof. The h-th power of any ideal in $K = \mathbb{Q}(\sqrt{m}\,)$ is principal. In particular, $\mathfrak{p}^h = (\frac{x+y\sqrt{m}}{2})$ for suitable integers x, y, and taking the norm yields $p^h = |\frac{x^2-my^2}{4}|$. □

Proof of Theorem 9.1. Let $c = [\mathfrak{a}]$ be an ideal class represented by an ideal $\mathfrak{a}$. We may and will assume that $\mathfrak{a}$ is primitive. Therefore $\mathfrak{a} = (a, \alpha)$ with $a = N\mathfrak{a}$ and $\alpha = b + \omega = s + \frac{1}{2}\sqrt{d}$ for some $s \in \mathbb{Q}$ with $2s \in \mathbb{Z}$. If $a^2 \le \mu_K$, we are done; if not, we apply the Euclidean algorithm to the pair (s, a) and find $q \in \mathbb{Z}$ such that $s - qa = r$ and

$$\begin{aligned} |r| &\le \frac{a}{2} \quad \text{if } d < 0, \\ \frac{a}{2} \le |r| &\le a \quad \text{if } d > 0. \end{aligned}$$

Setting $\alpha_1 = r + \frac{1}{2}\sqrt{d}$ we find $\alpha_1 \in \mathfrak{a}$, $|N\alpha_1| \le \frac{1}{4}(a^2 - d) < a^2$, and $\mathfrak{a}_1 := \frac{1}{a}\alpha_1'\mathfrak{a} \sim \mathfrak{a}$ is an integral ideal with $[\mathfrak{a}_1] = [\mathfrak{a}]$ and $N\mathfrak{a}_1 < N\mathfrak{a}$. We repeat this step until we find an ideal of norm $\le \mu_K$; since the decreases with each step, the algorithm terminates.

The proof of the inequality $|N\alpha_1| \le \frac{1}{4}(a^2 - d) < a^2$ is simple: if $d < 0$, then $|N\alpha_1| = |r^2 - \frac{d}{4}| \le \frac{a^2+|d|}{4} < 1$ since $a^2 > \mu_K = \frac{|d|}{3}$, and if $d > 0$, we have $-a^2 = \frac{a^2-5a^2}{4} < r^2 - \frac{d}{4} < a^2$.

It remains to show that the ideal $\mathfrak{a}_1$ is integral; but this is clear in light of $\frac{1}{a}\alpha_1'\mathfrak{a} \subseteq \mathcal{O}_K \iff \alpha'\mathfrak{a} \subseteq (a) = \mathfrak{a}\mathfrak{a}' \iff (\alpha') \subseteq \mathfrak{a}'$. □

10. The Bachet-Mordell Equation

Let us now see what we can say about the integral solutions of the diophantine equation $y^2 = x^3 - d$ (named after Bachet and Mordell, who studied them). We will start with arbitrary d, but will impose conditions on d as we go along.

We start by factoring the equation over $K = \mathbb{Q}(\sqrt{d}\,)$:

$$x^3 = y^2 + d = (y + \sqrt{-d}\,)(y - \sqrt{-d}\,).$$

What can we say about the gcd of the ideals $\mathfrak{a} = (y + \sqrt{-d}\,)$ and $\mathfrak{a}'$? Any common prime factor $\mathfrak{p}$ (with $\mathfrak{p} \mid p$) also divides $2\sqrt{-d}$; since $\mathfrak{p} \mid \sqrt{-d}$ (and $p \ne 2$) implies $p \mid d$, $p \mid y$, $p \mid x$ and finally $p^2 \mid d$, we can exclude this possibility by demanding that d be $\boxed{\text{squarefree}}$.

We now have to discuss the remaining possibility $\mathfrak{p} \mid 2$:

- $d \equiv 2 \bmod 4$: then $\mathfrak{p} \mid (\sqrt{-d}\,)$ (since $\mathfrak{p} = (2, \sqrt{-d}\,)$), hence $\mathfrak{p} \mid y$, $p \mid y$ and finally $x^3 = y^2 + d \equiv 2 \bmod 4$: contradiction, since cubes cannot be divisible exactly by 2.
- $d \equiv 1 \bmod 4$: here $\mathfrak{p} = (2, 1 + \sqrt{-d}\,)$, hence $\mathfrak{p} \mid (y + \sqrt{-d}\,)$ if and only if y is odd. This implies $x^3 = y^2 + d \equiv 1 + 1 \equiv 2 \bmod 4$, which again is a contradiction.
- $d \equiv 3 \bmod 4$: here $y + \sqrt{-d}$ is divisible by $\mathfrak{p}$ (even by 2) if y is odd. Then $d = x^3 - y^2$ implies that x is even, hence $d \equiv -y^2 \equiv -1 \bmod 8$. Thus if we assume that $\boxed{d \not\equiv 7 \bmod 8}$, find that no $\mathfrak{p} \mid 2$ can be a common divisor of $\mathfrak{a}$ and $\mathfrak{a}'$.

Thus $\mathfrak{a}$ and $\mathfrak{a}'$ are coprime. Since their product is a cube, there exists an ideal $\mathfrak{b}$ such that $\mathfrak{a} = \mathfrak{b}^3$; conjugation then shows that $\mathfrak{a}'^3 = \mathfrak{b}'^3$.

Now let h denote the class number of $\mathbb{Q}(\sqrt{-d}\,)$. Since both $\mathfrak{b}^3$ as well as fb^h are principal, we can conclude that $\mathfrak{b}$ is principal if we assume that $\boxed{3 \nmid h}$. Thus $\mathfrak{b} = (\frac{r+s\sqrt{-d}}{2})$ with $r \equiv s \bmod 2$.

In the case $\boxed{d > 0,\ d \neq 1, 3}$ the only units are ±1, hence the ideal equation yields the equation of numbers

$$y + \sqrt{-d} = \Big(\frac{r + s\sqrt{-d}}{2}\Big)^3,$$

where we have subsumed the sign into the cube. Comparing coefficients now yields $1 = \frac18(3r^2s - ds^3)$, hence $8 = 3r^2s - ds^3 = s(3r^2 - ds^2)$.

This implies $s \mid 8$, hence $s = \pm1$ or $r \equiv s \equiv 0 \bmod 2$. In the first case we get $\pm 8 = 3r^2 - d$, hence $d = 3r^2 \mp 8$; in the second case we put $r = 2t$, $s = 2u$ and find $1 = u(3t^2 - du^2)$, that is $u = \pm 1$ and $d = 3t^2 \mp 1$.

Thus we have shown: if d, under the above assumptions, does not have the form $3t^2 \pm 1$ or $3t^2 \pm 8$, then the diophantine equation $y^2 = x^3 - d$ does not have an integral solution.

What happens if d has this form? Assume e.g. that $d = 3r^2 - 8$; then comparing coefficients (using $s = 1$) yields $8y = r^3 - 3dr = r^3 - 9r^3 + 24r = 24r - 8r^3$, that is $y = (3 - r^2)r$, as well as $y^2 + d = r^6 - 6r^4 + 12r^2 - 8 = (r - 2)^3$, hence $x = r - 2$. Thus $d = 3r^2 - 8$ yields the solution $(r^2 - 2, \pm(3 - r^2)r)$ of our diophantine equation. Similarly, other representations yield other solutions: $d = 3r^2 + 8$, $3t^2 + 1$, $3t^2 - 1$ gives rise to the solutions $(r^2 + 2, \pm r(r^2 + 3))$, $(4t^2 + 1, \pm t(8t^2 + 3))$, $(4t^2 - 1, \pm t(8t^2 - 3))$.

The only question that remains is: can d have more than one of these representations? The answer is: $d = 11$ has exactly two representations, all other d have at most one. The proof is simple: equations such as $3r^2 - 8 = 3t^2 - 1$ are impossible modulo 3; $3r^2 - 8 = 3t^2 + 1$ leads to $3(r^2 - t^2) = 9$, hence $r^2 - t^2 = (r - t)(r + t) = 3$, whose only solution is $r = \pm 2$, $t = \pm 1$, which leads to $d = 4$, but this is not squarefree; the possibility $3r^2 + 8 = 3t^2 - 1$ yields $3 = t^2 - r^2$, hence $t = \pm 2$, $r = \pm 1$ and thus $d = 3 + 8 = 3 \cdot 2^2 - 1 = 11$).

We have proved:

Theorem 10.1. *Let $d \neq 1, 3$ be a squarefree natural number, and assume that $d \not\equiv 7 \bmod 8$. If the class number of $\mathbb{Q}(\sqrt{-d}\,)$ is not divisible by 3, then the diophantine equation $y^2 = x^3 - d$ has*

1. *exactly two pairs of integral solutions $(3, \pm 4)$ and $(15, \pm 58)$ for $d = 11$;*
2. *exactly one pair of integral solutions if $d \neq 11$ has the form $d = 3t^2 \pm 1$ or $d = 3t^2 \pm 8$;*
3. *no integral solutions otherwise.*

Consider the case $d = 26 = 3 \cdot 3^2 - 1$: the equation $y^2 = x^3 - 26$ has the predicted solution $(207, \pm 42849)$ as well as $(3, \pm 1)$. The theorem implies that the class number of $\mathbb{Q}(\sqrt{-26}\,)$ must be divisible by 3; in fact we have $h = 6$.

Similarly it can be proved that the integral solutions of $x^p + y^p = z^p$ are only the trivial solutions if p does not divide the class number of $\mathbb{Q}(\zeta_p)$ – this is Kummer's approach to Fermat's problem.