is the Kronecker symbol ([82, Chapter 10.5]). Dirichlet proved the following formulas for the class number of quadratic fields:

$$h(\mathbb{K}) = \frac{L(1,\chi_{d_{\mathbb{K}}})\sqrt{|d_{\mathbb{K}}|}w_{\mathbb{K}}}{2\pi} \quad \text{for } d<0, \qquad h(\mathbb{K}) = \frac{L(1,\chi_{d_{\mathbb{K}}})\sqrt{d_{\mathbb{K}}}}{\ln\varepsilon} \quad \text{for } d>0,$$

where $h(\mathbb{K})$ is the class number, $\varepsilon = \frac{1}{2}(t + u\sqrt{u})$ for (t,u) the fundamental solution of Pell's equation $t^2 - du^2 = 4$ (ε is either the fundamental unit or the square of the fundamental unit of $\mathbb{K}$), and $w_{\mathbb{K}}$ is the number of roots of unity in $\mathbb{K}$, i.e. $w_{\mathbb{K}} = 4$ if $d_{\mathbb{K}} = -4$, $w_{\mathbb{K}} = 6$ if $d_{\mathbb{K}} = -3$, and $w_{\mathbb{K}} = 2$ otherwise (see [54, Chapter 7.4.5], [176, Chapter 11]). Let us also mention that the function $P(s) = \prod_{\chi \bmod k} L(s,\chi)$ from the proof of Dirichlet's theorem on primes in arithmetic progression is in close connection to the Dedekind zeta function of the *cyclotomic field* $\mathbb{Q}(e^{2i\pi/k})$ (see [82, Chapter 10.5]).

12.6 Exercises

1. Find all units of the quadratic fields $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{5})$.

2. Prove that $1+i$ is prime in $\mathbb{Q}(i)$.

3. Using the fact that $\mathbb{Q}(i)$ has the property of unique factorization, from $(x+iy)(x-iy) = z^2$, derive the formulas for the Pythagorean triples.

4. Explain why two factorizations of the number 13 in the field $\mathbb{Q}(\sqrt{-3})$:

$$13 = \frac{7+\sqrt{-3}}{2}\cdot\frac{7-\sqrt{-3}}{2} = (1+2\sqrt{-3})(1-2\sqrt{-3})$$

   are not contradictory to the fact that the field $\mathbb{Q}(\sqrt{-3})$ has the unique factorization property.

5. Prove that $\mathbb{Q}(\sqrt{3}, \sqrt[3]{2}) = \mathbb{Q}(\sqrt{3} + \sqrt[3]{2})$.

6. Find the minimal polynomials of the algebraic numbers $1+\sqrt{2}$, $1+\sqrt{2}+\sqrt{3}$, $\sqrt[3]{7}$ and $(1+\sqrt[3]{7})/2$.

7. Which of the numbers from the previous exercise are algebraic integers?

8. If α is an algebraic number of degree n, prove that $\alpha - 1$ is also an algebraic number of degree n.

9. Let $\alpha = \alpha_1 + i\alpha_2$, where $\alpha_1, \alpha_2 \in \mathbb{R}$, be an algebraic integer. Do α_1 and α_2 have to be algebraic integers?

10. Find $\alpha \in \mathbb{Q}(i)$ such that $N(\alpha) \in \mathbb{Z}$, but α is not an algebraic integer.

11. Prove that the set of all real algebraic numbers forms a field and that the set of all real algebraic integers forms a ring.

12. Let $\mathbb{K}$ be an algebraic number field of degree n and let d be its discriminant. Prove that $d \equiv 0$ or $1 \pmod 4$.

13. Let p be a prime number, ζ a primitive p-th root of unity and $\mathbb{K} = \mathbb{Q}(\zeta)$. Prove that $\{1, \zeta, \dots, \zeta^{p-1}\}$ is an integral basis of $\mathbb{K}$.

14. Let $\mathbb{K} = \mathbb{Q}(\theta)$, where $\theta^3 - \theta^2 - 2\theta - 8 = 0$. Prove that $\mathbb{K}$ does not have a power integral basis and that $\{1, \theta, (\theta^2 + \theta)/2\}$ is one integral basis of $\mathbb{K}$.

15. Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals. Prove that $\mathfrak{a} + \mathfrak{b}$ is an ideal.

16. Let $\mathfrak{a}$, $\mathfrak{b}$ and $\mathfrak{c}$ be ideals. Prove that $\mathfrak{a}(\mathfrak{b} + \mathfrak{c}) = \mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c}$.

17. Prove that the ideal $\langle 2, x \rangle$ is not a principal ideal in the ring $\mathbb{Z}[x]$.

18. Prove that in the ring $\mathbb{C}[x, y]$ of polynomials in two variables with complex coefficients, the ideal $\langle x, y \rangle$, which contains all polynomials from $\mathbb{C}[x, y]$ with the free coefficient equal to 0, is not a principal ideal. The rings $\mathbb{Z}[x]$ and $\mathbb{C}[x, y]$ are examples of unique factorization domains (and also the so-called *Noetherian rings* – the rings in which each increasing sequence of ideals is stationary; see [9, Chapter 3], [397, Chapter 9]) which are not principal ideal domains.

19. Express the ideal $\langle 51 - 5i, 43 + 7i \rangle$ in $\mathbb{Q}(i)$ as a principal ideal.

20. Suppose that the principal ideals $\langle \alpha \rangle$ and $\langle \beta \rangle$ are equal. Prove that there is a unit ε such that $\alpha = \varepsilon\beta$.

21. Prove that the roots of unity in an algebraic number field $\mathbb{K}$ form a cyclic group.

22. Prove that $\varepsilon = 1 + \sqrt[3]{2} + \sqrt[3]{4}$ is a unit in the field $\mathbb{Q}(\sqrt[3]{2})$.

23. Determine the fundamental unit of the field $\mathbb{Q}(\sqrt[3]{7})$.

24. Factorize the numbers 2 and 3 into prime elements in the field $\mathbb{K} = \mathbb{Q}(\sqrt{-23})$. Let $\omega = (1 + \sqrt{-23})/2$. Prove that

$$\langle 2, w\rangle\langle 3, w\rangle = \langle w\rangle.$$

25. Compute the class numbers of $\mathbb{Q}(\sqrt{-23})$ and $\mathbb{Q}(\sqrt{-31})$.

26. Compute the class numbers of $\mathbb{Q}(\sqrt{6})$ and $\mathbb{Q}(\sqrt{14})$.

27. Let p be a prime number and $p \equiv 11 \pmod{12}$. If $p > 3^n$, prove that the ideal class group of $\mathbb{Q}(\sqrt{-p})$ has an element whose order is greater than n.