12. Algebraic numbers

12.1 Quadratic fields

In Chapter 10.2, we solved the Pythagorean equation $x^2+y^2=z^2$ by writing it in the form $y^2=z^2-x^2=(z+x)(z-x)$ and applying the property of unique factorization to prime factors (in $\mathbb{Z}$) to conclude that $(z+x)/2$ and $(z-x)/2$ are perfect squares (after we checked that they are relatively prime). We encounter the question of whether we could apply the same idea directly to the equation $x^2+y^2=z^2$ without "modification", by using the factorization $(x+iy)(x-iy)=z^2$. Does it follow from this that $x+iy$ and $x-iy$ are squares in the corresponding ring which extends $\mathbb{Z}$? Or if we consider the equation $x^3=y^2+31$ (which we will, later on, solve in Example 16.5), can it be solved by using the factorization $x^3=(y+\sqrt{-31})(y-\sqrt{-31})$, and concluding that the factors on the right-hand side are cubes in the corresponding ring? We see that with the problems which are completely formulated in the set of integers (we want to find integer solutions of an equation with integer coefficients), we naturally come across the need to consider extensions of the ring $\mathbb{Z}$ (and the field $\mathbb{Q}$) and the need to consider which notions and results that we already proved in $\mathbb{Z}$ (especially the ones regarding divisibility, primes and unique factorization), can be translated into a more general situation, which problems emerge and is it possible and in which ways, to solve them.

The above-stated motivation leads us to study the properties of algebraic number fields and their rings of integers, and the simplest ones among them (except the field $\mathbb{Q}$ and ring $\mathbb{Z}$) are quadratic fields, so we will start our considerations in this chapter with them.

Definition 12.1. *A complex number α is called* an algebraic number *if there is a polynomial $Q(x)$ with rational coefficients, different from the zero polynomial, such that $Q(\alpha)=0$. A complex number is called* transcendental *if it is not algebraic.*

Theorem 12.1. *For any algebraic number α, there is a unique polynomial*

$$P(x) = a_d x^d + \cdots + a_1 x + a_0$$

with the following properties:

1) $P(x) \in \mathbb{Z}[x]$,

2) $a_d > 0$ *and* $\gcd(a_0, a_1, \ldots, a_d) = 1$,

3) $P(\alpha) = 0$,

4) *if* $P_0(x) \in \mathbb{Q}[x]$ *such that* $P_0(\alpha) = 0$, *then* $P(x) \mid P_0(x)$ *in* $\mathbb{Q}[x]$,

5) $P(x)$ *is irreducible over* $\mathbb{Q}$.

Proof: Let $\mathcal{M}$ be the set of all polynomials in $\mathbb{Q}[x]$, different from the zero polynomial, with the root α. The set of all positive integers which are degrees of polynomials in $\mathcal{M}$ is non-empty, so it contains the minimal element. Let that minimal element be d. Hence, there is $P_1(x) \in \mathbb{Q}[x]$ such that $\deg P_1 = d$ and $P_1(\alpha) = 0$. If we multiply $P_1(x)$ by the least common multiple of denominators of its coefficients, we obtain the polynomial $P_2(x)$ with integer coefficients. Let us divide $P_2(x)$ by the greatest common divisor of its coefficients and multiply it by -1 if its leading coefficient is negative. In this manner, we obtain a polynomial $P(x)$ for which we claim to satisfy all conditions of the theorem. The first three conditions are evidently satisfied.

Let $P_0 \in \mathbb{Q}[x]$ be such that $P_0(\alpha) = 0$. Let us divide polynomial $P_0(x)$ by $P(x)$. We obtain

$$P_0(x) = P(x)S(x) + R(x), \quad S(x), R(x) \in \mathbb{Q}[x], \quad \deg R(x) \le d - 1.$$

Since $P_0(\alpha) = P(\alpha) = 0$, we have also $R(\alpha) = 0$, so due to the minimality of d, the polynomial $R(x)$ has to be the zero polynomial. Hence, $P(x) \mid P_0(x)$ and property 4) is proved.

Let us prove that $P(x)$ is irreducible over $\mathbb{Q}$. If it were reducible, we would have $P(x) = Q_1(x)Q_2(x)$, where $1 \le \deg Q_i \le d - 1$, so we would have $Q_1(\alpha) = 0$ or $Q_2(\alpha) = 0$, contradicting the assumption on the minimality of the degree of $P(x)$.

Finally, let us show the uniqueness of $P(x)$. Let $T(x) \in \mathbb{Q}[x]$ be a polynomial which satisfies the properties 1) – 5). Then there is a polynomial $U(x)$ such that $T(x) = P(x)U(x)$. From the irreducibility of $T(x)$, it follows that $U(x)$ is a constant, while from property 2), it follows that $U(x) = 1$, so $T(x) = P(x)$. □

Definition 12.2. *The* minimal polynomial over $\mathbb{Z}$ *of an algebraic number α is the polynomial $P(x)$ described in Theorem 12.1. The* minimal polynomial *of α is the polynomial $g(x) = \frac{1}{a_d}P(x)$, hence, it is the irreducible monic polynomial with rational coefficients such that $g(\alpha) = 0$. The* degree *of an algebraic number is the degree of its minimal polynomial.*

Theorem 12.2. *The set of all algebraic numbers forms a field.*

Proof: Let α and $\beta \neq 0$ be algebraic numbers. We need to show that then $\alpha + \beta$, $\alpha\beta$, $-\beta$ and β^{-1} are algebraic numbers. Let $f(x)$ and $g(x)$ be the minimal polynomials of α, and β. If we apply Corollary 11.22 to the polynomials $f(x)$ and $g(x)$, we conclude that $\alpha + \beta$ and $\alpha\beta$ are algebraic numbers because they are roots of the polynomials (defined in the corollary) $h_1(x)$ and $h_2(x)$, respectively, with the coefficients from $\mathbb{Q}$. The number $-\beta$ is algebraic because it is a root of the polynomial $g(-x)$, while the number β^{-1} is algebraic because it is a root of the polynomial $x^m g(1/x)$, where m is the degree of g. □

Definition 12.3. *An algebraic number α is an* algebraic integer *if its minimal polynomial has integer coefficients; in other words, if its minimal polynomial over $\mathbb{Z}$ is monic.*

Proposition 12.3. *Among rational numbers, the only algebraic integers are precisely the (ordinary) integers.*

Proof: Each $m \in \mathbb{Z}$ is an algebraic integer because its minimal polynomial is $f(x) = x - m$. On the other hand, if $\frac{m}{q}$, where $\gcd(m, q) = 1$, is an algebraic integer, then we have

$$\left(\frac{m}{q}\right)^n + a_{n-1}\left(\frac{m}{q}\right)^{n-1} + \cdots + a_0 = 0,$$
$$m^n + a_{n-1}qm^{n-1} + \cdots + a_0q^n = 0.$$

Hence, $q \mid m^n$, so from $\gcd(m, q) = 1$, it follows that $q = \pm 1$, which means that $\frac{m}{q} \in \mathbb{Z}$. □

Definition 12.4. *Let d be a square-free integer and $d \neq 1$. A* quadratic field *$\mathbb{Q}(\sqrt{d})$ is the set of all numbers of the form $u + v\sqrt{d}$, $u, v \in \mathbb{Q}$, with the usual operations of addition and multiplication of complex numbers.*

In Definition 12.4, we could take that the number d is an integer which is not a perfect square. Evidently, $\mathbb{Q}(\sqrt{dm^2}) = \mathbb{Q}(\sqrt{d})$ for $m \in \mathbb{Q}$, $m \neq 0$, so the assumption that d is square-free is no loss of generality.

It is easily proved that $\mathbb{Q}(\sqrt{d})$ is indeed a field. Let us show that any element $u+v\sqrt{d} \in \mathbb{Q}(\sqrt{d})\setminus\{0\}$ has an inverse in $\mathbb{Q}(\sqrt{d})$. We have $u^2 - dv^2 \neq 0$, so

$$(u+v\sqrt{d})^{-1} = \frac{u}{u^2-dv^2} - \frac{v}{u^2-dv^2}\sqrt{d} \in \mathbb{Q}(\sqrt{d}).$$

For an element $\alpha = u + v\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, the *norm* of α is defined as $N(\alpha) = u^2 - dv^2$. Hence, $N(\alpha) = \alpha\overline{\alpha}$, where $\overline{\alpha} = u - v\sqrt{d}$ is the conjugate of α. In particular, the field $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i)$ is called the *field of Gaussian rationals* and its elements are usually written in the form $u+vi$. In this case, $N(\alpha) = u^2 + v^2$.

Theorem 12.4. *If $d \equiv 2$ or $3 \pmod 4$, then the algebraic integers in $\mathbb{Q}(\sqrt{d})$ are all numbers of the form $u + v\sqrt{d}$, $u, v \in \mathbb{Z}$. If $d \equiv 1 \pmod 4$, then the algebraic integers in $\mathbb{Q}(\sqrt{d})$ are all numbers of the form $s+t\cdot\frac{1+\sqrt{d}}{2}$, $s,t \in \mathbb{Z}$. In other words, algebraic integers in $\mathbb{Q}(\sqrt{d})$ are all numbers of the form $u+v\sqrt{d}$, $u, v \in \mathbb{Z}$ and if $d \equiv 1 \pmod 4$, also the numbers of the form $\frac{u+v\sqrt{d}}{2}$, u, v odd.*

Proof: Let $\alpha = u+v\sqrt{d}$ be an algebraic integer in $\mathbb{Q}(\sqrt{d})$ and let $a = 2u$, $b = 2v$, $c = N(\alpha) = u^2 - dv^2$. Then α is a root of the polynomial $f(x) = x^2 - ax + c$. Therefore, rational numbers a and c have to be integers. We have $db^2 = a^2 - 4c$, and since d is square-free, we see that it is also $b \in \mathbb{Z}$.

Let now $d \equiv 2$ or $3 \pmod 4$. From $a^2 \equiv b^2 d \pmod 4$, $a^2 \equiv 0$ or $1 \pmod 4$, $b^2 d \equiv 0$, 2 or $3 \pmod 4$, it follows that a and b are even numbers, so $u, v \in \mathbb{Z}$.

If $d \equiv 1 \pmod 4$, then from $a^2 \equiv b^2 \pmod 4$, it follows that a and b have the same parity. Therefore, the number $u - v = \frac{1}{2}(a-b)$ is an integer. Let $s = u - v$, $t = 2v$. Then $s, t \in \mathbb{Z}$ and $u + v\sqrt{d} = s + t\cdot\frac{1+\sqrt{d}}{2}$. □

Definition 12.5. A unit *(or an invertible element) in $\mathbb{Q}(\sqrt{d})$ is an algebraic integer ε with the property that $\frac{1}{\varepsilon}$ is also an algebraic integer.*

Theorem 12.5.

1) $N(\alpha\beta) = N(\alpha)N(\beta)$

2) $N(\alpha) = 0 \iff \alpha = 0$

3) *If α is an algebraic integer in $\mathbb{Q}(\sqrt{d})$, then $N(\alpha) \in \mathbb{Z}$.*

4) *Let γ be an algebraic integer in $\mathbb{Q}(\sqrt{d})$. Then γ is a unit if and only if $N(\gamma) = \pm 1$.*

Proof:

1) Let $\alpha = u + v\sqrt{d}$, $\beta = s + t\sqrt{d}$. Then

$$\begin{aligned}\overline{\alpha\beta} &= \overline{(us + vtd + (ut + vs)\sqrt{d})} = us + vtd - (ut + vs)\sqrt{d} \\ &= (u - v\sqrt{d})(s - t\sqrt{d}) = \overline{\alpha} \cdot \overline{\beta}.\end{aligned}$$

   Therefore,

$$N(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = \alpha\beta\overline{\alpha}\overline{\beta} = (\alpha\overline{\alpha})(\beta\overline{\beta}) = N(\alpha)N(\beta).$$

2) If $\alpha = 0$, then $\overline{\alpha} = 0$ and $N(\alpha) = 0$. If $N(\alpha) = 0$, then $\alpha\overline{\alpha} = 0$, so $\alpha = 0$ or $\overline{\alpha} = 0$. However, from $\overline{\alpha} = 0$, it follows that $\alpha = 0$.

3) This is proved in the proof of Theorem 12.4.

4) If γ is a unit, then $N(\gamma)N(\frac{1}{\gamma}) = N(1) = 1$, so since $N(\gamma)$ and $N(\frac{1}{\gamma})$ are integers, it follows that $N(\gamma) = \pm 1$.

   Conversely, if $N(\gamma) = \pm 1$, then $\gamma\overline{\gamma} = \pm 1$, so $\frac{1}{\gamma} = \pm\overline{\gamma}$ is an algebraic integer, which means that γ is a unit. □

We call a quadratic field $\mathbb{Q}(\sqrt{d})$ *real* if $d > 0$, and *imaginary* if $d < 0$.

Theorem 12.6. *Let d be a negative square-free integer. The quadratic field $\mathbb{Q}(\sqrt{d})$ has units ± 1, and those are the only units except in the cases $d = -1$ and $d = -3$. The units of $\mathbb{Q}(i)$ are ± 1, $\pm i$, and of $\mathbb{Q}(\sqrt{-3})$ are ± 1, $\frac{1 \pm \sqrt{-3}}{2}$, $\frac{-1 \pm \sqrt{-3}}{2}$.*

Proof: According to Theorem 12.5.4), we need to find all algebraic integers α such that $N(\alpha) = \pm 1$. If $d \equiv 2$ or $3 \pmod 4$, then α has the form $\alpha = x + y\sqrt{d}$, $x, y \in \mathbb{Z}$, so the equations $x^2 - dy^2 = \pm 1$ need to be solved. Since d is negative, the case $x^2 - dy^2 = -1$ can be discarded. If $d \leq -2$, then $x^2 - dy^2 \geq 2y^2$, so the only solutions are $(x, y) = (\pm 1, 0)$, which gives $\alpha = \pm 1$. If $d = -1$, then we have the equation $x^2 + y^2 = 1$ whose solutions (x, y) are given by $x = \pm 1$, $y = 0$ and $x = 0$, $y = \pm 1$, i.e. $\alpha = \pm 1$, $\pm i$.

If $d \equiv 1 \pmod 4$, then α has the form $x + y \cdot \frac{1+\sqrt{d}}{2}$, so $N(\alpha) = (x + \frac{y}{2})^2 - \frac{1}{4}dy^2$. Again, since $d < 0$, the equation $N(\alpha) = -1$ does not have solutions. If $d \leq -7$, then $(x + \frac{y}{2})^2 - \frac{1}{4}dy^2 \geq \frac{7}{4}y^2$, so from $N(\alpha) = 1$, it follows that $y = 0$, $x = \pm 1$, i.e. $\alpha = \pm 1$. If $d = -3$, then we have the equation

$$\left(x + \frac{y}{2}\right)^2 + \frac{3}{4}y^2 = 1, \tag{12.1}$$

and we get $x^2 + xy + y^2 = 1$. From (12.1), it follows that $|y| \leq 1$. If $y = 0$, then $x = \pm 1$, so $\alpha = \pm 1$. If $y = 1$, then $x = 0$ or $x = -1$, so $\alpha = \frac{1+\sqrt{-3}}{2}$ or $\alpha = \frac{-1+\sqrt{-3}}{2}$, if $y = -1$, then $x = 0$ or $x = 1$, so $\alpha = \frac{-1-\sqrt{-3}}{2}$ or $\alpha = \frac{1-\sqrt{-3}}{2}$. □

Theorem 12.7. *Every real quadratic field has infinitely many units.*

Proof: The numbers $\alpha = x + y\sqrt{d}$, $x, y \in \mathbb{Z}$ are algebraic integers in $\mathbb{Q}(\sqrt{d})$ with the norm $N(\alpha) = x^2 - dy^2$. If $x^2 - dy^2 = 1$, then α is a unit. However, the equation $x^2 - dy^2 = 1$ is Pell's equation and, for a square-free integer $d > 1$, it has infinitely many solutions. □

We see that the problem of finding units of real quadratic fields is in tight connection to Pell's equations. To be more precise:

- if $d \equiv 2$ or $3 \pmod 4$, then $u + v\sqrt{d}$ is a unit in $\mathbb{Q}(\sqrt{d})$ if and only if $u^2 - dy^2 = \pm 1$,

- if $d \equiv 1 \pmod 4$, then $\frac{u+v\sqrt{d}}{2}$ is a unit in $\mathbb{Q}(\sqrt{d})$ if and only if $u^2 - dy^2 = \pm 4$.

Therefore, apart from the ordinary Pell's equation $x^2 - dy^2 = 1$, the equations $x^2 - dy^2 = -1, 4, -4$ also should be considered, as we did in Chapter 10.3 (they are also often called Pell's equations).

The results from Chapter 10.3 on the equations $x^2 - dy^2 = \pm 1, \pm 4$ will now be interpreted in terms of units of real quadratic fields, which was a part of our motivation for studying them. The following corollary is a direct consequence of Theorems 10.11, 10.14, 10.16 and 10.18, in which the structure of the set of all solutions of Pell's equations is given.

Corollary 12.8. *The group of units of a real quadratic field $\mathbb{Q}(\sqrt{d})$ has two generators: -1 and ϵ_d, where $\epsilon_d = a + b\sqrt{d}$ or $\frac{a+b\sqrt{d}}{2}$, while $a + b\sqrt{d}$ is the fundamental solution of one of Pell's equations $x^2 - dy^2 = \pm 1, \pm 4$. Therefore, each unit can be written in the form $\pm\epsilon_d^n$, $n \in \mathbb{Z}$. The generator ϵ_d is called* the fundamental unit *of the quadratic field $\mathbb{Q}(\sqrt{d})$. If $x_1 + y_1\sqrt{d}$ is the fundamental solution of Pell's equation $x^2 - dy^2 = 1$, then $x_1 + y_1\sqrt{d} = (a + b\sqrt{d})^\nu$, where $\nu \in \{1, 2, 3, 6\}$.*

More precise information on the exponent is given in the following table, which can be used to determine ν from congruence properties of the numbers a, b, d (see also [419]).

d	a^2-db^2	b	a	ν	example
$\equiv 3 \pmod 4$	1			1	$d=3$
$\equiv 1,2 \pmod 4$	1	$\equiv 0 \pmod 2$		1	$d=6$
$\equiv 1,2 \pmod 4$	-1	$\equiv 1 \pmod 2$		2	$d=2$
$\equiv 5 \pmod{16}$	4	$\equiv 1 \pmod 2$	$\equiv \pm 3b \pmod 8$	3	$d=21$
$\equiv 5 \pmod{16}$	-4	$\equiv 1 \pmod 2$	$\equiv \pm b \pmod 8$	6	$d=5$
$\equiv 13 \pmod{16}$	4	$\equiv 1 \pmod 2$	$\equiv \pm b \pmod 8$	3	$d=45$
$\equiv 13 \pmod{16}$	-4	$\equiv 1 \pmod 2$	$\equiv \pm 3b \pmod 8$	6	$d=13$

Table 12.1: The connection between fundamental solutions and fundamental units

Definition 12.6. *For algebraic integers α, β in $\mathbb{Q}(\sqrt{d})$, we say that α* divides *β and write $\alpha \mid \beta$ if there is an algebraic integer γ in $\mathbb{Q}(\sqrt{d})$ such that $\beta = \alpha\gamma$. Accordingly, the units are exactly the divisors of 1. We say that α and β are* associated *if α/β is a unit.*

We call an algebraic integer α in $\mathbb{Q}(\sqrt{d})$, which is not 0 nor a unit in $\mathbb{Q}(\sqrt{d})$, irreducible *if it is divisible only by units and associated numbers. We call an algebraic integer π in $\mathbb{Q}(\sqrt{d})$* prime *if π is not 0 nor a unit in $\mathbb{Q}(\sqrt{d})$ and if π has the property that if π divides $\beta\gamma$, where β, γ are algebraic integers in $\mathbb{Q}(\sqrt{d})$, then π divides β or π divides γ.*

It is clear that every prime number is irreducible. Indeed, if $\pi = \beta\gamma$, then one of the numbers β/π or γ/π is an algebraic integer so one of the numbers γ or β is a unit. In the set of integers $\mathbb{Z}$, the converse also holds (Proposition 2.11); however, generally, an irreducible element does not need to be prime. For example, the number 2 is irreducible in $\mathbb{Q}(\sqrt{-5})$ because from $2 = \beta\gamma$, it follows that $N(\beta)N(\gamma) = 4$, and since the equations $x^2 + 5y^2 = \pm 2$ do not have integer solutions, it follows that $N(\beta) = \pm 1$ or $N(\gamma) = \pm 1$, so one of the numbers β or γ is a unit. However, the number 2 is not prime in $\mathbb{Q}(\sqrt{-5})$ since 2 divides $(1+\sqrt{-5})(1-\sqrt{-5}) = 6$, but 2 does not divide $1+\sqrt{-5}$ nor $1-\sqrt{-5}$ because $N(2) = 4$ does not divide $N(1+\sqrt{-5}) = N(1-\sqrt{-5}) = 6$.

Theorem 12.9. *If the norm of an algebraic integer α in $\mathbb{Q}(\sqrt{d})$ is equal to $\pm p$, where p is an (ordinary) prime number, then α is irreducible.*

Proof: Assume that $\alpha = \beta\gamma$, where β and γ are integers in $\mathbb{Q}(\sqrt{d})$. According to Theorem 12.5.1), $N(\alpha) = N(\beta)N(\gamma) = \pm p$. Since $N(\beta)$ and $N(\gamma)$ are integers, one of them has to be equal to ± 1. Accordingly, one of the numbers β and γ is a unit and the other is associated with α. □

Theorem 12.10. *Every algebraic integer α in $\mathbb{Q}(\sqrt{d})$, which is not 0 nor a unit, can be represented as a product of irreducible numbers in $\mathbb{Q}(\sqrt{d})$.*

Proof: If α is not irreducible, then it can be factorized into the product $\beta\gamma$, where β and γ are not units. By continuing this process, we factorize β and γ if they are not irreducible. This process of factorization has to finish because, otherwise, we would obtain that α has the form $\beta_1\beta_2\cdot\ldots\cdot\beta_n$, where n is arbitrary large, and none of β_j is a unit. From this, it would follow that

$$|N(\alpha)| = \prod_{j=1}^{n} |N(\beta_j)| \geq 2^n$$

since $|N(\beta_j)|$ is a positive integer greater than 1. However, that is evidently a contradiction. □

Even though we demonstrated that a factorization into the irreducible factors in $\mathbb{Q}(\sqrt{d})$ always exists; it does not need to be unique.

Example 12.1. Let us consider the number 10 and its two factorizations in $\mathbb{Q}(\sqrt{-6})$:

$$10 = 2\cdot 5 = (2+\sqrt{-6})(2-\sqrt{-6}).$$

The numbers 2, 5, $2+\sqrt{-6}$, $2-\sqrt{-6}$ are irreducible in $\mathbb{Q}(\sqrt{-6})$.

Indeed, let us notice first that if an algebraic integer α in $\mathbb{Q}(\sqrt{-6})$ is not 0 nor a unit, then $N(\alpha) = N(a+b\sqrt{-6}) = a^2+6b^2 \geq 4$ and $N(\alpha) \neq 5$. If $2 = \alpha\beta$, then from $N(\alpha)N(\beta) = 4$, it follows that $N(\alpha) = \pm 1$ or $N(\beta) = \pm 1$. Analogously, if $5 = \alpha\beta$, then from $N(\alpha)N(\beta) = 25$, it follows that $N(\alpha) = \pm 1$ or $N(\beta) = \pm 1$. Finally, if $2 \pm \sqrt{-6} = \alpha\beta$, then from $N(\alpha)N(\beta) = 10$, it follows again that $N(\alpha) = \pm 1$ or $N(\beta) = \pm 1$.

Accordingly, the number 10 does not have a unique factorization to irreducible factors in $\mathbb{Q}(\sqrt{-6})$. ◇

The important question is, for which values of d does $\mathbb{Q}(\sqrt{d})$ have the property of unique factorization? We will see that this question is connected to Euclid's algorithm.

Definition 12.7. *We say that a quadratic field $\mathbb{Q}(\sqrt{d})$ has the* unique factorization property *if every algebraic integer in $\mathbb{Q}(\sqrt{d})$, which is not 0 nor a unit, can be uniquely factorized into irreducible factors, up to the order of the factors and the replacement of the factors by associated numbers.*

We say that a quadratic field is Euclidean *if it is possible to apply an analogue of Euclid's algorithm to algebraic integers in $\mathbb{Q}(\sqrt{d})$, i.e. if for any algebraic integers α, β in $\mathbb{Q}(\sqrt{d})$, $\beta \neq 0$, there exist algebraic integers γ and δ in $\mathbb{Q}(\sqrt{d})$ such that $\alpha = \beta\gamma + \delta$ and $|N(\delta)| < |N(\beta)|$.*

Theorem 12.11. *Every Euclidean quadratic field has the unique factorization property.*

Proof: Let us first show that if α and β are algebraic integers in $\mathbb{Q}(\sqrt{d})$ which do not have common divisors except units, then there are algebraic integers λ_0, μ_0 in $\mathbb{Q}(\sqrt{d})$ such that

$$\alpha\lambda_0 + \beta\mu_0 = 1.$$

Let $\mathcal{S}$ be the set of all numbers of the form $\alpha\lambda + \beta\mu$, where λ and μ run through the set of all algebraic integers in $\mathbb{Q}(\sqrt{d})$. The numbers $|N(\alpha\lambda+\beta\mu)|$ are non-negative integers, so let us choose an element $\varepsilon = \alpha\lambda_1 + \beta\mu_1$ of the set $\mathcal{S}$ such that $|N(\varepsilon)|$ takes the smallest positive value among the numbers $|N(\alpha\lambda + \beta\mu)|$. By applying Euclid's algorithm to α and ε, we obtain

$$\alpha = \varepsilon\gamma + \delta, \quad |N(\delta)| < |N(\varepsilon)|.$$

Then $\delta = \alpha - \gamma(\alpha\lambda_1 + \beta\mu_1) = \alpha(1 - \gamma\lambda_1) + \beta(-\gamma\mu_1) \in \mathcal{S}$. According to the definition of ε, we have $N(\delta) = 0$, i.e. $\delta = 0$. Hence, $\alpha = \varepsilon\gamma$ and $\varepsilon \mid \alpha$. It is similarly shown that $\varepsilon \mid \beta$, so ε is a unit. Now, ε^{-1} is also a unit, and we have

$$1 = \varepsilon^{-1}\varepsilon = \varepsilon^{-1}(\alpha\lambda_1 + \beta\mu_1) = \alpha(\varepsilon^{-1}\lambda_1) + \beta(\varepsilon^{-1}\mu_1) = \alpha\lambda_0 + \beta\mu_0.$$

Let us now prove that if π is irreducible in $\mathbb{Q}(\sqrt{d})$, then π is prime, i.e. if $\pi \mid \alpha\beta$, then $\pi \mid \alpha$ or $\pi \mid \beta$. Indeed, if $\pi \nmid \alpha$, then π and α do not have common divisors except units, so there are algebraic integers λ_0 and μ_0 such that $\pi\lambda_0 + \alpha\mu_0 = 1$. Then $\beta = \pi\beta\lambda_0 + \alpha\beta\mu_0$, so $\pi \mid \beta$. From this, it follow by induction that if $\pi \mid (\alpha_1 \cdot \ldots \cdot \alpha_n)$, then π divides at least one of the factors α_j.

From this point, the proof is identical to the proof of Theorem 2.12. □

It is known that there are exactly 21 Euclidean quadratic fields $\mathbb{Q}(\sqrt{d})$ (Chatland and Davenport, 1950):

$$d = -11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73.$$

These are not all quadratic fields with unique factorization property. Heegner (1952), Baker (1966) and Stark (1967) showed that if $d < 0$, then $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$ (compare this list with the list from Chapter 5.2 of negative discriminants d for which the class number $h(d)$ is equal to 1). A conjecture is that for $d > 0$, there are infinitely many such fields (see [384]).

Example 12.2. *Prove that the quadratic fields $\mathbb{Q}(\sqrt{d})$ for $d = -11, -7, -3, -2, -1, 2, 3, 5$ are Euclidean.*

Solution: Let α, β be algebraic integers in $\mathbb{Q}(\sqrt{d})$ and $\beta \neq 0$. Then $\frac{\alpha}{\beta} = u + v\sqrt{d}$, $u, v \in \mathbb{Q}$. Let us choose $x, y \in \mathbb{Z}$ which are the nearest to u and v, respectively, i.e.

$$0 \leq |u - x| \leq \frac{1}{2}, \quad 0 \leq |v - y| \leq \frac{1}{2}.$$

Let $x + y\sqrt{d} = \gamma$, $\alpha - \beta\gamma = \delta$. The numbers γ and δ are integers in $\mathbb{Q}(\sqrt{d})$ and

$$\begin{aligned} N(\delta) &= N(\alpha - \beta\gamma) = N(\beta)N(\frac{\alpha}{\beta} - \gamma) = N(\beta)N((u - x) + (v - y)\sqrt{d}) \\ &= N(\beta)((u - x)^2 - d(v - y)^2), \end{aligned}$$

so

$$|N(\delta)| = |N(\beta)| \cdot |(u - x)^2 - d(v - y)^2|. \tag{12.2}$$

If $d > 0$, then $-\frac{d}{4} \leq (u - x)^2 - d(v - y)^2 \leq \frac{1}{4}$, and if $d < 0$, then $0 \leq (u - x)^2 - d(v - y)^2 \leq \frac{1}{4} + \frac{1}{4}(-d)$. Therefore, if $d = 2, 3, -1, -2$, then from (12.2), we obtain $|N(\delta)| < |N(\beta)|$, so for those values of d, the field $\mathbb{Q}(\sqrt{d})$ is Euclidean.

For $d = -11, -7, -3, 5$, we proceed slightly differently. Let us notice that in all these cases, we have $d \equiv 1 \pmod 4$. Let u and v be defined as before. Choose $y \in \mathbb{Z}$ as the nearest integer to $2v$ and put $s = v - \frac{1}{2}y$. Then $|s| \leq \frac{1}{4}$. Furthermore, choose $x \in \mathbb{Z}$ as the nearest integer to $u - \frac{1}{2}y$ and put $r = u - x - \frac{1}{2}y$. Then $|r| \leq \frac{1}{2}$. Let $x + y \cdot \frac{1+\sqrt{d}}{2} = \gamma$, $\alpha - \beta\gamma = \delta$. Now, $N(\delta) = N(\beta)(r^2 - ds^2)$. Since $|d| \leq 11$, we have $|r^2 - ds^2| \leq \frac{1}{4} + 11 \cdot \frac{1}{16} < 1$, so we conclude that $|N(\delta)| < |N(\beta)|$, which needed to be proved. ♢

Theorem 12.12. *Let $\mathbb{Q}(\sqrt{d})$ have the unique factorization property. Then to any irreducible number π in $\mathbb{Q}(\sqrt{d})$, there corresponds exactly one (ordinary) prime number p such that $\pi \mid p$.*

Proof: The irreducible number π divides the integer $N(\pi)$, so there are positive integers which are divisible by π. Let p be the smallest such number. Let us prove that p is prime in $\mathbb{Z}$ (primes in $\mathbb{Z}$ are sometimes called "rational primes", to distinguish them from primes in quadratic fields or other number fields; similarly, elements of $\mathbb{Z}$ are sometimes called "rational integers"). Otherwise, it would be $p = n_1 n_2$, so due to the unique factorization property, $\pi \mid n_1$ or $\pi \mid n_2$, which is a contradiction since $1 < n_1, n_2 < p$.

Let us assume that π divides another rational prime number q. Then $\gcd(p, q) = 1$, so there are integers x, y such that $px + qy = 1$. From this, it follows that $\pi \mid 1$, which is a contradiction. Accordingly, the prime number p is unique. □

Theorem 12.13. *Prime numbers in $\mathbb{Q}(i)$ are rational primes of the form $p = 4k + 3$, factors π and π' from the factorization $p = \pi\pi'$ of rational primes of the form $p = 4k + 1$, number $1 + i$, and numbers which are associated to the above-listed (i.e. those which are obtained from them by multiplying by ± 1 or $\pm i$).*

Proof: Let p be a rational prime number. If p is divisible by an irreducible number π in $\mathbb{Q}(i)$, then from $p = \pi\lambda$, it follows that $N(\pi)N(\lambda) = p^2$. Now, we have two possibilities: it is either $N(\lambda) = 1$, which means that p is prime in $\mathbb{Q}(i)$ or $N(\lambda) = p$, from which it follows that $N(\pi) = p$, so $p = \pi\lambda$ is a product of two irreducible numbers in $\mathbb{Q}(i)$.

If $p \equiv 3 \pmod 4$, then according to Proposition 5.2, it cannot be $N(\pi) = N(a + bi) = a^2 + b^2 = p$. Therefore, p is irreducible in $\mathbb{Q}(i)$.

If $p \equiv 1 \pmod 4$, then according to Propositions 5.5 and 5.6, there are unique positive integers a, b such that $p = a^2 + b^2 = (a + bi)(a - bi)$ and from the previous discussion, the numbers $a + bi$ and $a - bi$ are irreducible in $\mathbb{Q}(i)$.

For the number 2, we have $2 = (1 + i)(1 - i)$. Numbers $1 + i$, $1 - i$ are irreducible in $\mathbb{Q}(i)$, and they are associated, which completes the proof. □

12.2 Algebraic number fields

Studying algebraic number fields (or shorter, number fields) began in 19th century by Kummer, Dedekind and Weber. The motivation came from solving Diophantine equations, and, first of all, Fermat's Last Theorem. This is a central topic in the branch of mathematics which is called algebraic number theory. The systematic consideration of this topic would require its own book (such as numerous books devoted to algebraic number theory, e.g. [9, 234, 287, 322, 325, 357, 387]), so in this book, we decided to provide a concise overview, based mostly on [24] and [344].

Let α be an algebraic number. The algebraic number field $\mathbb{Q}(\alpha)$ generated by α is the smallest field which contains $\mathbb{Q}$ and α. It is said that $\mathbb{Q}(\alpha)$ is a *simple algebraic extension* of $\mathbb{Q}$. From the definition, it follows that $\mathbb{Q}(\alpha)$ is the set of all quotients of the form $f(\alpha)/h(\alpha)$ where $f(x)$ and $h(x)$ are polynomials over $\mathbb{Q}$ and $h(\alpha) \neq 0$. The following theorem shows that $\mathbb{Q}(\alpha)$