GALOIS THEORY THROUGH EXERCISES

Juliusz Brzezinski

Contents

1

Solving algebraic equations

An **algebraic equation** of **degree** n with complex coefficients is an equation:

$$f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n = 0,$$

where $a_i \in \mathbb{C}$, $n \geq 0$ and $a_0 \neq 0$ (if $n = 0$, $f(X)$ is a **constant polynomial**). According to the Fundamental theorem of algebra (proved by C.F. Gauss[1] in 1799), if $f(X)$ is non-constant polynomial, then the equation $f(X) = 0$ has n complex solutions (roots) $x_1, \ldots, x_n$ and $f(X) = a_0(X - x_1)\cdots(X - x_n)$. Some of the x_i may be equal and the number of occurrences of x_i as a root of $f(X) = 0$ is called its **multiplicity**.

One of the main mathematical problems before 18th century was to express solutions of algebraic equations through their coefficients using the four arithmetical operations (addition, subtraction, multiplication, division) and radicals. Such possibility was known for $n = 1, 2$ since antiquity, and for $n = 3, 4$ since 15th century. Finding similar expressions for equations of degree 5 was an unachievable task. The idea that such formulae may not exist was a motivation for the works of many mathematicians during 18th century and finally lead to the results, which are a part of the theory developed by Évariste Galois in the beginning of 19th century.

In this chapter, we look at some methods of solving the equations when general formulae exist. We can always assume that $a_0 = 1$ (if not, divide both sides of the equation by $a_0 \neq 0$). We recall how to solve quadratic equations and afterwards discuss the cases of cubic and quartic equations.

[1] Johann Carl Friedrich Gauss (1777 – 1855) was a German mathematician – one of the most prominent in the history of the subject. He left very important contributions in many parts of mathematics and many other natural sciences including number theory, algebra, statistics, analysis, differential geometry, geodesy, geophysics, mechanics, electrostatics, astronomy and optics.

1.1 Quadratic equations. A quadratic equation $f(X) = 0$ has 2 roots x_1, x_2 and $f(X) = a_0X^2 + a_1X + a_2 = a_0(X - x_1)(X - x_2)$. Comparing the coefficients on the left and right in this equality, we get the **Vieta formulae**[2]:

$$\begin{aligned} x_1 + x_2 &= -\frac{a_1}{a_0} \\ x_1x_2 &= \frac{a_2}{a_0} \end{aligned}$$

Denoting $\frac{a_1}{a_0} = p$ and $\frac{a_2}{a_0} = q$, we get an equivalent equation:

$$X^2 + pX + q = 0$$

and solve it by transforming to an equation with roots $x_i + \frac{p}{2}$ whose sum is 0, that is, replacing the equation above by the equivalent expression in which $X^2 + pX$ is completed to a square:

$$\left(X + \frac{p}{2}\right)^2 + \left(q - \frac{p^2}{4}\right) = 0.$$

Solving, we get the two solutions:

$$x_1 = -\frac{p}{2} - \sqrt{\frac{p^2}{4} - q} \quad \text{and} \quad x_2 = -\frac{p}{2} + \sqrt{\frac{p^2}{4} - q}.$$

The number $\Delta = p^2 - 4q = (x_1 + x_2)^2 - 4x_1x_2 = (x_1 - x_2)^2$ is called the **discriminant** of the polynomial $X^2 + pX + q$ (see p. 258). It is non-zero if and only if the roots x_1, x_2 are different.

1.2 Cubic equations. A cubic equation $f(X) = 0$ has 3 roots x_1, x_2, x_3 and $f(X) = a_0X^3 + a_1X^2 + a_2X + a_3 = a_0(X - x_1)(X - x_2)(X - x_3)$. Comparing the coefficients on the left and right in this equality, we get the Vieta formulae:

$$\begin{aligned} x_1 + x_2 + x_3 &= -\frac{a_1}{a_0}, \\ x_1x_2 + x_2x_3 + x_1x_3 &= \frac{a_2}{a_0}, \\ x_1x_2x_3 &= -\frac{a_3}{a_0}, \end{aligned} \tag{1.1}$$

[2] Franciscus Vieta, in Franch François Viète, (1540–1603) was a Franch mathematician who introduced modern notation in connection with algebraic equations.

The equation having the roots $x_i + \frac{a_1}{3a_0}$, where $i = 1, 2, 3$, has the coefficient of x^2 equal to 0, since the sum of these 3 numbers is zero. Technically, we get such an equation substituting $X = Y - \frac{a_1}{3a_0}$ in the given cubic equation:

$$a_0X^3 + a_1X^2 + a_2X + a_3 =$$

$$a_0\left(Y - \frac{a_1}{3a_0}\right)^3 + a_1\left(Y - \frac{a_1}{3a_0}\right)^2 + a_2\left(Y - \frac{a_1}{3a_0}\right) + a_3 = a_0(Y^3 + pY + q)$$

where p and q are easily computable coefficients (it is not necessary to remember these formulae, since it is easier to remember the substitution and to transform each time, when it is necessary). Thus we can start with an equation:

$$X^3 + pX + q = 0. \tag{1.2}$$

We compare the last equality with the well-known identity:

$$(a + b)^3 - 3ab(a + b) - (a^3 + b^3) = 0 \tag{1.3}$$

and choose a, b in such a way that:

$$\begin{aligned} p &= -3ab, \\ q &= -(a^3 + b^3). \end{aligned} \tag{1.4}$$

If a, b are so chosen, then evidently $x = a + b$ is a solution of the equation (1.2). Since

$$\begin{aligned} a^3 + b^3 &= -q, \\ a^3b^3 &= -\frac{p^3}{27}, \end{aligned}$$

a^3, b^3 are solutions of the quadratic equation:

$$t^2 + qt - \frac{p^3}{27} = 0.$$

Solving this equation gives a^3, b^3. Then we choose a, b, which satisfy (1.4) and get $x = a+b$. An (impressing) formula, which hardly needs to be memorized (it is easier to start "from the beginning", that is, from the identity (1.3), than to remember it) is thus the following:

$$x_1 = a + b = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \tag{1.5}$$

We leave a discussion of different choices of signs of the roots to exercises, but notice that in order to solve a cubic equation, it is sufficient to find one root x_1 and solve a quadratic equation after dividing the cubic by $x - x_1$. The above expression (in different notations) was first published by Gerolamo Cardano[3] in his book "Ars Magna" in 1545 and is known today as Cardano's formula. However, the history surrounding the formula is very involved and several Italian mathematicians knew the method before Cardano (notably, Scipione del Ferro, Antonio Fiore and Niccoló Tartaglia about 20 years earlier that the appearance of Cardano's book).

The **discriminant** of the cubic (1.2) is $\Delta = -(4p^3 + 27q^2) = [(x_1 - x_2)(x_2 - x_3)(x_3 - x_1)]^2$. See p. 258 and Ex. 1.3 below.

1.3 Quartic equations. Such an equation $f(X) = a_0X^4 + a_1X^3 + a_2X^2 + a_3X + a_4 = a_0(x - x_1)(X - x_2)(X - x_3)(X - x_4)$ has 4 roots x_1, x_2, x_3, x_4. Similarly as for quadratic and cubic equations, we can write down the Vieta formulae expressing relations between the roots and the coefficients of the equation (we leave it as an exercise). Solving a quartic equation (we assume $a_0 = 1$ and denote the remaining coefficients avoiding indices):

$$X^4 + mX^3 + pX^2 + qX + r = 0, \tag{1.6}$$

it is not important to assume that $m = 0$ (but it could be achieved substituting $X - \frac{m}{4}$ instead of X similarly as in the quadratic and cubic cases). We simply complement $X^4 + mX^3$ in such a way that we get a square of a quadratic polynomial and when it is done, we find a parameter λ so that the quadratic polynomial in square brackets

$$\left(X^2 + \frac{m}{2}X + \frac{\lambda}{2}\right)^2 - \left[\left(\frac{m^2}{4} + \lambda - p\right)X^2 + \left(\frac{m\lambda}{2} - q\right)X + \left(\frac{\lambda^2}{4} - r\right)\right] = 0 \tag{1.7}$$

is a square of a first degree polynomial. This is achieved when the discriminant of the quadratic polynomial in the square bracket equals 0 (see Ex. 1.8), that is,

$$\left(\frac{m\lambda}{2} - q\right)^2 - 4\left(\frac{m^2}{4} + \lambda - p\right)\left(\frac{\lambda^2}{4} - r\right) = 0 \tag{1.8}$$

This is a cubic equation with respect to λ. Solving it, we get a root λ, which gives a possibility to factorize the quartic polynomial (1.7) into a product of two quadratic polynomials and

[3] Girolamo Cardano (1501 – 1576) was an Italian mathematician and physicists. He is also known as a technical inventor.

then solve two quadratic equations. The method described above was given by L. Ferrari[4] in the middle of 16th century and published in Cardano's book mentioned above.

As we noted before, many attempts to solve quintics (that is, fifth degree polynomial equations) were fruitless. Already during 18th century some mathematicians suspected that similar formulae as for equations of degrees less than 5 are impossible. It is not too difficult to see that the situation with the equations of degree 5 differs from the situation in the case of equations of lower degree (see Ex. 1.6). J.L. Lagrange[5] was the first mathematician who tried to prove that there are no algebraic formulae for solutions of the general fifth degree algebraic equations. His thorough analysis of polynomial equations and their solutions led him to a notion of resolvent, which was later used by Galois and found broader applications in the modern numerical applications related to computations of Galois groups. The final proof that it is is impossible to express a solutions of general quintic equations using the four arithmetical operations (addition, subtraction, multiplication, division) and extracting roots applied to the coefficients of the equation was proved by Abel[6] in 1823 (earlier an incomplete proof was published by Ruffini[7] in 1799). Galois gave an independent proof of the same result using different methods, which we follow in Chapter 13.

EXERCISES 1

1.1. Solve the following equations using Cardano's or Ferrari's methods:

(a) $X^3 - 6X + 9 = 0$;
(b) $X^3 + 9\,X^2 + 18\,X + 28 = 0$;
(c) $X^3 + 3X^2 - 6X + 4 = 0$;
(d) $X^3 + 6X + 2 = 0$;
(e) $X^4 - 2X^3 + 2X^2 + 4X - 8 = 0$;
(f) $X^4 - 3X^3 + X^2 + 4X - 6 = 0$;
(g) $X^4 - 2X^3 + X^2 + 2X - 1 = 0$;
(h) $X^4 - 4X^3 - 20X^2 - 8X + 4 = 0$.

1.2. Show that the system (1.4) has exactly three solutions (a, b) and find all three solutions of the equation $X^3 + pX + q = 0$ following the discussion above concerning Cardano's formula.

1.3. (a) Using Vieta's formulae (1.1) show that the discriminant $\Delta(f) = [(x_1 - x_2)(x_2 - x_3)(x_3 - x_1)]^2$ of $f(X) = X^3 + pX + q$ is equal to $\Delta(f) = -(4p^3 + 27q^2)$ (x_1, x_2, x_3 denote the zeros of $f(X)$). Note that the equation $X^3 + pX + q = 0$ has multiple roots if and only if $\Delta = 0$.

[4] Lodovico Ferrari (1522-1565) was an Italian mathematician who was a servant, later a student and finally a successor of G. Cardano at the Universisty of Pavia.

[5] Joseph-Louis Lagrange (1736-1813) was an Italian mathematician, who mostly worked in France. His contributions to the theory of algebraic equations are very important as well as his contributions in many other fields of mathematics, physics and astronomy.

[6] Nils Henrik Abel (1801–1829) was a Norwegian mathematician who first proved that the general quintic equation is impossible to solve by purely algebraic means.

[7] Paulo Ruffini (1765 – 1822) was an Italian mathematician and physician.

(b) Assume that p, q are real numbers. Show that the equation $f(X) = X^3 + pX + q = 0$ has 3 different real roots if and only if $\Delta(f) > 0$.

1.4. The discriminant of the polynomial $X^3 - 6X + 4$ equals $\Delta = 432$, so the equation $X^3 - 6X + 4 = 0$ has three different real roots (see Ex. 1.3). The formula (1.5) gives

$$x_1 = \sqrt[3]{-2 + 2i} + \sqrt[3]{-2 - 2i}.$$

Find the solutions of the equation without using Cardano's formula and identify these solutions with the expressions given by Cardano's formula.

Remark. The case of the cubic polynomials having 3 real roots in the context of Cardano's formula was a serious problem for mathematicians during at least 300 years. As $\Delta = -(4p^3 + 27q^2) > 0$, we have $\frac{q^2}{4} + \frac{p^3}{27} < 0$ in the formulae (1.5), so in order to compute the real number x_1, we have to manipulate with complex numbers on the right hand side. The Cardano's formulae were considered as "not correct" as the real values (even integer values) of the roots are expressed through the complex numbers which were considered with great suspicion. Mathematician tried to find "better" formulae in which negative numbers under square roots do not appear in order to eliminate what was known as **"Casus Irreducibilis"**. First during the 19th century it became clear that it is impossible to find "better" formulae – in general, it is impossible to express the real roots of a cubic with 3 real roots by so called real radicals, that is, without help of complex numbers. We explain this phenomenon closer in Chapter 13.

1.5. Assume that a cubic equation $X^3 + pX + q = 0$ has 3 real solutions, that is, $\Delta = -(4p^3 + 27q^2) > 0$. Show that there exists $r \in \mathbb{R}$ and $\varphi \in [0, 2\pi]$ such that the solutions of the cubic equation are

$$x_1 = 2\sqrt[3]{r}\cos\frac{\varphi}{3}, \qquad x_2 = 2\sqrt[3]{r}\cos\frac{\varphi + 2\pi}{3}, \qquad x_3 = 2\sqrt[3]{r}\cos\frac{\varphi + 4\pi}{3}.$$

1.6. (a) Find a cubic equation having a solution $\alpha = \sqrt[3]{a + \sqrt{b}} + \sqrt[3]{a - \sqrt{b}}$, where $a^2 - b = c^3$ and $a, b, c \in \mathbb{Q}$. Write down all solutions of the equation you have found and motivate that a solution to any cubic equation $x^3 + px + q = 0$, where p, q are rational numbers, can be written as α above.

(b) Find a quintic equation (that is, an equation of degree 5) having a solution $\alpha = \sqrt[5]{a + \sqrt{b}} + \sqrt[5]{a - \sqrt{b}}$, where $a^2 - b = c^5$ and $a, b, c \in \mathbb{Q}$. Choose a, b in such a way that the polynomial having α as its zero is irreducible over $\mathbb{Q}$. Can every quintic equation with rational coefficients be solved by a number given as α above?

Remark. The quintic equation, whose one of the zeros is α in (b) above (see it on p. 136), is sometimes called **de Moivre's quintic**. Of course, we have a formula giving a solution of such an equation, since we construct it starting from a solution. But our objective is to prove that there are cases when for a quintic equations with rational coefficients it is

impossible to express a solution using the four arithmetical operations (addition, subtraction, multiplication, division) and extracting roots applied to the coefficients of the equation. Here we have an example that sometimes it is possible even if the polynomial can not be factored (over the rational numbers) into a product of polynomials of degrees less than 5. In fact, there are less complicated examples which exemplify this statement like $X^5 - 2$, but compering (a) and (b) gives an idea what can make a difference that there exists a formula for a general cubic equation, while there is no such a formula for general quintic equations.

1.7. Solve the binomial equation $X^n - a = 0$ of degree $n > 0$, where $a \in \mathbb{C}$.

1.8. Show that a given trinomial $aX^2+bX+c \in \mathbb{C}[X]$ is a square of a binomial $pX+q \in \mathbb{C}[X]$ if and only if the discriminant of the trinomial $b^2 - 4ac = 0$.

USING COMPUTERS 1

Maple gives a possibility to find solutions of equations of low degrees in closed form (expressed by arithmetical operations on coefficients and using radicals). Thus all equations of degree at most 4 and some other simple equations (like the equations $f(X^n) = 0$ when f has degree at most 3) can be solved. The solutions are obtained by:

```
>solve(f(X))
```

in order to solve the equation $f(X) = 0$. The numerical real values of zeros can be obtained using `>fsolve(f(X))` and all values by `>fsolve(f(X),complex)`. Of course, you can use these commands in order to find the zeros of the equations, for example, in Ex. 1.1, but the intention in this section is rather to get some experience and feeling of raw computations before the computer era. Nevertheless, if you want to get exact values of all zeros (when such values are possible to give and the suitable procedures are implemented), then it is possible to use the command `>solve` as above or the following commands, which give a greater flexibility already for polynomials of degree 4 and which we explain through an example (see Ex. 1.1(h)):

```
>alias(a=RootOf(X^4-4*X^3-20*X^2-8*X+4))
```

$$a$$

```
>allvalues(a)
```

$$1+\sqrt{7}-\sqrt{6+2\sqrt{7}},\ 1+\sqrt{7}+\sqrt{6+2\sqrt{7}},\ 1-\sqrt{7}+\sqrt{6-2\sqrt{7}},\ 1-\sqrt{7}-\sqrt{6-2\sqrt{7}}$$

Notice that the command `alias(a=RootOf(f(X)))` defines one of the zeros of $f(X)$. Asking `allvalues(a)`, we get all possible values. If we want to identify the value denoted by a, we

can compere it with all possible values. So for example `allvalues(a)[1]` gives the first one and we can consider the difference of it with a defined by `alias(a=RootOf(f(X)))`. If it is 0, then a denotes just this value.

It is also possible to get the discriminants of the polynomials (see p. 258) pointing the variable with respect to which the discriminant should be computed:

```
> discrim(X^3+pX+q, X);
```

$$-4p^3 - 27q^2$$

but it may be instructive to try to get this result without use of a computer (see Ex. 1.3 and its solution).

2

Field extensions

A short introduction to groups, rings and fields is presented in the Appendix. Here we only recall some notations, which play an important role in this chapter. If a field K is a subfield of a field L, then we say that $K \subseteq L$ is a **field extension**. If K_i, $i \in I$ (I an index set) are subfields of L, then the intersection $\cap K_i$, $i \in I$, is also a subfield of L. If $L \supseteq K$ and X is a subset of L, then $K(X)$ denotes the intersections of all subfields of L, which contain both K and X ($K(X)$ is the least subfield of L containing both K and X). If $X = \{\alpha_1, \ldots, \alpha_n\}$, then we usually write $K(X) = K(\alpha_1, \ldots, \alpha_n)$. If $X = K'$ is a subfield of L, then $K(K')$ is denoted by KK' and called the **compositum** of K and K'. Every field is an extension of the smallest field contained in it – the intersection of all its subfields. Such an intersection does not contain any smaller fields. A field without any smaller subfields (one says often **proper subfields**) is called a **prime field**.

The rational numbers is the only infinite prime field (up to isomorphism of fields). For every prime number p, there is a finite prime field $\mathbb{F}_p$ consisting of the residues $0, 1, \ldots, p-1$ of the integers $\mathbb{Z}$ modulo p, which are added and multiplied modulo p (the field $\mathbb{F}_p$ is the quotient of $\mathbb{Z}$ modulo the ideal generated by the prime number p – see **A.4** for more details).

By the **characteristic** of a field K, we mean the number 0 if the prime subfield of K is infinite and the number of elements in the prime subfield of K if it is finite. The characteristic of K is denoted by $\mathrm{char}(K)$.

T. 2.1 (*a*) *The characteristic of a field is* 0 *or a prime number.*

(*b*) *Any field K of characteristic* 0 *contains a unique subfield isomorphic to the rational numbers $\mathbb{Q}$ and any field of characteristic p contains a unique subfield isomorphic to $\mathbb{F}_p$.*

EXERCISES 2

2.1. Which of the following subsets of $\mathbb{C}$ are fields with respect to the usual addition and multiplication of numbers:

(a) $\mathbb{Z}$;
(b) $\{0, 1\}$;
(c) $\{0\}$;
(d) $\{a + b\sqrt{2},\ a, b \in \mathbb{Q}\}$;
(e) $\{a + b\sqrt[3]{2},\ a, b \in \mathbb{Q}\}$;
(f) $\{a + b\sqrt[4]{2}, a, b \in \mathbb{Q}\}$;
(g) $\{a + b\sqrt{2},\ a, b \in \mathbb{Z}\}$;
(h) $\{z \in \mathbb{C} : |z| \leq 1\}$.

2.2. Show that every subfield of $\mathbb{C}$ contains $\mathbb{Q}$.

2.3. Give an example of an infinite field of characteristic $\neq 0$.

2.4. Show that the characteristic of a field K is the least natural number $n > 0$ such that $na = 0$ for each $a \in K$ or it is 0 if such n does not exist.

2.5. (a) Let $L \supseteq K$ be a field extension and let $\alpha \in L \setminus K$, $\alpha^2 \in K$. Show that

$$K(\alpha) = \{a + b\alpha,\ \text{where}\ \ a, b \in K\}.$$

(b) Let $K(\sqrt{a})$ and $K(\sqrt{b})$, where $a, b \in K, ab \neq 0$, be two field extensions of K. Show that $K(\sqrt{a}) = K(\sqrt{b})$ if and only if ab is a square in K (that is, there is $c \in K$ such that $ab = c^2$).

2.6. Give a description of all numbers belonging to the fields:

(a) $\mathbb{Q}(\sqrt{2})$; (b) $\mathbb{Q}(i)$; (c) $\mathbb{Q}(\sqrt{2}, i)$; (d) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

2.7. Show that

(a) $\mathbb{Q}(\sqrt{5}, i\sqrt{5}) = \mathbb{Q}(i, \sqrt{5})$;
(b) $\mathbb{Q}(\sqrt{2}, \sqrt{6}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$;
(c) $\mathbb{Q}(\sqrt{5}, \sqrt{7}) = \mathbb{Q}(\sqrt{5} + \sqrt{7})$;
(d) $\mathbb{Q}(\sqrt{a}, \sqrt{b}) = \mathbb{Q}(\sqrt{a} + \sqrt{b})$, when $a, b \in \mathbb{Q}$, $\sqrt{a} + \sqrt{b} \neq 0$.

2.8. Give a description of the following subfields of $\mathbb{C}$:

(a) $\mathbb{Q}(X)$, where $X = \{\sqrt{2},\ 1 + 2\sqrt{8}\}$;
(b) $\mathbb{Q}(i)(X)$, where $X = \{\sqrt{2}\}$;
(c) K_1K_2, where $K_1 = \mathbb{Q}(i)$, $K_2 = \mathbb{Q}(\sqrt{5})$;
(d) $\mathbb{Q}(X)$, where $X = \{z \in \mathbb{C} : z^4 = 1\}$.

2.9. Let K be a field.

(a) Show that all the matrices $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, where $a, b \in K$, form a field L with respect to matrix addition and matrix multiplication if and only if the equation $X^2 + 1 = 0$ has not solutions in K.

(b) Show that L contains a field isomorphic to K.

(c) Use (a) in order to construct a field with 9 elements and find its characteristic.

Remark. We discuss finite fields in Chapter 5, where general construction of finite fields is given.

2.10. Let K be a field

(a) Formulate a suitable condition such that all matrices $\begin{bmatrix} a & b \\ -b & a-b \end{bmatrix}$, $a, b \in K$, form a field with respect to the matrix addition and multiplication.

(b) Use (a) in order to construct a field with 4 elements and write down the addition and the multiplication tables for the elements in this field.

2.11. In a field K the equality $a^4 = a$ is satisfied for all $a \in K$. Find the characteristic of the field K.

2.12. Let K be a field of characteristic p.

(a) Show that $(a+b)^{p^m} = a^{p^m} + b^{p^m}$ when $a, b \in K$ and m is a natural number.

(b) Let p divide a positive integer n. Show that $a^n + b^n = (a^{\frac{n}{p}} + b^{\frac{n}{p}})^p$ when $a, b \in K$.

(c) Define $\varphi : K \to K$ such that $\varphi(x) = x^p$. Show that the image of φ, which we denote by K^p, is a subfield of K.

2.13. Let $K \subseteq L$ be a field extension and let M_1, M_2 be two fields containing K and contained in L.

(a) Motivate that M_1M_2 consists of all quotients of finite sums $\sum \alpha_i\beta_i$, where $\alpha_i \in M_1$ and $\beta_i \in M_2$.

(b) Motivate that for each $x \in M_1M_2$ there are $\alpha_1, \ldots, \alpha_m \in M_1$ and $\beta_1, \ldots, \beta_n \in M_2$ such that $x \in K(\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n)$.

2.14. Let K be a field of characteristic p. Show that for any $a \in K$, the polynomial $f(X) = X^p - X + a$ has p zeros in K or no zeros in K (H137).

3

Polynomials and irreducibility

In this chapter, we gather a few facts concerning zeros of polynomials and discuss some simple metods helping to decide whether a polynomial is irreducible or reducible. In many practical situations, this information is very essential for studies of field extensions. A short presentation of polynomial rings can be found in the Appendix (see **A.6**).

Let K be a field and let $f(X) = a_n X^n + \cdots + a_1 X + a_0$ be a polynomial with coefficients $a_i \in K$. When $a_n \neq 0$, then n is called the degree of $f(X)$ and is denoted by $\deg f$. The zero polynomial is the one with all coefficients equal to 0. Its degree is usually not defined, but sometimes it is defined as 1 or ∞. For practical reasons, we shall assume that the degree of the zero polynomial is 1.

If L is a field containing K, then we say that $\alpha \in L$ is a zero of $f \in K[X]$ if $f(\alpha) = 0$.

T. 3.1 Factor Theorem. *Let $K \subseteq L$ be a field extension.*

(a) The remainder of $f \in K[X]$ divided by $X - a$, $a \in L$, is equal $f(a)$;

(b) An element $a \in L$ is a zero of $f \in K[X]$ if and only if $X - a | f(X)$ (in $L[X]$).

A polynomial $f \in K[X]$ is **reducible** (in $K[X]$ or over K) if $f = gh$, where $g, h \in K[X]$, $\deg g \geq 1$ and $\deg h \geq 1$. A non-constant polynomial which is not reducible is called **irreducible**. Of course, every polynomial of degree 1 is irreducible.

In the polynomial rings over fields, every non constant polynomial is a product of irreducible factors and such a product is unique in the following sense:

T. 3.2 *Let K be a field. Every polynomial of degree degree ≥ 1 in $K[X]$ is a product of irreducible polynomials . If*

$$f = p_1 \dots p_k = p'_1 \dots p'_l,$$

where p_i and p'_i are irreducible polynomials, then $k = l$ and with suitable numbering of the factors p_i, p'_j, we have $p'_i = c_i p_i$, where $c_i \in K$.

We gather a few facts about irreducible polynomials in different rings. More detailed information is given in the exercises.

In the ring $\mathbb{C}[X]$, the only irreducible polynomials are exactly the polynomials of degree 1. This is the content of the **Fundamental Theorem of (polynomial) Algebra**, which was the first time proved by C.F. Gauss in 1799: If $f(X) \in \mathbb{C}[X]$, then $f(X) = c(X-z_1)\dots(X-z_n)$, where n is the degree of the polynomial $f(X)$, $c \in \mathbb{C}$ and $z_i \in \mathbb{C}$ are all its zeros (with suitable multiplicities).

In the ring $\mathbb{R}[X]$ all irreducible polynomials are of degree 1 and the polynomials of degree 2 of the shape $c(X^2+pX+q)$ such that $\Delta = p^2-4q < 0$ and $c \in \mathbb{R}, c \neq 0$. This follows easily from the description of the irreducible polynomials in $\mathbb{C}[X]$ (see Ex. 3.5).

In the ring $\mathbb{Q}[X]$ of the polynomials with rational coefficients, there are irreducible polynomials of arbitrary degrees. For example, the polynomials $X^n - 2$ are irreducible for every $n \geq 1$ (see Ex. 3.7). In order to prove that a polynomial with integer coefficients is irreducible in $\mathbb{Q}[X]$ (which is a frequent situations in many exercises in Galois Theory), it is convenient to study the irreducibility of this polynomial in $\mathbb{Z}[X]$ in combination with Gauss's Lemma or reductions of the polynomial modulo suitable prime numbers (see Ex. 3.8).

T. 3.3 Gauss's Lemma. *A nonconstant polynomial with integer coefficients is reducible in $\mathbb{Z}[X]$ if and only if it is reducible in $\mathbb{Q}[X]$. More exactly, if $f \in \mathbb{Z}[X]$ and $f = gh$, where $g, h \in \mathbb{Q}[X]$, then there are rational numbers r, s such that $rg, sh \in \mathbb{Z}[X]$ and $rs = 1$, so $f = (rg)(sh)$.*

Remark. Gauss's Lemma is true for every principal ideal domain R and its quotient field K instead of $\mathbb{Z}$ and $\mathbb{Q}$. The proof of this more general version is essentially the same as the proof of the above version on p. 93.

If $f(X) = a_nX^n + \dots + a_1X + a_0$ is a polynomial with integer coefficients a_i for $i = 0, 1, \dots, n$, then its **reductions modulo a prime number** p is the polynomial $\bar{f}(X) = \bar{a}_nX^n + \dots + \bar{a}_1X + \bar{a}_0$ whose coefficients are the residues of a_i modulo p. We denote the reduction modulo p by $f(X) \pmod p$. The reduction modulo p is a ring homomorphism of the polynomial ring $\mathbb{Z}[X]$ onto the polynomial ring $\mathbb{F}_p[X]$ (compare the text on reduction modulo a ring homomorphism on p. 77).

EXERCISES 3

3.1. (a) Show that a polynomial $f \in K[X]$ of degree 2 or 3 is reducible in $K[X]$ if and only if f has a zero in K, that is, there is $x_0 \in K$ such that $f(x_0) = 0$.

(b) Show that the polynomial $X^4 + 4$ over the rational numbers $\mathbb{Q}$, has no rational zeros, but is reducible in $\mathbb{Q}[X]$ (notice that $\mathbb{Q}$ may be replaced by $\mathbb{R}$).

3.2. Make a list of all irreducible polynomials of degrees 1 to 5 over the field $\mathbb{F}_2$ with 2 elements.

3.3. Show that if a rational number $\frac{p}{q}$, where p, q are relatively prime integers, is a solution of an equation $a_n X^n + \cdots + a_1 X + a_0 = 0$ with integer coefficients a_i, $i = 0, 1, \ldots, n$, then $p|a_0$ and $q|a_n$.

3.4. Factorize the following polynomials as a product of irreducible ones:

(a) $X^4 + 64$ in $\mathbb{Q}[X]$; (e) $X^3 - 2$ in $\mathbb{Q}[X]$;
(b) $X^4 + 1$ in $\mathbb{R}[X]$; (f) $X^6 + 27$ in $\mathbb{R}[X]$;
(c) $X^7 + 1$ in $\mathbb{F}_2[X]$; (g) $X^3 + 2$ in $\mathbb{F}_3[X]$;
(d) $X^4 + 2$ in $\mathbb{F}_5[X]$; (h) $X^4 + X + 2$ in $\mathbb{F}_3[X]$.

3.5. (a) Show that if a real polynomial $f(X) \in \mathbb{R}[X]$ has a complex zero z, then also the conjugated number $\bar{z}$ is a zero of $f(X)$.

(b) Show that a real polynomial of degree at least 1 is a product of irreducible polynomials of degrees 1 or 2.

3.6. Using Gauss's Lemma show that the following polynomials are irreducible in $\mathbb{Q}[X]$:

(a) $X^4 + 1$; (b) $X^4 - 10X^2 + 1$; (c) $X^4 - 4\,X^3 + 12\,X^2 - 16\,X + 8$.

Remark. The polynomials (a)–(c) are chosen in such a way that any reduction of them modulo a prime number gives a reducible polynomial over $\mathbb{F}_p$. Se Ex. 5.12.

3.7. (a) Prove **Eisentein's criterion**: Let $f(X) = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$ and let p be a prime number such that $p|a_0, p|a_1, \ldots, p|a_{n-1}, p \nmid a_n$ and $p^2 \nmid a_0$. Show that $f(X)$ is irreducible in $\mathbb{Z}[X]$.

(b) Show that the polynomials $X^n - 2$ for $n = 1, 2, \ldots$ are irreducible over $\mathbb{Q}$.

(c) Show that the polynomial $f(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + \cdots + X + 1$ is irreducible over $\mathbb{Q}$ for every prime number p.

3.8. (a) Show that if a reduction of a monic polynomial $f(X) \in \mathbb{Z}[X]$ modulo a prime number p is irreducible as a polynomial in $\mathbb{F}_p[X]$, then $f(X)$ is irreducible in $\mathbb{Q}[X]$.

(b) Show that if a monic polynomial $f(X) \in \mathbb{Z}[X]$ has reductions modulo two prime numbers p, q such that $f(X) \pmod p$ is a product of two irreducible factors of degrees d_{1p}, d_{2p} and $f(X) \pmod q$ is a product of two irreducible factors of degrees d_{1q}, d_{2q} and $\{d_{1p}, d_{2p}\} \neq \{d_{1q}, d_{2q}\}$, then $f(X)$ is irreducible in $\mathbb{Q}[X]$.

(c) Using (a) or (b) show that the following polynomials are irreducible in $\mathbb{Q}[X]$:

(c_1) $X^4 + X + 1$; (c_2) $X^5 + X^2 + 1$; (c_2) $X^4 + 3X + 4$;
(c_4) $X^5 + 3X + 1$; (c_5) $X^6 + 5X^2 + X + 1$; (c_6) $X^7 + X^4 + X^2 + 1$.

3.9. (a) Let $f(X) = X^4 + pX^2 + qX + r$ be a polynomial with coefficients in a field K. Show that $f(X) = (X^2 + aX + b)(X^2 + a'X + b')$, where a, b, a', b' are in a some field containing

K if and only if a^2 is a solution of the equation $r(f)(T) = T^3 + 2pT^2 + (p^2 - 4r)T - q^2 = 0$ called the **resolvent** of $f(X)$.

(b) Show that $f(X)$ in (a) is a product of two quadratic polynomials over K if and only if

$(*)$ $q \neq 0$ and the resolvent $r(f)$ has a zero, which is a square in K or

$(**)$ $q = 0$ and the resolvent $r(f)$ has two zeros, which are squares in K or $\delta = p^2 - 4r$ is a square in K.

3.10. Show that over every field there exists infinitely many irreducible polynomials.

3.11. Show that if a monic polynomial with rational coefficients divides a monic polynomial with integer coefficients, then has also integer coefficients.

USING COMPUTERS 3

An implementation of algorithms giving a possibility to factorize polynomials over the rational numbers $\mathbb{Q}$ or over finite fields $\mathbb{F}_p$ is usual in many program packages. In Maple, it is possible to construct finite field extensions of $\mathbb{Q}$ and $\mathbb{F}_p$ and factor polynomials over them, but we postpone our general discussion of field extensions to the next chapter. The command `>factor(f(X))` gives a possibility to factor a polynomial $f(X) \in \mathbb{Q}[X]$ over $\mathbb{Q}$ or to establish its irreducibility. If we want to know the same over the real or complex numbers, we can use `>factor(f(X),real)`, respectively `>factor(f(X),complex)`. The command `>irreduc(f(X))` gives `true` or `false` depending whether $f(X)$ is irreducible or not over the field of rational numbers. The same over the real numbers is achieved by `>irreduc(f(X),real)`.

The same thing over any finite field $\mathbb{F}_p$ is achieved by the command `>Factor(f(X)) mod p`. Observe the usage of the capital letter F in the last command. Over the finite fields $\mathbb{F}_p$, there is the command `>Irreduc(f(X)) mod p`. For example, the following command lists all quadratic irreducible polynomials over the field $\mathbb{F}_5$:

```
> for i from 0 to 4 do for j from 0 to 4 do if Irreduc(x^2+i*x+j) mod 5 = true
then print(x^2+i*x+j) fi od od
```

3.12. List all monic irreducible polynomials of degrees less than 4 over the field $\mathbb{F}_3$.

3.13. Verify the results of Ex. 3.1, 3.4 and 3.8 using Maple.

4

Algebraic extensions

Let $K \subseteq L$ be a field extension. We say that an element $\alpha \in L$ is **algebraic** over K if there is a non-zero polynomial $f \in K[X]$ such that $f(\alpha) = 0$. If such a polynomial does not exist, α is called **transcendental** over K. If $\alpha \in \mathbb{C}$ is algebraic over $\mathbb{Q}$, then we say that α is an **algebraic number**. A number $\alpha \in \mathbb{C}$, which is not algebraic is called **transcendental**. If $\alpha \in L$ is algebraic over K, then any non-zero polynomial of the least possible degree among all the polynomials $f \in K[X]$ such that $f(\alpha) = 0$ is called a **minimal polynomial** of α over K. The degree of f is called the **degree** of α over K.

T. 4.1 *Let $\alpha \in L \supseteq K$ be algebraic over K.*

(a) Any minimal polynomial of α over K is irreducible and divides every polynomial in $K[X]$ which has α as its zero.

(b) An irreducible polynomial $f \in K[X]$ such that $f(\alpha) = 0$ is a minimal polynomial of α over K.

(c) All minimal polynomials of α over K can be obtained by multiplying one of them by nonzero elements of K.

Using the last statement, we usually choose **the minimal polynomial**, which is the unique minimal polynomial whose highest coefficient equals 1. The degree of the minimal polynomial of α over K is called the **degree** of α over K. An extension $K(\alpha)$ of K is called **simple** and α is called its **generator**.

T. 4.2 Simple extension theorem. *(a) If $\alpha \in L \supseteq K$ is algebraic over K, then each element in $K(\alpha)$ can be uniquely represented as $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$, where $a_i \in K$ and n is the degree of the minimal polynomial of α over K. Thus $[K(\alpha) : K] = n$ and $1, \alpha, \ldots, \alpha^{n-1}$ is a basis of $K(\alpha)$ over K.*

(b) If $\alpha \in L \supseteq K$ is transcendental over K, then $K[\alpha] \simeq K[X]$, where $K[X]$ is the ring of polynomials over K.

If $L \supseteq K$ is a field extension, then L can be considered as a vector space over K. By the **degree** $[L : K]$, we mean the dimension of the linear space L over K. If this dimension is not finite, we write $[L : K] = \infty$. **T.4.2** says that $[K(\alpha) : K] = \deg(f)$ when α is algebraic and f its minimal polynomial.

T. 4.3 Tower Law. *Let $M \supseteq L$ and $L \supseteq K$ be finite field extensions. Then $M \supseteq K$ is a finite field extension and $[M : K] = [M : L][L : K]$.*

An extension $L \supseteq K$ is called **algebraic** if every element in L is algebraic over K. It is called **finite** if $[L : K] \neq \infty$. We say that the extension $L \supseteq K$ is **finitely generated** if $L = K(\alpha_1, \ldots, \alpha_n)$, where $\alpha_i \in L$.

T. 4.4 *A field extension $L \supseteq K$ is finite if and only if it is algebraic and finitely generated.*

T. 4.5 *If $K \subseteq M \subseteq L$ are field extensions such that M is algebraic over K and $\alpha \in L$ is algebraic over M, then it is algebraic over K.*

T. 4.6 *Let $L \supseteq K$. All elements in L algebraic over K form a field.*

If $L \supseteq K$, then the field of all elements of L algebraic over K is called the **algebraic closure of K in L**. If $K = \mathbb{Q}$ and $L = \mathbb{C}$, then the field of algebraic elements over $\mathbb{Q}$ will be denoted by $\mathbb{A}$ and called **the field of algebraic numbers**. A field K is called **algebraically closed** if it does not posses algebraic extensions, that is, for every field $L \supseteq K$, if $\alpha \in L$ is algebraic over K, then $\alpha \in K$. This means that K is algebraically closed when the only irreducible polynomials over K are polynomials of degree 1. The fields $\mathbb{C}$ and $\mathbb{A}$ are algebraically closed (see Ex. 13.14 for $\mathbb{C}$ and Ex. 4.17 for $\mathbb{A}$).

EXERCISES 4

4.1. Which of the following numbers are algebraic?

(a) $1 + \sqrt{2} + \sqrt{3}$;
(b) $\sqrt{3} + \sqrt[4]{3}$;
(c) $\sqrt[3]{3} + \sqrt{2}$;
(d) $\sqrt{\pi} + 1$;
(e) $\sqrt{\pi} + \sqrt{2}$;
(f) $\sqrt[3]{1 + \sqrt{e}}$.

4.2. (a) Show that if $f \in K[X]$ is irreducible over K and $L \supseteq K$ is a field extension such that the degree $\deg f$ and the degree $[L : K]$ are relatively prime, then f is irreducible over L.

(b) Prove **Nagell's Lemma**: Let $L \supset K$ be a field extension of prime degree q. If $f \in K[X]$ has prime degree p and is irreducible over K, but reducible over L, then $q = p$.

Remark. We use Nagell's Lemma in Ex. 13.6, where following Nagell, we prove, in a very simple way, insolvability in radicals of some fifth degree equations.

4.3. Find the minimal polynomial and the degree of α over K when:

(a) $K=\mathbb{Q}$, $\alpha=\sqrt[3]{\sqrt{3}+1}$;
(b) $K=\mathbb{Q}$, $\alpha=\sqrt{2}+\sqrt[3]{2}$;
(c) $K=\mathbb{Q}$, $\alpha^5=1$, $\alpha\neq 1$;
(d) $K=\mathbb{Q}(i)$, $\alpha=\sqrt{2}$;
(e) $K=\mathbb{Q}(\sqrt{2})$, $\alpha=\sqrt[3]{2}$;
(f) $K=\mathbb{Q}$, $\alpha^p=1$, $\alpha\neq 1$, p a prime number.

4.4. Find the degree and a basis of the following extensions $L\supseteq K$:

(a) $K=\mathbb{Q}$, $L=\mathbb{Q}(\sqrt{2},\,i)$;
(b) $K=\mathbb{Q}$, $L=\mathbb{Q}(\sqrt{2},\sqrt{3})$;
(c) $K=\mathbb{Q}$, $L=\mathbb{Q}(i,\sqrt[3]{2})$;
(d) $K=\mathbb{Q}$, $L=\mathbb{Q}(\sqrt[3]{2}+2\sqrt[3]{4})$;
(e) $K=\mathbb{R}(X+\frac{1}{X})$, $L=\mathbb{R}(X)$;
(f) $K=\mathbb{Q}$, $L=\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$;
(g) $K=\mathbb{Q}(\sqrt{3})$, $L=\mathbb{Q}(\sqrt[3]{1+\sqrt{3}})$;
(h) $K=\mathbb{F}_2$, $L=\mathbb{F}_2(\alpha)$, where $\alpha^4+\alpha^2+1=0$;
(i) $K=\mathbb{F}_3$, $L=\mathbb{F}_3(\alpha)$, where $\alpha^3+\alpha^2+2=0$;
(j) $K=\mathbb{R}(X^2+\frac{1}{X^2})$, $L=\mathbb{R}(X)$.

4.5. Show that a complex number $z=a+bi$ is algebraic (over $\mathbb{Q}$) if and only if a and b are algebraic.

4.6. Show that the numbers $\sin r\pi$ and $\cos r\pi$ are algebraic if r is a rational number.

4.7. Let $L=\mathbb{Q}(\sqrt[3]{2})$. Find $a,b,c\in\mathbb{Q}$ such that $x=a+b\sqrt[3]{2}+c\sqrt[3]{4}$ when

(a) $x=\dfrac{1}{\sqrt[3]{2}}$; (b) $x=\dfrac{1}{1+\sqrt[3]{2}}$; (c) $x=\dfrac{1+\sqrt[3]{2}}{1+\sqrt[3]{2}+\sqrt[3]{4}}$.

4.8. Let $L=\mathbb{Q}(\sqrt{2},\sqrt{3})$. Find $a,b,c,d\in\mathbb{Q}$ such that $x=a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$ when

(a) $x=\dfrac{1}{\sqrt{2}+\sqrt{3}}$; (b) $x=\dfrac{1}{1+\sqrt{2}+\sqrt{3}}$; (c) $x=\dfrac{\sqrt{2}+\sqrt{3}}{1+\sqrt{2}+\sqrt{3}+\sqrt{6}}$.

4.9. Let $L=\mathbb{F}_2(\alpha)$, where $\alpha^4+\alpha+1=0$. Find $a,b,c,d,\in\mathbb{F}_2$ such that $x=a+b\alpha+c\alpha^2+d\alpha^3$ when

(a) $x=\dfrac{1}{\alpha}$; (b) $x=\alpha^5$; (c) $x=\alpha^{15}$; (d) $x=\dfrac{1}{\alpha^2+\alpha+1}$.

4.10. (a) Show that if $\alpha\in K(X)\smallsetminus K$, $\alpha=\frac{p(X)}{q(X)}$, where $p,q\in K[X]$ and $SGD(p,q)=1$, then $[K(X):K(\alpha)]\leq n$, where $n=\max(\deg p,\deg q)$.

(b) Show that if $\alpha\in K(X)\smallsetminus K$, then α is transcendent over K.

(c) Show that with the notations in (a), there is an equality $[K(X):K(\alpha)]=n$.

Remark. A famous theorem of Lüroth says that all subfields L of $K(X)$ containing K are of the form $K(\alpha)$, where $\alpha\in K(X)$. The results of the exercise may be used in a proof of Lüroth's theorem (for a proof see XX[**?**]).

4.11. Let M_1,M_2 be two fields between K and L.

(a) Prove that if M_1 and M_2 are algebraic extensions of K, then also M_1M_2 is an algebraic extension of K.

(b) Prove that if $[M_1 : K] \neq \infty$ and $[M_2 : K] \neq \infty$, then $[M_1M_2 : K] \neq \infty$.

(c) Show that if $[M_1 : K] = r$ and $[M_2 : K] = s$, where $(r, s) = 1$, then $[M_1M_2 : K] = rs$ and $M_1 \cap M_2 = K$.

(d) Is there any "general" relation between $[M_1 : K]$, $[M_2 : K]$ and $[M_1M_2 : K]$?

4.12. Show that if $[K(\alpha) : K]$ is odd, then $K(\alpha) = K(\alpha^2)$. Is it true that $K(\alpha) = K(\alpha^2)$ implies that $[K(\alpha) : K]$ is odd?

4.13. (a) Show that if L is a field containing $\mathbb{C}$ and $[L : \mathbb{C}] \neq \infty$, then $L = \mathbb{C}$.

(b) Show that if L is a field containing $\mathbb{R}$ and $[L : \mathbb{R}] \neq \infty$, then $L = \mathbb{R}$ or $L \cong \mathbb{C}$.

4.14. Is it true that for each divisor d to $[L : K]$ there exists a field M between K and L such that $[M : K] = d$?

4.15. It is (well-)known that the numbers e and π are transcendental. It is not known whether $e + \pi$ and $e\pi$ are transcendental. Show that at least one of the numbers $e + \pi$ or $e\pi$ must be transcendental.

4.16. (a) Let $K \subseteq L$ be a field extension and let $f(\alpha) = 0$, where $\alpha \in L$ and $f(X)$ is a polynomial whose coefficients are algebraic over K. Prove that α is also algebraic over K.

(b) Assume that the number α is algebraic. Prove that also the following numbers are algebraic:

(b_1) α^2; (b_2) $\sqrt{\alpha}$; (b_3) $\sqrt[3]{1 + \sqrt{\alpha}}$.

4.17. Show that the algebraical closure of a field K in an algebraically closed field L containing it is also algebraically closed (for example, since $\mathbb{A}$ is the algebraical closure of $\mathbb{Q}$ in $\mathbb{C}$, it is algebraically closed – see Ex. 13.14).

USING COMPUTERS 4

Finite algebraic extensions of rational numbers $\mathbb{Q}$ and of finite fields $\mathbb{F}_p$ can be constructed in Maple using the command `RootOf` like:

```
> alias(a = RootOf(X^2+1));
```

$$a$$

which defines the extension $\mathbb{Q}(i)$ with i denoted here by a. If a field $K = \mathbb{Q}(a)$, where a is defined by `RootOf` (see p. 7), then we can both factorize a polynomial $g(X)$ over K by `>factor(g(X),a)` or ask whether it is irreducible using `>irreducible(g(X),a)`. For example, the polynomial $X^4 + 1$ over the field $\mathbb{Q}(i)$ is factored by the command:

```
> factor(X^4+1,a);
```

$$(X^2 - a)(X^2 + a)$$

If we want to define a finite field as an extension of $\mathbb{F}_p$ for a prime number p, then we write

```
> alias(b = RootOf(X^3+X+1 mod 2));
```

We have defined the field $\mathbb{F}_2(b)$ (we use b if it is the same session in which we used a above), whose degree is 8 over $\mathbb{F}_2$ (the polynomial $X^3 + X + 1$ is irreducible over $\mathbb{F}_2$) and we can make computations with it. For example:

```
>simplify(b^7 mod 2);
                                    1
```

which could be expected in the group of order 7 of all nonzero elements in the field $\mathbb{F}_2(b)$. It is possible to solve problems like Ex. 4.7, 4.8 or 4.9 finding for example `>simplify(1/(b^2+b+1))` in the field $\mathbb{F}_2(b)$.

In Maple, it is possible to find the minimal polynomial of an algebraic number over $\mathbb{Q}$ and over finite algebraic extensions of it (even if these tools are far from being perfect as yet and the results of computations should be always checked). For example, take $\alpha = \sqrt[3]{1+\sqrt{3}}$. We guess that this number has degree 6 over $\mathbb{Q}$ (but one can try with bigger values than the expected degree of the minimal polynomial and one has to be cautious). We use the following commands:

```
> with(PolynomialTools);
> r:= evalf((1+sqrt(3))^(1/3));
                                  1.397964868
> MinimalPolynomial(r,6);
                                      3     6
                              -2 - 2 _X  + _X
```

One can check the irreducibility of this polynomial (of course, it is irreducible by Eisenstein's criterion):

```
>factor(X^6-2*X^3-2)
```

$$X^6 - 2X^3 - 2$$

In general, we can find the minimal polynomial of α over a finite extension K of $\mathbb{Q}$ finding such polynomial over $\mathbb{Q}$ and then factoring this polynomial over K. We can check which of

the factors has α as its zero. If we continue with α above and if we want to get the minimal polynomial of this number over $K = \mathbb{Q}(\sqrt{3})$, then we note easily that $X^3 - (1 + \sqrt{3})$ is a polynomial with coefficients in K of degree 3 having α as its zero. Since we already know that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$ and $[K : \mathbb{Q}] = 2$, so $[\mathbb{Q}(\alpha) : K] = 3$, which means that the polynomial $X^3 - (1 + \sqrt{3})$ is minimal for α over K by **T.4.2**. In Maple, we can use the command:

```
>factor(X^6-2*X^3-2,sqrt(3))
```

$$(X^3 - 1 + \sqrt{3})(-X^3 + 1 + \sqrt{3})$$

which says that the two polynomials of degree 3 are irreducible (the second factor is the minimal polynomial of α). Observe, that instead of `sqrt(3)` one could define the field K using construction with `RootOf`.

Working in a field generated by algebraic numbers, it is possible to express the elements of the field by the elements of a basis using the command `rationalise` as the following example shows. We work in the field $\mathbb{Q}(\sqrt{5}, \sqrt{7})$ and we want express a number in this field by the powers of the generators $\sqrt{5}, \sqrt{7}$:

```
>a:= sqrt(5); b := sqrt(7)
```

$$5^{\frac{1}{2}}$$

$$7^{\frac{1}{2}}$$

```
>expand(rationalize(1/(a+b)))
```

$$\frac{3}{19}\sqrt{5} + \frac{11}{19} - 1/19\sqrt{7} - 2/19\sqrt{7}\sqrt{5}$$

4.18. Solve some of the exercises in Ex. 4.7, 4.8 or 4.9 using Maple.

4.19. Find minimal polynomials of the following numbers α over given fields:

(a) $\alpha = \sqrt[4]{2} + \sqrt{2} + 1$ over $\mathbb{Q}$;
(b) $\alpha = \sqrt[3]{2} + i$ over $\mathbb{Q}$;
(c) $\alpha = \sqrt[3]{2} + \sqrt{2} + 1$ over $\mathbb{Q}(\sqrt{2})$;
(d) $\alpha = \sqrt[4]{2} + i + 1$ over $\mathbb{Q}(i)$.

4.20. Factorize the given polynomial $f(X) \in \mathbb{Q}[X]$ into irreducible factors over $K = \mathbb{Q}(a)$, where a is a zero of $f(X)$:

(a) $f(X) = X^6 - 2$;
(b) $f(X) = X^5 - 5X + 12$;
(c) $f(X) = X^6 + 3X^3 + 3$;
(d) $f(X) = X^6 - 3X^2 - 1$;
(e) $f(X) = X^6 + 2X^3 - 2$;
(f) $f(X) = X^7 + 7X^3 + 7X^2 + 7X - 1$.

5

Splitting fields. Finite fields

If K is a field and $f \in K[X]$, then we say that L is a **splitting field** of f over K if $L = K(\alpha_1, \ldots, \alpha_n)$ and $f(X) = a(X - \alpha_1) \ldots (X - \alpha_n)$, where $a \in K$. We say that f has all its zeros in L and that L is generated over K by these zeros. Sometimes, the splitting field of f over K is denoted by K_f. If $\tau : K \to K'$ is an **embedding** of the field K into a field K', that is, τ is a injective function such that $\tau(x + y) = \tau(x) + \tau(y)$ and $\tau(xy) = \tau(x)\tau(y)$ for $x, y \in K$, then τ can be extended to an embedding of the polynomial rings $\tau : K[X] \to K'[X]$ (denoted by the same letter): $\tau(f(X)) = \tau(a_n)X^n + \cdots + \tau(a_1)X + \tau(a_0)$ when $f(X) = a_n X^n + \ldots + a_1 X + a_0 \in K[X]$ (compare to a more general context on p. 77). Very often, we consider the case when $\tau(K) = K'$, that is, the function τ is an **isomorphism** of the fields K and K'.

T. 5.1 *(a) If f is an irreducible polynomial over K, then there exists a field $L \supseteq K$ such that $L = K(\alpha)$ and $f(\alpha) = 0$.*

(b) If $\tau : K \to K'$ is a field isomorphism, f an irreducible polynomial over $K, L = K(\alpha)$, where $f(\alpha) = 0$ and $L' = K'(\alpha')$, where $\tau(f)(\alpha') = 0$, then there is an isomorphism $\sigma : K(\alpha) \to K'(\alpha')$ such that in the diagram:

$$\begin{array}{ccc} K(\alpha) & \xrightarrow[\sigma]{} & K'(\alpha') \\ \uparrow & & \uparrow \\ K & \xrightarrow[\tau]{} & K' \end{array},$$

we have $\sigma(\alpha) = \alpha'$ and $\sigma|_K = \tau$.

In particular, if $K = K'$ and $\tau = id$, then σ is an isomorphism over K (that is, the isomorphism σ maps each element in K on itself) of the two simple extensions of K by two arbitrary roots of $f(X) = 0$.

Usually, the above result is called **Kronecker's**[1] **theorem**. An inductive argument gives the following theorem, which will be used frequently:

T. 5.2 (*a*) *Every polynomial $f \in K[X]$ has a splitting field over K.*

(*b*) *If $\tau : K \to K'$ is an isomorphism of fields, L is a splitting field of a polynomial $f \in K[X]$ and L' is a splitting field of the polynomial $\tau(f) \in K'[X]$, then there exists an isomorphism $\sigma : L \to L'$*

$$\begin{array}{ccc} L & \xrightarrow[\sigma]{} & L' \\ \uparrow & & \uparrow \\ K & \xrightarrow[\tau]{} & K' \end{array}$$

which extends τ (that is $\sigma|_K = \tau$). In particular, if $K = K'$ and $\tau = id$, then two splitting fields for f over K are K-isomorphic (that is, the isomorphism σ maps each element in K on itself).

Moreover, if f is separable, then there are exactly $[L : K]$ different possibilities for σ when τ is given.

If $f(X) = a_0X + \ldots + a_nX^n \in K[X]$, then we define the **derivative** f' of f as the polynomial $f'(X) = a_1 + 2a_2X + \ldots + na_nX^{n-1}$. Exactly as for the polynomials in $\mathbb{R}[X]$, we have $(f_1 + f_2)' = f_1' + f_2'$ and $(f_1f_2)' = f_1'f_2 + f_1f_2'$, which can be checked by an uncomplicated computation.

T. 5.3 *A polynomial $f \in K[X]$ has no multiple zeros in any extension $L \supseteq K$ if and only if $SGD(f, f') = 1$.*

Using this theorem and the construction of the splitting fields, it possible to give a description of all finite fields.

T. 5.4 *The number of elements in a finite field is a power of a prime number.*

(*a*) *If p is a prime number and $n \geq 1$, then the splitting field for $X^{p^n} - X$ over $\mathbb{F}_p$ is a finite field with p^n element.*

(*b*) *Two finite fields with the same number of elements are isomorphic. More exactly, every finite field with p^n element is a splitting field of $X^{p^n} - X$ over $\mathbb{F}_p$.*

If a field K is algebraically closed, then all polynomials with coefficients in K split already in K, that is, for every polynomial $f(X) \in K[X]$, we have $f(X) = a_0(X - \alpha_1) \cdots (X - \alpha_n)$, where $a_0, \alpha_i \in K$ (see p. 18). The field of all complex numbers or the field of algebraic

[1] Leopold Kronecker (1823 – 1891) was a German mathematician known for his very important contributions in many fields of mathematics, but especially in number theory.

numbers have this property (see Ex. 13.14 for $\mathbb{C}$ and Ex. 4.17 for $\mathbb{A}$). By an **algebraic closure** of a field K, we mean a field $\overline{K}$, which is algebraic over K and algebraically closed. This means that such a field $\overline{K}$ contains a splitting field of every polynomial with coefficients in K. We have:

T. 5.5 *For every field K there exists an algebraic closure $\overline{K}$ and two algebraic closures of the same field K are K-isomorphic.*

EXERCISES 5

5.1. Find the degree and a basis of the splitting field over K for $f \in K[X]$ when

(a) $K = \mathbb{Q}$, $f = (X^2 - 2)(X^2 - 5)$;
(b) $K = \mathbb{Q}$, $f = X^3 - 2$;
(c) $K = \mathbb{Q}$, $f = X^4 - 2$;
(d) $K = \mathbb{Q}$, $f = X^4 + X^2 - 1$;
(e) $K = \mathbb{Q}$, $f = X^4 + 1$;
(f) $K = \mathbb{Q}(i)$, $f = X^4 - 2$;
(g) $K = \mathbb{Q}(i)$, $f = (X^2 - 2)(X^2 - 3)$;
(h) $K = \mathbb{Q}$, $f = X^p - 1$, p a prime number.

5.2. Decide whether the following pairs of fields are isomorphic:

(a) $\mathbb{Q}(\sqrt[4]{2})$ and $\mathbb{Q}(i\sqrt[4]{2})$;
(b) $\mathbb{Q}(\sqrt[3]{1+\sqrt{3}})$ and $\mathbb{Q}(\sqrt[3]{1-\sqrt{3}})$;
(c) $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$.

5.3. Let L be a splitting field of a polynomial $f(X)$ of degree n with coefficients in a field K. Show that $[L : K] \leq n!$.

5.4. Prove that a field with p^n elements contains a field with p^m elements if and only if $m|n$.

5.5. (a) Let $f(X)$ be an irreducible polynomial of degree n over a field $\mathbb{F}_p$. Show that $\mathbb{F}_p[X]/(f(X))$ is a field with p^n element, which is isomorphic with the splitting field of the polynomial $X^{p^n} - X$ and $f(X)$ divides $X^{p^n} - X$.

(b) Let $f(X)$ be an irreducible polynomial in $\mathbb{F}_p[X]$. Show that $f(X)|X^{p^n} - X$ if and only if $\deg(f(X))|n$.

5.6. Let $v_p(n)$ denote the number of the irreducible polynomials of degree n in $\mathbb{F}_p[X]$. Prove that

$$\sum_{d|n} dv_p(d) = p^n \quad \text{and} \quad v_p(n) = \frac{1}{n}\sum_{d|n} p^d \mu\left(\frac{n}{d}\right),$$

where $\mu(n)$ is the **Möbius function**, that is, $\mu(n) = 0$ if there is a prime number p whose square divides n, $\mu(n) = (-1)^k$ if n is a product of k different primes, and $\mu(1) = 1$.

5.7. (a) Prove that a finite subgroup of the multiplicative group K^* of a field K is cyclic.

(b) Prove that if $L \supseteq K$ are finite fields, then there is an element $\gamma \in L$ such that $L = K(\gamma)$.

5.8. (a) An irreducible polynomial $f \in \mathbb{F}_p[X]$ of degree n is called **primitive** if $f \nmid X^m - X$ when $m < p^n$. Prove that the number of primitive polynomials of degree n is equal to $\frac{1}{n}\varphi(p^n - 1)$, where φ is the Euler function, that is, $\varphi(n)$ for integer $n > 0$ equals the number of $0 < k < n$ such that $\gcd(k, n) = 1$.

(b) Show that for every finite field $\mathbb{F}$ and for every n there exists irreducible polynomials of degree n over $\mathbb{F}$.

5.9. Show that $(fg)' = f'g + fg'$ when $f, g \in K[X]$.

5.10. (a) Let L be a splitting field of the polynomial $X^n - 1$ over a field K. Show that the zeros of this polynomial, that is, the n-th roots of 1, form a finite cyclic group and that $L = K(\varepsilon)$, where ε is a generator of this group.

(b) Motivate that the number of the n-th roots of 1 in a splitting field of $X^n - 1$ over a field K is n if and only if the characteristic of K is 0 or it is relatively prime to n (does not divide n).

(c) Let L be a splitting field of a polynomial $X^n - a$ over a field K ($a \in K^*$). Show that $L = K(\varepsilon, \alpha)$, where ε generates the group of solutions of $X^n - 1 = 0$ in L and α is any fixed solution of the equation $X^n - a = 0$ in L. Motivate that all solutions of $X^n - a = 0$ are $\eta\alpha$, where η are all different n-th roots of 1.

5.11. (a) Let $a \in K$, where K is a field and let p be a prime number. Show that the polynomial $X^p - a$ is irreducible over K or has a zero in this field.

(b) Show that (a) is not true in general for binomials $X^n - a$ when n is not a prime number.

Remark. The result in (a) was first proved by Abel (see [Tsch, p. 287]). A more general result on reducibility of binomial polynomials $X^n - a$ is known as Capelli's Theorem (see [Tsch], p. 294): The polynomial $X^n - a$, where $a \in K$ (K of characteristic 0), is reducible over K if and only if there is a prime p dividing n and $b \in K$ such that $a = b^p$ or $n = 4$ and $a = -4b^4$ (for a proof see [Tsch], IV §2, [XXSchinzel]).

5.12. The polynomial $X^4 + 1$ is irreducible over $\mathbb{Q}$. Show that any reduction of $X^4 + 1$ modulo any prime number p gives a reducible polynomial over $\mathbb{F}_p$.

5.13. Let $\overline{K}$ be an algebraic closure of a field K and let L be an extension of K contained in $\overline{K}$. Show that $\overline{K}$ is also an algebraic closure of L.

USING COMPUTERS 5

It is possible to construct a splitting field of a polynomial (of not too high degree) using the command `>RootOf` (see p. 7) and the command `>allvalues`, which gives values of all zeros of the polynomial whose zero is defined by the command `>RootOf`, for example:

```
>alias(a=RootOf(X^4-10*X^2+1))
```

$$a$$

```
>allvalues(a)
```

$$\sqrt{3}-\sqrt{2}, \sqrt{3}+\sqrt{2}, -\sqrt{3}+\sqrt{2}, -\sqrt{3}-\sqrt{2}$$

```
>factor(X^4-10*X^2+1,a)
```

$$(-X-10a+a^3)(X-10a+a^3)(X+a)(-X+a)$$

Thus the field $K=\mathbb{Q}(\sqrt{2}+\sqrt{3})$ is the splitting field of $f(X)=X^4-10X^2+1$, since it splits in the linear factors when one of its zeros is adjoint to the field $\mathbb{Q}$ (in fact, we have `allvalues(a)[2]` equal to $\sqrt{2}+\sqrt{3}$, but all zeros give, of course, the same field).

The command `>factor(f(X),{a,b})` gives a possibility to check whether the extension by the chosen zeros of $f(X)$(here a, b) really gives a splitting field (in its splitting field, the polynomial $f(X)$ should split completely into linear factors). Unfortunately, the command `>alias` can not be defined in terms of another alias, which sometimes makes that the output in terms of different `RootOf`s is not easy to grasp. For example, we find that the splitting field of $f(X)=X^3-2$ is generated by two of its zeros (we choose a simple example in order to save the space - see Ex. 5.16):

```
>a:=RootOf(X^3-2)
```

$$RootOf(\_Z^3-2)$$

```
>factor(X^3-2,a)
```

$$-(-X+RootOf(\_Z^3-2))(X^2+RootOf(\_Z^3-2)X+RootOf(\_Z^3-2)^2)$$

```
>b:=RootOf(X^2+a*X+a^2)
```

$$RootOf(\_Z^2+RootOf(\_Z^3-2)_Z+RootOf(\_Z^3-2)^2)$$

```
> factor(X^3-2, {a, b})
```

$$(-X + RootOf(\_Z^2 + RootOf(\_Z^3 - 2)\_Z + RootOf(\_Z^3 - 2)^2))$$
$$(X+RootOf(\_Z^2+RootOf(\_Z^3-2)\_Z+RootOf(\_Z^3-2)^2)+RootOf(\_Z^3-2))(-X+RootOf(\_Z^3-2))$$

Using a, b the output is $(-X + b)(X + a + b)(-X + a)$ (which is $X^3 - 2$ – use command `>simplify` to the product). It is easy to check that $a = \sqrt[3]{2}$ and $b = \varepsilon\sqrt[3]{2}$, where $\varepsilon = \frac{-1+i\sqrt{3}}{2}$ is a 3rd root of 1.

5.14. Check that the fields you constructed in Ex. 5.1 really are splitting fields of the given polynomials f.

5.15. Find the degree of the splitting field over the rational numbers for polynomials f in Ex. 4.20.

5.16. Find the least number of zeros of the polynomial $f(X)$, which generate its splitting field over $\mathbb{Q}$:

(a) $f(X) = X^5 - 2$; (b) $f(X) = X^5 - 5X + 12$; (c) $f(X) = X^5 - X + 1$.

6

Automorphism groups of fields. Galois groups

Let L be a field. An **automorphism** of L is a bijective function $\sigma : L \to L$ such that

(a) $\sigma(x+y) = \sigma(x) + \sigma(y)$
(b) $\sigma(xy) = \sigma(x)\sigma(y)$

for arbitrary $x, y \in L$. If $L \supseteq K$ is a field extension, then an automorphism $\sigma : L \to L$ is called **K-automorphism** if

(c) $\sigma(x) = x$ for every $x \in K$.

T. 6.1 *All K-automorphisms of L form a group with respect to the composition of automorphisms.*

The group of all K-automorphisms of L is denoted by $G(L/K)$ and called the **Galois group** of L over K[1]. If G is an arbitrary group, which consists of automorphisms of L (e.g. $G = G(L/K)$, where $L \supseteq K$), then we define

$$L^G = \{x \in L : \forall_{\sigma \in G}\ \sigma(x) = x\}.$$

It is easy to check that L^G is a subfield of L. Sometimes, we want to construct some elements of the field L^G. Two most usual constructions are given by the **trace** (denoted Tr_G) and the **norm** (denoted Nr_G) with respect to G:

$$\mathrm{Tr}_G(\alpha) = \sum_{\sigma \in G} \sigma(\alpha), \qquad \text{and} \qquad \mathrm{Nr}_G(\alpha) = \prod_{\sigma \in G} \sigma(\alpha), \tag{6.1}$$

since clearly $\mathrm{Tr}_G(\alpha), \mathrm{Nr}_G(\alpha) \in L^G$ for $\alpha \in L$. Notice that $\mathrm{Tr}_G(\alpha+\beta) = \mathrm{Tr}_G(\alpha) + \mathrm{Tr}_G(\beta)$ and $\mathrm{Nr}_G(\alpha\beta) = \mathrm{Nr}_G(\alpha)\mathrm{Nr}_G(\beta)$ for $\alpha, \beta \in L$. The norm and the trace are often denoted by Tr_{L/L^G} and Nr_{L/L^G}.

[1] Sometimes, the group of all K-automorphisms of L is called Galois group only if $L \supseteq K$ is a Galois extension (see its definition in Chap. 9). We prefer the present convention for pedagogical reasons (in particular, to decrease the number of notions and notations).

T. 6.2 *If G is a group of automorphisms of L (finite or infinite), then L^G is a subfield of L and $[L : L^G] = |G|$.*

Almost all exercises will concentrate around this important theorem whose part claiming the inequality $[L : L^G] \leq |G|$ is often called **Artin's Lemma**. The theorem is a consequence of the following result:

T. 6.3 Dedekind's Lemma. *If $\sigma_1, \sigma_2, \ldots, \sigma_n$ are different automorphisms of a field L and the equality $a_1\sigma_1(x) + a_2\sigma_2(x) + \ldots + a_n\sigma_n(x) = 0$, where $a_i \in L$, holds for every $x \in L$, then $a_1 = a_2 = \ldots = a_n = 0$.*

Dedekind's Lemma can be also formulated as a statement saying that different automorphisms of a field L are linearly independent over L (e.g. in the vector space over L consisting of all the functions $f : L \to L$). By the **Galois group** over K of an equation $f(X) = 0$ or the polynomial $f(X)$, where $f(X) \in K[X]$, we mean the Galois group of any splitting field K_f over K. Instead of the notation $G(K_f/K)$, sometimes we denote it by G_f (when K is clear from the context) or $G_f(K)$.

If $K_f = K(\alpha_1, \ldots, \alpha_n)$, where α_i, $i = 1, \ldots, n$ are all zeros of $f(X) = 0$ and $\sigma \in G(K_f/K)$, then $\sigma(\alpha_i)$ is also a zero of $f(X) = 0$ (see Ex. 6.1). We write $\sigma(\alpha_i) = \alpha_{\sigma(i)}$, that is, we use the same symbol σ in order to denote the permutation $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ of the indices $1, \ldots, n$ of the zeros of $f(X)$ corresponding to σ. It is also an easy exercise (see Ex. 6.3) to show that the permutations σ of $1, \ldots, n$ corresponding to the automorphisms in the Galois group $G(K_f/K)$ form a subgroup of the symmetric group S_n (this subgroup depends of course on the numbering of the zeros of $f(X) = 0$). We shall denote any permutation group corresponding to $f(X) = 0$ by $\mathrm{Gal}(K_f/K)$ or Gal_f or $\mathrm{Gal}_f(K)$. In fact, Galois worked with his groups just in this way considering them as permutations groups. Since this notational distinction is not usual, we shall refer to "permutation (Galois) group" each time we want to consider the Galois group of a polynomial as a permutation group of its zeros. The Galois group $G(K_f/K)$ acts on the set $X_n = \{1, \ldots, n\}$ when the zeros $\alpha_1, \ldots, \alpha_n$ of $f(X)$ are ordered in some way and the action of $\sigma \in G(K_f/K)$ is defined by $\sigma(i) = j$ if and only if $\sigma(\alpha_i) = \alpha_j$. We shall apply the general terminology concerning actions of groups on sets as presented in the Appendix (see A.8).

EXERCISES 6

6.1. Let $L \supseteq K$ be a field extension.

(a) Show that if $\alpha \in L$ is a zero of $f \in K[X]$ and $\sigma \in G(L/K)$, then $\sigma(\alpha)$ is also a zero of f.

(b) Show that if $L = K(\alpha_1, \ldots, \alpha_r)$ and two automorphisms σ, $\tau \in G(L/K)$ are equal for every generator α_i (that is, $\sigma(\alpha_i) = \tau(\alpha_i)$ for each i), then $\sigma = \tau$ (that is, $\sigma(\alpha) = \tau(\alpha)$ for every $\alpha \in L$).

6.2. Find the Galois groups $G = G(L/K)$ for the following extensions $L \supseteq K$:

(a) $L = \mathbb{Q}(\sqrt{2})$, $K = \mathbb{Q}$;
(b) $L = \mathbb{Q}(\sqrt[3]{2})$, $K = \mathbb{Q}$;
(c) $L = \mathbb{Q}(\sqrt[4]{2})$, $K = \mathbb{Q}$;
(d) $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, $K = \mathbb{Q}$;
(e) $L = \mathbb{F}_2(X)$, $K = \mathbb{F}_2(X^2)$;
(f) $L = \mathbb{F}_5(X)$, $K = \mathbb{F}_5(X^4)$.

6.3. (a) Show that any automorphism of any field restricts to the identity on its prime field. In particular, the identity is the only automorphism of a prime field (that is, $\mathbb{Q}$ or $\mathbb{F}_p$).

(b) Let K be a field of characteristic $p \neq 0$. Show that $\sigma(x) = x^p$, $x \in K$ is an automorphism of K.

(c) Use (a) and (b) in order to prove Fermat's Little Theorem: If a is an integer and p a prime number, then p divides $a^p - a$.

6.4. Show that the field of the real numbers $\mathbb{R}$ has no non-trivial automorphisms.

6.5. Show that if $[L : K] < \infty$, then the order of the Galois group $G(L/K)$ divides the degree $[L : K]$.

6.6. (a) Show that if σ is a K-automorphism of the field $K(X)$, then $\sigma(X) = \frac{aX+b}{cX+d}$, where $a, b, c, d \in K$ and $ad - bc \neq 0$.

(b) Show that all functions on $K(X)$ of the form defined in (a) form the group of all automorphism of $K(X)$ over K (the functions of this form are often called **Möbius functions** by analogy with the case $K = \mathbb{R}$).

(c) Show that the group of automorphism of $K(X)$ over K is isomorphic to the quotient of the matrix group $GL_2(K)$ of all nonsingular (2×2)-matrices by the subgroup of scalar matrices aI, where $a \in K$, $a \neq 0$ and I is the (2×2) identity matrix.

6.7. Let $L = \mathbb{F}_2(X)$ and let G be the group of all $\mathbb{F}_2$-automorphisms of L (see Ex. 6.6). Find L^G.

6.8. Let $L = \mathbb{F}_3(X)$ and let G be the group of all automorphisms of L such that $\sigma(X) = aX + b$, where $a, b \in \mathbb{F}_3$ and $a \neq 0$. Find L^G.

6.9. (a) Let $L = \mathbb{R}(X, Y)$ and $G = \{\sigma_1, \sigma_2\}$, where σ_1 is the identity and σ_2 is defined by $\sigma_2(X) = -X$, $\sigma_2(Y) = Y$. Find L^G.

(b) Prove with the help of (a) that if $f(X, Y) \in \mathbb{R}(X, Y)$ is such that $f(-X, Y) = -f(X, Y)$, then $\int f(\sin x, \cos x)dx = \int g(t)dt$ for a function $g \in \mathbb{R}(t)$ and $t = \cos x$.

6.10. (a) Let $L = \mathbb{R}(X, Y)$ and $G = \{\sigma_1, \sigma_2\}$, where σ_1 is the identity and σ_2 is defined by $\sigma_2(X) = -X$, $\sigma_2(Y) = -Y$. Find L^G.

(b) Let $f(X, Y) \in \mathbb{R}(X, Y)$ and $f(-X, -Y) = f(X, Y)$. Using (a) show how to express the integral $\int f(\sin x, \cos x)dx$ as an integral of a rational function.

6.11. Let $L = \mathbb{Q}(X, Y)$ and $G = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ be the group of automorphisms of L defined by the table:

	X	Y
σ_1	X	Y
σ_2	$-X$	Y
σ_3	X	$-Y$
σ_4	$-X$	$-Y$

Find L^G.

6.12. Let $L = \mathbb{Q}(X)$ and $G =< \sigma >$, where $\sigma(X) = X + 1$. Find L^G.

6.13. (a) Let $L = K(X, Y)$ and $G =< \sigma_1, \sigma_2 >$, where σ_1 is the identity and $\sigma_2(X) = Y$, $\sigma_2(Y) = X$. Find L^G.

(b) Let $L = K(X_1, \ldots, X_n)$ and $G = S_n$, where for $\sigma \in S_n$, $\sigma(X_i) = X_{\sigma(i)}$. Show that $L^G = K(s_1, \ldots, s_n)$, where s_i are the elementary symmetric polynomials of $X_1, \ldots, X_n$, that is, $s_1 = \sum_{1 \le i \le n} X_i$, $s_2 = \sum_{1 \le i < j \le n} X_i X_j$, $s_3 = \sum_{1 \le i < j < k \le n} X_i X_j X_k$, ..., $s_n = X_1 X_2 \cdots X_n$.

6.14. Is it true that if $[L : K_1] \neq \infty$ and $[L : K_2] \neq \infty$, then $[L : K_1 \cap K_2] \neq \infty$, where K_1, K_2 are subfields of the field L?

USING COMPUTERS 6

There is not an evident general procedure to find the automorphism group of a given field extension $L \supset K$. In some cases, it is possible to describe such a group using Ex. 6.1 when the extension is represented as $L = K(\alpha)$ and the minimal polynomial $f(X)$ of α over K is given. Then each automorphism is uniquely determines by the image of α and such an image is a zero of the polynomial $f(X)$ in L. For example, take $K = \mathbb{Q}(\sqrt[4]{2})$. Then we define

```
>alias(a=RootOf(X^4-2))
```

$$a$$

```
>factor(X^4-2,a)
```

$$(X - a)(X + a)(X^2 + a^2)$$

Thus $f(X) = X^4 - 2$ has two zeros $\pm a$ in $K = \mathbb{Q}(a)$, where $a = \sqrt[4]{2}$ and there are two automorphisms $\sigma(a) = a$ (the identity) and $\sigma(a) = -a$.

Take $f(X) = X^3 - 7X + 7$ and define $K = \mathbb{Q}(a)$, where a is a zero of $f(X)$. Thus:

```
>alias(a=RootOf(X^3-7X+7))
```

$$a$$

```
>factor(X^3-7X+7,a)
```

$$(-X-14+4a+3a^2)(X-14+5a+3a^2)(-X+a)$$

Thus the zeros of $f(X)$ in K are $a, -14+4a+3a^2, 14-5a-3a^2$ and there are 3 automorphisms $\sigma_0(a)=a, \sigma_1(a)=-14+4a+3a^2, \sigma_2(a)=14-5a-3a^2$. We can check that $\sigma_1^2(a)=\sigma_2(a)$ (that is, $\sigma_1^2=\sigma_2$ (which is evident, since $G(K/\mathbb{Q})=\{\sigma_0,\sigma_1,\sigma_2\}$ is a cyclic group of order 3). In Maple, this can be done in the following way:

```
σ:=a -> -14+4*a+3*a^2
```

$$a \to -14+4a+3a^2$$

```
simplify(σ(σ(a)))
```

$$14-5a-3a^2$$

Thus $\sigma_1^2(a)=\sigma_2(a)$.

Let us consider one more example. Let $K=\mathbb{Q}(i)$ and let $f(X)=X^4-2$, so that $L=K(\sqrt[4]{2})=\mathbb{Q}(i,\sqrt[4]{2})$. We find all automorphisms of L over K defining:

```
>alias(c=RootOf(X^2+1))
```

$$a$$

```
>alias(d=RootOf(X^4-2))
```

$$b$$

```
>factor(X^4-2,{c,d})
```

$$(-X+cd)(X+cd)(X+d)(-X+d)$$

Thus, we have 4 automorphisms of $L=\mathbb{Q}(i,\sqrt[4]{2})$ over $K=\mathbb{Q}(i)$ given by $\sigma(d)=\pm d, \pm cd$, where $c=i, d=\sqrt[4]{2}$.

6.15. Find the orders of the Galois groups $G=G(K/\mathbb{Q})$ and find all automorphisms of the field K when:

(a) $K = \mathbb{Q}(a)$, a is a zero of $f(X) = X^6 - 2X^3 - 1$;

(b) $K = \mathbb{Q}(a)$, a is a zero of $f(X) = X^8 - 2X^4 + 4$;

(c) $K = \mathbb{Q}(a)$, a is a zero of $f(X) = X^{12} - 10X^6 + 1$.

7

Normal extensions

An extension $L \supseteq K$ is **normal** if every irreducible polynomial $f(X) \in K[X]$, which has one zero in L has all its zeros in L (that is, L contains a splitting field of $f(X)$).

T. 7.1 *A finite extension $L \supseteq K$ is normal if and only if L is a splitting field of a polynomial with coefficients in K.*

N is called the **normal closure** of $L \supseteq K$ if $N \supseteq L$ is a field extension such that $N \supseteq K$ is normal and if $N \supseteq N' \supseteq L$, where N' is a normal extension of K, then $N' = N$.

T. 7.2 *Let $L = K(\alpha_1, \ldots, \alpha_n)$ be a finite extension. Then the normal closure of $L \supseteq K$ is unique up to a K-isomorphism. More exactly, every normal closure of $L \supseteq K$ is a splitting field over K of $f = f_1 \cdots f_n$, where f_i is the minimal polynomial of α_i over K.*

EXERCISES 7

7.1. Which of the following extensions $L \supset K$ are normal:

(a) $L = \mathbb{Q}(\sqrt[4]{2})$, $K = \mathbb{Q}$;
(b) $L = \mathbb{Q}(\sqrt[3]{2})$, $K = \mathbb{Q}$;
(c) $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, $K = \mathbb{Q}$;
(d) $L = \mathbb{C}$, $K = \mathbb{R}$;
(e) $L = \mathbb{Q}(\sqrt[3]{2}, i)$, $K = \mathbb{Q}$;
(f) $L = \mathbb{Q}(\sqrt[4]{2})$, $K = \mathbb{Q}(\sqrt{2})$;
(g) $L = \mathbb{Q}(\sqrt[4]{2}, i)$, $K = \mathbb{Q}$;
(h) $L = \mathbb{Q}(X)$, $K = \mathbb{Q}(X^3)$;
(i) $L = \mathbb{C}(X)$, $K = \mathbb{C}(X^3)$;
(j) $L = \mathbb{F}_3(X)$, $K = \mathbb{F}_3(X^2)$.

7.2. Find the normal closure of the following field extensions $L \supset K$:

(a) $L = \mathbb{Q}(\sqrt[4]{2})$, $K = \mathbb{Q}$;
(b) $L = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$, $K = \mathbb{Q}$;
(c) $L = \mathbb{Q}(\varepsilon), \varepsilon^5 = 1$, $\varepsilon \neq 1$, $K = \mathbb{Q}$;
(d) $L = \mathbb{Q}(X)$, $K = \mathbb{Q}(X^3)$;
(e) $L = \mathbb{Q}(X)$, $K = \mathbb{Q}(X^4)$;
(f) $L = \mathbb{F}_3(X)$, $K = \mathbb{F}_3(X^4)$.

7.3. Let $L \supseteq M \supseteq K$ be field extensions.

(a) Let $L \supseteq M$ and $M \supseteq K$ be normal extensions. Is $L \supseteq K$ normal?
(b) Let $L \supseteq K$ be normal. Is $L \supseteq M$ normal?
(c) Let $L \supseteq K$ be normal. Is $M \supseteq K$ normal?

7.4. (a) Let $L \supseteq K$ be a normal extension and $\alpha, \beta \in L$ two zeros of an irreducible polynomial with coefficients in K. Show that there is an automorphism $\sigma \in G(L/K)$ such that $\sigma(\alpha) = \beta$.

(b) Show that if L is a finite normal extension of K and $\tau : M \to M'$ is a K-isomorphism of M with a subfield M' of L containing K, then there is an automorphism $\sigma \in G(L/K)$ whose restriction to M is equal to τ (in particular, every automorphism of M over K has an extension to an automorphism of L over K).

7.5. Let $L \supseteq M \supseteq K$ be field extensions.

(a) Show that if $M \supseteq K$ is normal and $\sigma \in G(L/K)$, then $\sigma M = M$.

(b) Show that if $L \supseteq K$ is normal, then $M \supseteq K$ is normal if and only if $\sigma M = M$ for each $\sigma \in G(L/K)$.

7.6. Let $L \supseteq K$ and M_1, M_2 be two fields between K and L. Prove that

(a) if $M_1 \supseteq K$ and $M_2 \supseteq K$ are normal, then $M_1 M_2 \supseteq K$ and $M_1 \cap M_2 \supseteq K$ are normal;

(b) if $M_1 \supseteq K$ is normal, then $M_1 M_2 \supseteq M_2$ is normal.

7.7. Let $L \supseteq K$ be a field extension and $\alpha, \beta \in L$. Show that if $K(\alpha) \supseteq K$ and $K(\beta) \supseteq K$ are normal extensions and $K(\alpha) \cap K(\beta) = K$, then $[K(\alpha, \beta) : K] = [K(\alpha) : K][K(\beta) : K]$.

7.8. Let $K \subset L$ be a normal extension and let $f(X)$ be a monic polynomial irreducible over K but reducible over L. Show that for every two monic irreducible factors $f_i(X)$ and $f_j(X)$ of $f(X)$ in $L[X]$, there is an automorphism $\sigma_{ij} : L \to L$ such that $\sigma_{ij}(f_i(X)) = f_j(X)$ (σ_{ij} maps the coefficients of $f_i(X)$ onto the corresponding coefficients of $f_j(X)$). In particular, all irreducible factors of $f(X)$ in $L[X]$ have the same degree.

7.9. An irreducible polynomial $f \in K[X]$ is called **normal** if a splitting field K_f of f over K can be obtained extending K by only one of the zeros of f, that is, $K_f = K(\alpha)$, where $f(\alpha) = 0$.

(a) Show that an irreducible polynomial $f \in K[X]$ is normal if and only if its splitting field over K has degree equal to the degree of $f(X)$.

(b) Show that the binomials $X^n - 2$ over $\mathbb{Q}$ are not normal when $n > 2$.

USING COMPUTERS 7

In the exercises below you can use the command `>galois(f(X))`, which gives the Galois group of the polynomial $f(X)$ over $\mathbb{Q}$ and the factorization of $f(X)$ over the extension of $\mathbb{Q}$ by a zero of $f(X)$ using `>factor(f(X),a)`.

7.10. For the given polynomial $f(X)$ and its zero a find the degree over $\mathbb{Q}$ of the normal closure L of $K = \mathbb{Q}(a)$ and the minimal number of zeros of $f(X)$, which generate L over $\mathbb{Q}$:

(a) $f(X) = X^6 - 2X^3 - 1$;
(b) $f(X) = X^6 - X^3 + 1$;
(c) $f(X) = X^6 + 2X^3 - 2$;
(d) $f(X) = X^6 + 3X^2 + 3$;
(e) $f(X) = X^7 - X + 1$;
(f) $f(X) = X^7 + 7X^3 + 7X^2 + 7X - 1$.

7.11. Decide whether the polynomial $f(X)$ is normal over $\mathbb{Q}$ (see Ex. 7.9):

(a) $f(X) = X^5 - X^4 - 4X^3 + 3X^2 + 3X - 1$;

(b) $f(X) = X^5 - 5X + 12$;

(c) $f(X) = X^7 + X^6 - 12X^5 - 7X^4 + 28X^3 + 14X^2 - 9X + 1$;

(d) $f(X) = X^8 - 72X^6 + 180X^4 - 144X^2 + 36$ (see [D]).

8

Separable extensions

An irreducible polynomial $f \in K[X]$ is called **separable** over K if it has no multiple zeros (in any extension $L \supseteq K$ – see **T.5.3**). We say that $\alpha \in L \supseteq K$ is a **separable element** over K if it is algebraic and its minimal polynomial over K is separable. We say that $L \supseteq K$ is a **separable extension** if every element of L is separable over K. A field K is called **perfect** if every algebraic extension of it is separable (that is, every irreducible polynomial in $K[X]$ is separable).

T. 8.1 (*a*) *All fields of characteristic* 0 *and all finite fields are perfect.*

(*b*) *If char* $(K) = p$*, then an irreducible polynomial* $f \in K[X]$ *is not separable if and only if* $f' \equiv 0$*, which is equivalent to* $f(X) = g(X^p)$*, where* $g \in K[X]$*.*

We say that $\gamma \in L$ is a **primitive element** (sometimes called **field primitive element**) of the extension $L \supseteq K$ if $L = K(\gamma)$ (see a remark after the proof of the theorem below for a comment concerning this terminology).

T. 8.2 Primitive element theorem. *If* $L = K(\alpha_1, \ldots, \alpha_n)$*, where* $\alpha_1, \ldots, \alpha_n$ *are algebraic and all with at most one exception are separable over* K*, then there is a primitive element of* L *over* K*. In particular, every finite separable extension has a primitive element.*

Sometimes we say that a field extension $K \subseteq L$ is **simple** if it has a primitive element, that is, there is $\gamma \in L$ such that $L = K(\gamma)$.

EXERCISES 8

8.1. (a) Show that $\mathbb{F}_2(X)$ is not separable over the field $\mathbb{F}_2(X^2)$.

(b) For every prime number p give an example of a non separable extension of a suitable field of characteristic p.

(c) Motivate that the field extension in (a) is normal.

8.2. Let $K \subset L$ be a quadratic field extension. Show that $L = K(\alpha)$, where $\alpha^2 = a \in K$ unless characteristic of K is 2 and L is separable over K. Show that then, we have $L = K(\alpha)$, where $\alpha^2 = \alpha + a$ for some $a \in K$. Motivate that $K \subset L$ is not separable if and only if characteristic of K is 2 and $L = K(\alpha)$, where $\alpha^2 = a \in K$.

8.3. Let K be a field of finite characteristic p.

(a) Let $\alpha \in L \supseteq K$, where L is a finite extension of K. Show that α is separable over K if and only if $K(\alpha^p) = K(\alpha)$.

(b) Show that $K \subseteq L$ is separable if and only if $KL^p = L$ (see Ex. 2.12(c)).

(c) Show that K is perfect if and only if $K^p = K$.

(d) Show that if L is an algebraically closed field and K its subfield such that $[L : K] < \infty$, then L is a Galois extension of K (see also Ex. 11.9).

8.4. (a) Show that $L = K(\alpha_1, \ldots, \alpha_n) \supseteq K$ is separable if and only if the elements $\alpha_1, \ldots, \alpha_n$ of L are separable over K.

(b) Show that the normal closure of a finite separable extension $L \supseteq K$ (see p. 35) is a separable extension of K.

8.5. Let $L \supseteq K$ be a field extension. Show that all elements $\alpha \in L$ separable over K form a subfield L_s between K and L.

Remark. The degree $[L_s : K]$ is called the **separable degree** of L over K and is denoted by $[L : K]_s$ (if $[L : K] < \infty$, then this means that $[L : K]_s$ divides $[L : K]$ and $[L : K]_s = [L : K]$ when $L \supseteq K$ is separable).

8.6. Let $L \supseteq K$ and char $(K) = p$. Show that for each $\alpha \in L$ there exists an exponent p^r such that α^{p^r} is separable over K (that is, $\alpha^{p^r} \in L_s$, where L_s is defined in Ex. 8.5).

8.7. (a) Let $N \supseteq L \supseteq K$, where N is a finite normal extension of K. Show that the number of different restrictions $\sigma|_L$, where $\sigma \in G(N : K)$ equals $[L : K]_s$ (see Ex. 8.5).

(b) Let $K \subseteq L$ be a finite field extension and let N be an algebraically closed field (see the definition on p. 18). Let $\tau : K \to N$ be an embedding of fields. Show that $[L : K]_s$ is equal to the number of different embeddings $\sigma : L \to N$ whose restriction to K equals τ.

8.8. Let L be a finite extension of K and let $L \supseteq M \supseteq K$. Show that the extension $L \supseteq K$ is separable if and only if the extensions $L \supseteq M$ and $M \supseteq K$ are separable.

8.9. Let L be a finite extension of K and $L \supseteq M \supseteq K$. Show that $[L : K]_s = [L : M]_s[M : K]_s$ (see Ex. 8.5).

8.10. Find a primitive element of $L \supseteq K$ when

(a) $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, $K = \mathbb{Q}$;
(b) $L = \mathbb{Q}(\sqrt{2} - i, \sqrt{3} + i)$, $K = \mathbb{Q}$;
(c) $L = \mathbb{Q}(\sqrt{2} + \sqrt{3}, \sqrt{2} + i, \sqrt{3} - i)$, $K = \mathbb{Q}$;
(d) $L = \mathbb{R}(X, Y)$, $K = \mathbb{R}(X^2, Y^2)$;
(e) $L = \mathbb{Q}(X, Y)$, $K = \mathbb{Q}(X + Y, XY)$;
(f) $L = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$, $K = \mathbb{Q}$.

8.11. Show that if $L = \mathbb{F}_2(X, Y)$, $K = \mathbb{F}_2(X^2, Y^2)$, then the extension $L \supset K$ is not simple, that is, one can not find $\gamma \in L$ such that $L = K(\gamma)$.

8.12. (a) Let $K \subset L = K(\gamma)$ be a finite field extension and let M be a field such that $K \subseteq M \subseteq L$. Show that M is generated over K by the coefficients of the minimal polynomial of γ over M.

(b) Show that the extension $L \supseteq K$ is simple and algebraic if and only if the number of fields between K and L is finite.

8.13. Give an example of a finite extension $L \supseteq K$ such that the number of fields between K and L is infinite.

8.14. Let $L \supseteq \mathbb{Q}$ be a finite and normal extension of odd degree. Show that $L \subseteq \mathbb{R}$.

8.15. Let $K \subseteq L$ be an extension of finite fields.

(a) Motivate that $L = K(\gamma)$ for any generator of the cyclic group L^* (see Ex. 5.7).

(b) Is it true that $L = K(\gamma)$ implies that γ is a generator of the group L^*?

Remark. It follows from (a) that any generator γ of the cyclic group L^* is a (field) primitive element of the extension $K \subseteq L$. In the theory of finite fields, such generators are also called primitive elements of this extension. In order to avoid misunderstandings, we shall use a longer term **group primitive elements** (see [R], p.214).

(c) Let $K = \mathbb{F}_3$ and $L = \mathbb{F}_{3^n}$. Find the numbers of group primitive and field primitive elements in L for $n = 2, 3, 4$.

8.16. Let M_1, M_2 be two fields between K and L. Prove that if M_1 and M_2 are separable extensions of K, then also $M_1 M_2$ and $M_1 \cap M_2$ are separable extensions of K.

USING COMPUTERS 8

The proof of **T.8.2** is effective if the zeros of the minimal polynomials of α, β such that $L = K(\alpha, \beta)$ are known (and K is infinite). Then it is possible to find $c \in K$ such that $\gamma = \alpha + c\beta$ is a primitive element of L over K (see the proof of **T.8.2** on p. 105). Another possibility is to try to guess γ and check that $L = K(\gamma) = K(\alpha, \beta)$. This can be done if we have the minimal polynomial of γ and we are able to define L, for example, using

the command `RootOf`. For example, we want to check that $\mathbb{Q}(\sqrt[3]{2},\sqrt[3]{3}) = \mathbb{Q}(\sqrt[3]{2}+\sqrt[3]{5})$. In some way (say, using Maple), we find the minimal polynomial of $\sqrt[3]{2}+\sqrt[3]{5}$, which is $f(X) = X^9 - 15X^6 - 87X^3 - 125$. Then we define:

```
>f:=X->X^9-15X^6-87X^3-125
```

```
>alias(c=RootOf(f(X))
```

We can denote `>r:=`$\sqrt[3]{2}+\sqrt[3]{5}$ and check `>simplify(f(r))`, which gives 0. We can also check that c is just r compering `>\evalf(r)` and `>\evalf(c)` (note that f has only one real zero). Now we take

```
>factor(X^3-2,c)
```

$$-\frac{1}{10125}(-225X^2-545X-175Xc^4+10Xc^7-209c^2-130c^5+7c^8)(45X-109c-35c^4+2c^7)$$

which shows that $\sqrt[3]{2} = \frac{1}{45}(109c+35c^4-2c^7) \in \mathbb{Q}(c)$ and similarly for $\sqrt[3]{3}$. Thus $\mathbb{Q}(\sqrt[3]{2},\sqrt[3]{3}) \subseteq \mathbb{Q}(\sqrt[3]{2}+\sqrt[3]{3})$, and the inverse inclusion is evident. But Maple can be successfully used in a similar way in order to prove that other elements than those chosen in the proof of **T.8.2** are primitive.

8.17. Find a primitive element c of $L \supseteq K$ when:

(a) $K = \mathbb{Q}, L = \mathbb{Q}(\sqrt{2},\sqrt[3]{2})$ (see Ex. 8.10(f));
(b) $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt[3]{3},\sqrt[5]{5})$;
(c) $K = \mathbb{Q}(\sqrt[3]{2})$, $L = K(\sqrt[3]{3},\sqrt[3]{5})$;
(d) $K = \mathbb{Q}(\sqrt[4]{2})$, $L = K(\sqrt[5]{2},\sqrt[6]{2})$.

9

Galois extensions

A field extension $L \supseteq K$ is called **Galois** if it is normal and separable.

T. 9.1 *Let $L \supseteq K$ be a finite field extension and $G(L/K)$ its Galois group. Then the following conditions are equivalent:*

(*a*) $[L : K] = |G(L/K)|$;

(*b*) $L^{G(L/K)} = K$;

(*c*) *There is a group G of K-automorphisms of L such that $K = L^G$ and then, $G = G(L/K)$;*

(*d*) *$L \supseteq K$ is normal and separable*;

(*e*) *L is a splitting field of a separable polynomial over K.*

If $L \supseteq K$ is a field extension, $\mathcal{F}$ the set of all fields between K and L and $\mathcal{G}$ the set of all subgroups to $G(L/K)$, then we define two functions:

$$f : \mathcal{G} \to \mathcal{F} \quad \text{and} \quad g : \mathcal{F} \to \mathcal{G}$$

in the following way:

$$f(H) = L^H = \{x \in L : \forall_{\sigma \in H} \sigma(x) = x\}$$

and

$$g(M) = G(L/M) = \{\sigma \in G(L/K) : \forall_{x \in M} \sigma(x) = x\}.$$

T. 9.2 The main theorem of Galois theory. *If $L \supseteq K$ is a finite Galois extension, then f and g are the inverse anti-automorphisms between partially ordered by inclusion sets $\mathcal{F}$ of all fields between K and L and the set $\mathcal{G}$ of all subgroups of $G(L/K)$, that is, $f \circ g = id_{\mathcal{F}}$, $g \circ f = id_{\mathcal{G}}$ and $f(H_1) \supseteq f(H_2)$ if $H_1 \subseteq H_2$, and $g(M_1) \supseteq g(M_2)$ if $M_1 \subseteq M_2$.*

Sometimes both the last theorem and the following one are called the main theorem of Galois theory:

T. 9.3 *Let $L \supseteq K$ be a Galois extension and M a field between K and L.*

(a) The extension $L \supseteq M$ is a Galois extension.

(b) The extension $M \supseteq K$ is a Galois extension if and only if $G(L/M)$ is normal in $G(L/K)$. If this holds, then $G(M/K) \cong G(L/K)/G(L/M)$.

EXERCISES 9

9.1. Which of the following extensions $L \supseteq K$ are Galois?

(a) $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt[3]{2})$;
(b) $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt[4]{2})$;
(c) $K = \mathbb{Q}(\sqrt{2})$, $L = \mathbb{Q}(\sqrt[4]{2})$;
(d) $K = \mathbb{Q}(i)$, $L = \mathbb{Q}(i, \sqrt[4]{2})$;
(e) $K = \mathbb{Q}(X^2)$, $L = \mathbb{Q}(X)$;
(f) $K = \mathbb{F}_p(X^2)$, $L = \mathbb{F}_p(X), p$ a prime number;
(g) $K = \mathbb{F}_2(X^2 + X)$, $L = \mathbb{F}_2(X)$;
(h) $K = \mathbb{R}(X^3)$, $L = \mathbb{R}(X)$.

9.2. Find all subgroups of the Galois group $G(L/K)$ of the splitting field L of the polynomial f as well as all corresponding subfields M between K and L when

(a) $K = \mathbb{Q}, f(X) = (X^2 - 2)(X^2 - 5)$;
(b) $K = \mathbb{Q}, f(X) = (X^4 - 1)(X^2 - 5)$;
(c) $K = \mathbb{Q}, f(X) = X^5 - 1$;
(d) $K = \mathbb{Q}, f(X) = X^4 + 1$;
(e) $K = \mathbb{Q}(i), f(X) = X^4 - 2$;
(f) $K = \mathbb{Q}, f(X) = X^3 - 5$;
(g) $K = \mathbb{Q}, f(X) = X^4 + X^2 - 1$;
(h) $K = \mathbb{Q}(i), f(X) = X^3 - 1$.

9.3. (a) Let $f(X) \in K[X]$ be a polynomial of degree n over a field K and let $K_f = K(\alpha_1, \ldots, \alpha_n)$ be a splitting field of $f(X)$ over K, where α_i are all zeros of $f(X)$ in K_f. Show that the permutations σ of the indices i of the zeros α_i corresponding to the automorphisms $\sigma \in G(L/K)$ according to $\sigma(\alpha_i) = \alpha_{\sigma(i)}$ form a subgroup of S_n.

(b) Give a description of the Galois group $G(K_f/K)$ as a permutation subgroup of S_n ($n = \deg f$) for polynomials $f(X)$ in Ex. 9.2.

9.4. (a) Let $f(X) \in K[X]$ be a polynomial and $f(X) = f_1(X) \cdots f_k(X)$ its factorization in $K[X]$ into a product of irreducible polynomials $f_i(X)$. Show that the permutation group $\mathrm{Gal}(K_f/K)$ consists of permutations, which have k orbits on the set $\{1, \ldots, n\}$.

(b) Show that the permutation group $\mathrm{Gal}(K_f/K)$ in (a) is transitive (that is, for each pair $i, j \in \{1, \ldots, n\}$, there is $\sigma \in \mathrm{Gal}(K_f/K)$ such that $\sigma(i) = j$) if and only if the polynomial $f(X)$ is irreducible in $K[X]$.

(c) Show that if the Galois group $\mathrm{Gal}(K_f/K)$ of a polynomial $f(X) \in K[X]$ acts on $X_n = \{1, \ldots, n\}$ with k orbits, then $f(X)$ is a product of k irreducible polynomials in $K[X]$.

9.5. Show that the extension $L \supseteq K$ is Galois, find the Galois group $G(L/K)$, all its subgroups and the corresponding subfields between K and L when

(a) $K = \mathbb{Q}, L = \mathbb{Q}(\sqrt{2}, i)$;
(b) $K = \mathbb{Q}, L = \mathbb{Q}(\sqrt[3]{2}, \varepsilon), \varepsilon^3 = 1, \varepsilon \neq 1$;
(c) $K = \mathbb{Q}, L = \mathbb{Q}(\sqrt[4]{2}, i)$;
(d) $K = \mathbb{R}(X^2 + \frac{1}{X^2}), L = \mathbb{R}(X)$;
(e) $K = \mathbb{R}(X^2, Y^2), L = \mathbb{R}(X, Y)$;
(f) $K = \mathbb{R}(X^2 + Y^2, XY), L = \mathbb{R}(X, Y)$.

9.6. Is it true that if $L \supseteq M$ and $M \supseteq K$ are Galois extensions, then $L \supseteq K$ is a Galois extension?

9.7. Let G be the automorphism group of the field $\mathbb{F}_3(X)$ consisting of all the automorphisms $X \to aX + b$, where $a \neq 0$ (see Ex. 6.8). Find all subgroups of G and the corresponding subfields between the field $\mathbb{F}_3(X)^G$ corresponding to G and $\mathbb{F}_3(X)$.

9.8. Let $L \supseteq K$ be a Galois extension and M a field between K and L. Show that $[M : K] = |G(L/K)|/|G(L/M)|$.

9.9. Let $L \supseteq K$ be a Galois extension and M a field between K and L.

(a) Show that $G(L/M)$ is a normal subgroup of $H(L/M) = \{\sigma \in G(L/K) | \sigma(M) = M\}$.

(b) Prove that the number of different fields between K and L, which are K-isomorphic to M equals

$$\frac{[M : K]}{|G(M/K)|} = \frac{|G(L/K)|}{|H(L/M)|}.$$

(c) Show that $M \supseteq K$ is Galois if and only if every automorphism $\sigma \in G(L/K)$ restricted to M maps M on M, that is, $H(L/M) = G(L/M)$.

(d) Let $\mathcal{N}(G(L/M))$ be the normaliser of the group $G(L/M)$ in $G(L/K)$ (see p. 227). Show that $H(L/M) = \mathcal{N}(G(L/M))$ and $G(M/K) = \mathcal{N}(G(L/M))/G(L/M)$.

(e) Let $\sigma \in G(L/M)$. Show that $G(L/\sigma(M)) = \sigma G(L/M)\sigma^{-1}$.

9.10. Let $L \supseteq K$ be a Galois extension with Galois group $G(L/K) = \{\sigma_1, \ldots, \sigma_n\}$. Let $\alpha \in L$ and let $G(L/K)\alpha$ be the orbit of α under the action of $G(L/K)$, that is, the set of all different images $\sigma_i(\alpha)$ for $\sigma_i \in G(L/K)$. Let $G_\alpha = \{\sigma \in G(L/K) \mid \sigma(\alpha) = \alpha\} = G(L/K(\alpha))$. Show that

(a) $\mid G(L/K)\alpha \mid = \frac{|G(L/K)|}{|G_\alpha|} = [K(\alpha) : K]$;

(b) The minimal polynomial of α over K is

$$f_\alpha(X) = \prod_{\sigma\alpha \in G(L/K)\alpha} (X - \sigma\alpha);$$

(c) Let

$$F_\alpha(X) = \prod_{\sigma \in G(L/K)} (X - \sigma\alpha).$$

Show that $F_\alpha(X) = f_\alpha(X)^{|G_\alpha|}$.

9.11. Let $K \subseteq L$ be a Galois extension and H a subgroup of the Galois group $G(L/K)$.

(a) Show that $\mathrm{Tr}_H : L \to L^H$ is a surjective linear mapping (see (6.1)).

(b) Let $\alpha_1, \ldots, \alpha_n$ be a basis of L over K. Show that $L^H = K(\mathrm{Tr}_H(\alpha_1), \ldots, \mathrm{Tr}_H(\alpha_n))$.

9.12. Let $L \supseteq K$ be finite fields and let $|K| = q$.

(a) Show that $L \supseteq K$ is a Galois extension.

(b) Show that the Galois group $G(L/K)$ is cyclic and generated by the automorphism $\sigma(x) = x^q$ (called the **Frobenius automorphism** of L over K).

(c) Find $\mathrm{Nr}_{L/K}(x)$ for $x \in L$ and show that every element of K is a norm of an element of L (see (6.1)).

9.13. Let $L = \mathbb{F}_2(\alpha)$, where α is a zero of the polynomial $X^4 + X + 1 \in \mathbb{F}_2[X]$. Show that $G(L/\mathbb{F}_2)$ contains exactly one subgroup H of order 2 and find $\beta \in L$ such that $L^H = \mathbb{F}_2(\beta)$.

9.14. Let $M_1 \supseteq K$ and $M_2 \supseteq K$ be finite Galois extensions and L a field, which contains both M_1 and M_2. Show that

(a) $M_1M_2 \supseteq K$ and $M_1 \cap M_2 \supseteq K$ are Galois extensions;

(b) $G(M_1M_2/M_2) \cong G(M_1/(M_1 \cap M_2))$;

(c) $G(M_1M_2/K) \cong G(M_1/K) \times G(M_2/K)$ if $M_1 \cap M_2 = K$.

(d) If there is an isomorphism of M_1 and M_2 over K (that is, there is an isomorphism $\tau : M_1 \to M_2$ which is the identity on K), then the Galois groups $G(L/M_1)$ and $G(L/M_2)$ are conjugated in $G(L/K)$ (that is, there is $\sigma \in G(L/K)$ such that $G(L/M_1) = \sigma G(L/M_2)\sigma^{-1}$).

9.15. Construct an extension $L \supset \mathbb{Q}$ whose Galois group is

(a) C_2;	(b) C_3;	(c) C_4;
(d) C_5;	(e) $C_2 \times C_2$	(f) $C_2 \times C_4$;
(g) $C_2 \times C_2 \times C_2$;	(h) $C_3 \times C_3$;	(i) D_4 (the symmetry group of a square);
(j) S_3;	(k) S_4;	(l) A_4.

Remark. The inverse Galois problem asks whether every finite group is (isomorphic to) the Galois group of some Galois extension of the rational numbers $\mathbb{Q}$. This problem is still unsolved even if for infinitely many finite groups G, it is possible to construct suitable Galois extensions $K \supset \mathbb{Q}$ having G as its Galois group. For example, all abelian groups, and even all solvable (see Chapter 13) groups have this property. Also the symmetric groups S_n

and alternate groups A_n can be realized as Galois groups over the rational numbers (see Ex. 13.4(c) and Ex. 15.12 for S_n and [MM], 9.2 for A_n). Notice that every finite group can be realized as the group of all automorphisms of a finite algebraic extension $K \supset \mathbb{Q}$ (see [KollarETCXXX]).

More generally, the same problem can be formulated for other fields K and the corresponding question whether a given finite group can be realized as the Galois group (or an automorphism group) of a suitable field extension of K has an answer in some cases and remains open in many other (see the presentations of the inverse Galois problem in e.g. [MM]).

(l) Using Ex. 13.4(c) and **A.9.3** show that for every finite group G there exists a Galois extension of number fields whose Galois group is isomorphic to G.

9.16. Prove that every cyclic group is a Galois group of a Galois extension $L \supseteq \mathbb{Q}$.

9.17. Is it true that $L \supset M \supset K$, where $[L : K] < \infty$ and $|G(L/K)| = 1$, implies $|G(M/K)| = 1$?

9.18. Let $L \supseteq K$ be a Galois extension and M_1, M_2 two fields between K and L. Let $G(L/M_1) = H_1$, $G(L/M_2) = H_2$. Find $G(L/M_1M_2)$ and $G(L/M_1 \cap M_2)$.

9.19. Let $L \supseteq K$ be a Galois extension with an abelian Galois group $G(L/K)$. Let f be the minimal polynomial of $\alpha \in L$ over K. Show that f is normal over K (that is, f has all its zeros in $K(\alpha)$ – see Ex. 7.9).

9.20. Let $K \subseteq L$ be a Galois extension and let N be a field containing L. Let M be any field such that $K \subseteq M \subseteq N$.

(a) Show that $LM \supseteq M$ is a Galois extension and the natural mapping of $\sigma \in G(LM/M)$ onto its restriction to L is an injection of $G(LM/M)$ into $G(L/K)$.

(b) Consider $G(LM/M)$ as a subgroup of $G(L/K)$ using the restriction in (a) and show that $L^{G(LM/M)} = L \cap M$ (so $[LM : M] = [L : L \cap M]$).

(c) Motivate that $G(LM/M) = G(L/K)$ if and only if $L \cap M = K$.

Remark. The property of Galois extensions given by (a) and (b) is often called the **theorem on natural irrationalities**.

9.21. Let $K \subseteq L$ be a Galois extension of number fields and assume that K is a real field, that is, $K \subseteq \mathbb{R}$. Show that either L is also real or L contains a subfield M such that $[L : M] = 2$ and M is real.

9.22. Let $K \subseteq L$ be a Galois extension with Galois group $G(L/K) = \{\sigma_1, \ldots, \sigma_n\}$. Show that if $\alpha \in L$ has n different images $\sigma_i(\alpha)$, then $L = K(\alpha)$, that is, the element α is primitive for the extension $K \subseteq L$.

9.23. Let K be a field of characteristic different from 2 and $f(X) \in K[X]$ be a separable polynomial of degree n. Denote by $\alpha_1, \ldots, \alpha_n$ the zeros of the polynomial $f(X)$ in its splitting field $L = K(\alpha_1, \ldots, \alpha_n)$ with (permutation) Galois group $\mathrm{Gal}(L/K)$. Let $\Delta(f) = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2$ be the discriminant of $f(X)$ (see p. 258).

(a) Show that $\Delta(f) \in K$.

(b) Show that $K(\sqrt{\Delta(f)})$ is the fixed field of the subgroup $\mathrm{Gal}_0(L/K)$ of $\mathrm{Gal}(L/K)$ consisting of all even permutations, in particular, all permutations in $\mathrm{Gal}(L/K)$ are even if and only if $\Delta(f)$ is a square in K.

9.24. Let K be a field of characteristic p such that $f(X) = X^p - X + 1$ has not a zero in K. Show that if α is a zero of $f(X)$ in its splitting field L over K, then all other zeros of this polynomial are $\alpha + i$ for $i = 1, \ldots, p-1$ and $L = K(\alpha)$. Deduce that L is a Galois extension of K, $f(X)$ is irreducible over K, $[L : K] = p$ and that $G(L/K)$ is a cyclic group of order p (see also Ex. 11.8).

USING COMPUTERS 9

f $K \subset L$ is a Galois field extension, then a description of its Galois group $G(L/K)$ is easiest if L is represented as a simple extension $L = K(a)$ and the minimal polynomial $f(X)$ of a over K is known. Then it is possible to factorize $f(X)$ over L (using `>factor(f(X),a)` where a is defined by `>alias(a=RootOf(f(X)))`) and define all automorphisms σ of L over K sending a onto all zeros of $f(X)$ in L (which can be obtained from the factorization of $f(X)$ over L). If $L = K(\alpha_1, \ldots, \alpha_k)$ for $\alpha_i \in L$ (in Maple it is easier to denote the zeros by, say, ai), then as we know from **T.7.2**, the field L is a splitting field of the polynomial $f(X)$, which is the product of the minimal polynomials $f_i(X)$ of α_i. In a particular case when $[L : K] = \prod_{i=1}^{k} \deg f_i(X)$, every automorphism is uniquely given by a mapping of every α_i on a fixed zero of $f_i(X)$. If L is obtained in several steps as a splitting field of a polynomial $f(X)$, then it is also possible to describe this field by gradually adjoining its zeros as in the following example:

```
>a:=RootOf(X^4-2)
```

$$a := RootOf(\_Z^4 - 2)$$

```
factor(X^4-2,a)
```

$$-(X^2 + RootOf(\_Z^4 - 2)^2)(X + RootOf(\_Z^4 - 2))(-X + RootOf(\_Z^4 - 2))$$

so $\mathbb{Q}(a)$ is not a splitting field. We continue and adjoin another zero:

```
>b := RootOf(X^2+RootOf(_Z^4-2)^2, a)
```

$$b := RootOf(\_Z^2 + RootOf(\_Z^4 - 2)^2, RootOf(\_Z^4 - 2))$$

```
>factor(X^4-2, {a, b})
```

$$(-X + RootOf(\_Z^4 - 2))(-X + RootOf(\_Z^2 + RootOf(\_Z^4 - 2)^2, RootOf(\_Z^4 - 2)))$$
$$(X + RootOf(\_Z^2 + RootOf(\_Z^4 - 2)^2, RootOf(\_Z^4 - 2)))(X + RootOf(\_Z^4 - 2))$$

which using a, b can be rewritten as $X^4 - 2 = (-X + a)(-X + b)(X + b)(X + a)$. Thus $\mathbb{Q}(a, b)$ is a splitting field of $X^4 - 2$.

9.25. Describe the Galois groups of the polynomials in Ex. 7.11(a),(c)(d) using a chosen zero generating the splitting field.

9.26. Show that the polynomials $f(X)$ are normal, list all automorphisms of their splitting fields K and describe the Galois groups when

(a) $f(X) = X^3-3X+1$; (b) $f(X) = X^6-X^3+1$; (c) $f(X) = X^6+3X^5+6X^4+3X^3+9X+9$.

9.27. Find the orders of the Galois groups of the following polynomials and determine the minimal number of zeros of each polynomial which generate its splitting field:

(a) $f(X) = X^5 - 5X + 12$; (b) $f(X) = X^5 + 20X + 16$; (c) $f(X) = X^5 - X + 1$.

10

Cyclotomic extensions

This chapter can be considered as an illustration of the general theory of Galois extensions in a special case, which plays a central role in number theory. If $\varepsilon \in \mathbb{C}$ is a **primitive** $n-$th root of 1, that is, $\varepsilon^n = 1$ and $\varepsilon^k \neq 1$, when $0 < k < n$ (for example, $\varepsilon = e^{\frac{2\pi i}{n}}$), then the field $\mathbb{Q}(\varepsilon)$ is called the **n-th cyclotomic field**.

T. 10.1 (*a*) *The degree* $[\mathbb{Q}(\varepsilon) : \mathbb{Q}] = \varphi(n)$, *where* ε *is a primitive* n*-th root of unity and* φ *is the Euler function.*

(*b*) *Each automorphism* σ *in the Galois group* $G(\mathbb{Q}(\varepsilon)/\mathbb{Q})$ *is given by* $\sigma_k(\varepsilon) = \varepsilon^k$, *where* $k \in \{1, \ldots, n\}$ *and* $\gcd(k, n) = 1$. *The mapping* $\sigma_k \mapsto k \pmod n$ *gives an isomorphism* $G(\mathbb{Q}(\varepsilon)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$.

The cyclotomic fields can be defined over arbitrary fields K. If n a positive integer, we denote by $\mathcal{C}_n(K)$ the splitting field of the polynomial $X^n - 1$ over K and by $\mathcal{G}_n(K)$ the group of all $n-$th roots of 1 in $\mathcal{C}_n(K)$, that is, the group of all solutions in $\mathcal{C}_n(K)$ of the equation $X^n - 1 = 0$. We call $\mathcal{C}_n(K)$ the $n-$th **cyclotomic field** over K. If K has characteristic p dividing n, then $X^n - 1 = (X^{\frac{n}{p}} - 1)^p$, so the splitting field of $X^n - 1$ is the same as the splitting field of $X^{\frac{n}{p}} - 1$, so investigating the cyclotomic fields over K, we can assume that the characteristic of K does not divide n. We always assume this in the exercises below. A consequence of this assumption is that the equation $X^n - 1$ has n different zeros (its derivative nX^{n-1} is relatively prime to it – see **T.5.3**). Thus the group $\mathcal{G}_n(K)$ has order n and is cyclic (see Ex. 5.7). The primitive $n-$th roots of 1 over K are the generators of the group $\mathcal{G}_n(K)$. If ε is one of them, then all others are given by ε^j, where $0 < j < n$ and $\gcd(j, n) = 1$ (see A.2.2). Thus the number of such generators is the value of the Euler function $\varphi(n)$ (see p. 256). The **n−th cyclotomic polynomial over** K is the polynomial

$$\Phi_{n,K}(X) = \prod_{\substack{0<k<n,\\ \gcd(k,n)=1}} (X - \varepsilon^k).$$

If $K = \mathbb{Q}$, then $\Phi_{n,K}(X)$ is usually denoted by $\Phi_n(X)$.

T. 10.2 *Let K be a field whose characteristic does not divide n.*

(a) We have:

$$X^n - 1 = \prod_{d|n} \Phi_{d,K}(X) \quad \text{and} \quad \Phi_{n,K}(X) = \prod_{d|n} (X^d - 1)^{\mu(\frac{n}{d})},$$

where μ denotes the Möbius function (see Ex. 5.6).

(b) The cyclotomic polynomials $\Phi_{n,K}(x)$ are monic and their coefficients are integer multiples of the unity of K.

(c) All irreducible factors of $\Phi_{n,K}(x)$ are of the same degree.

(d) If $K = \mathbb{Q}$, then $\Phi_n(X) = \Phi_{n,\mathbb{Q}}(x)$ is irreducible over $\mathbb{Q}$.

EXERCISES 10

10.1. Find the cyclotomic polynomials $\Phi_n(X)$ for $n = 1, 2, \ldots, 10$.

10.2. The **kernel** $r(n)$ of an integer $n > 1$ is the product of all different prime numbers dividing n. Show the following:

(a) $\Phi_p(X) = X^{p-1} + \cdots + X + 1$, where p is a prime,

(b) $\Phi_n(X) = \Phi_{r(n)}(X^{\frac{n}{r(n)}})$ when $n > 1$,

(c) $\Phi_{pn}(X) = \Phi_n(X^p)/\Phi_n(X)$, where p is a prime not dividing n,

Explain how to use (a), (b), (c) in order to compute the cyclotomic polynomials $\Phi_n(X)$. Compute $\Phi_{20}(X)$ and $\Phi_{105}(X)$.

10.3. Show the following identities:

(a) $\Phi_n(X) = \Phi_k(X^{\frac{n}{k}})$, where k is any divisor of n such that $r(k) = r(n)$ (see the definition of $r(k)$ in Ex. 10.2).

(b) If r, s are relatively prime positive integers,then

$$\Phi_{rs}(X) = \prod_{d|r} (\Phi_s(X^d))^{\mu(\frac{r}{d})}$$

10.4. Show that $\Phi_{2m}(X) = \Phi_m(-X)$, when $m > 1$ is an odd integer.

10.5. Let m, n be to relatively prime positive integers.

(a) Show that $\mathbb{Q}(\varepsilon_{mn}) = \mathbb{Q}(\varepsilon_m)\mathbb{Q}(\varepsilon_n)$ and $\mathbb{Q}(\varepsilon_m) \cap \mathbb{Q}(\varepsilon_n) = \mathbb{Q}$.

(b) Show that $\Phi_n(X)$ is irreducible over $\mathbb{Q}(\varepsilon_m)$.

(c) What can be said about $\mathbb{Q}(\varepsilon_m)\mathbb{Q}(\varepsilon_n)$ and $\mathbb{Q}(\varepsilon_m) \cap \mathbb{Q}(\varepsilon_n)$ when m, n are not necessarily relatively prime?

10.6. Find η such that $\mathbb{Q}(\eta)$ is the maximal real subfield of the $n-$th cyclotomic field $\mathbb{Q}(\varepsilon_n)$ $(n > 2)$ and motivate that $[\mathbb{Q}(\varepsilon_n) : \mathbb{Q}(\eta)] = 2$.

10.7. Let $K = \mathbb{Q}(\varepsilon_p)$ be $p-$th cyclotomic field, where p is a prime number. According to **T.10.1**, the group $G(K/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^*$.

(a) Show that the group $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic (of order $p-1$).

(b) Show that for each divisor d of $p-1$ there exists exactly one $M \subseteq K$ such that $[M : \mathbb{Q}] = d$.

(c) Let $\sigma \in G(K/\mathbb{Q}) = (\mathbb{Z}/p\mathbb{Z})^*$ generate this Galois group and let $\sigma(\varepsilon_p) = \varepsilon_p^g$, where g generates the cyclic group $(\mathbb{Z}/p\mathbb{Z})^*$. Show that if d is a divisor of $p-1$ and $p-1 = dm$, then $G_d = \{\sigma^0, \sigma^m, \ldots, \sigma^{(d-1)m}\}$ is the (unique) subgroup of $G(K/\mathbb{Q})$ of order d and $K^{G_d} = \mathbb{Q}(\theta_d)$, where

$$\theta_d = \varepsilon_p + \sigma^m(\varepsilon_p) + \cdots + \sigma^{(d-1)m}(\varepsilon_p)$$

Remark. The elements θ_d for d dividing $p-1$ are called **Gaussian periods**.

10.8. Find all quadratic subfields (that is, K with $[K : \mathbb{Q}] = 2$) in the following cyclotomic fields:

(a) $\mathbb{Q}(\varepsilon_8)$; (b) $\mathbb{Q}(\varepsilon_5)$; (c) $\mathbb{Q}(\varepsilon_7)$.

10.9. Using Gaussian periods (see Ex. 10.6) find the description of all subfields of the cyclotomic fields $K = \mathbb{Q}(\varepsilon_p)$ for

(a) $p = 5$, (b) $p = 7$, (c) $p = 17$.

In each case, find explicitly the corresponding Gaussian periods.

10.10. Let $p > 2$ be a prime. Show that the only quadratic subfield M of $K = \mathbb{Q}(\varepsilon_p)$ is $M = \mathbb{Q}(\sqrt{p})$ if $p = 1 \pmod 4$ and $M = \mathbb{Q}(\sqrt{-p})$ if $p = 3 \pmod 4$.

Remark. This result can be obtained using (quadratic) Gauss sums (see [L], Chap.VI, §3). The result shows that quadratic fields $\mathbb{Q}(\sqrt{\pm p})$ are subfields of cyclotomic fields. This is true for all quadratic fields, and in still more generality, for all finite abelian Galois extension of $\mathbb{Q}$. In fact, the Kronecker-Weber theorem says that every finite abelian extension of the rational numbers $\mathbb{Q}$ is a subfield of a cyclotomic field (see [XXX]).

10.11. Find and factorize the cyclotomic polynomials:

(a1) $\Phi_{7,\mathbb{F}_2}(X)$; (a2) $\Phi_{18,\mathbb{F}_7}(X)$; (a3) $\Phi_{26,\mathbb{F}_3}(X)$.

(b) Show that the orders of irreducible factors of $\Phi_{n,\mathbb{F}_p}(X)$ are equal to the order of p in the group $\mathbb{Z}_n^*$ if $p \nmid n$.

10.12. (a) Let d, n be positive integers and $d \mid n$. Show that if a prime p divides $\Phi_d(x)$ and $\Phi_n(x)$ for an integer x, then $p \mid n$;

(b) Show that if a prime p divides $\Phi_n(x)$ for an integer x, then $p \mid n$ or $p = 1 \pmod{n}$;

(c) Show that $\Phi_1(0) = -1$ and $\Phi_n(0) = 1$ when $n > 1$;

(d) Let n be a positive integer. Show that there exists infinitely many primes p with $p = 1 \pmod{n}$.

Remark. This is a special case of the famous **Dirichlet's theorem about primes in arithmetic progressions**, which says that in any arithmetical progression $ak + b$, where a, b are relatively prime integers and $k = 1, 2, \ldots$, there are infinitely prime numbers. The last part of this exercise says that there exists infinitely many primes in the progression $nk + 1$ $(a = n, b = 1)$. For a proof of the Dirichlet's theorem in its general version see [SCoursArith].

10.13. (a) Prove that for any finite abelian group there is a positive integer n and a surjective homomorphism $\varphi : (\mathbb{Z}/n\mathbb{Z})^* \to G$.

(b) Show that every finite abelian group G is a Galois group $G(K/\mathbb{Q})$ for a number field K. See the Remark after Ex. 9.15.

10.14. (a) Let L be a splitting field of a polynomial $X^n - a$ $(a \in K, a \neq 0)$ over a field K whose characteristic does not divide n (see Ex. 5.10). Show that the Galois group $G(L/K)$ contains a normal subgroup H isomorphic to a subgroup of $\mathbb{Z}_n$ such that the quotient G/H is isomorphic to a subgroup of $\mathbb{Z}_n^*$. What is the maximal possible order of $G(L/K)$?

(b) Show that the Galois group $G(L/K)$ in (a) is isomorphic to a subgroup of the group of matrices $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$, where $a \in \mathbb{Z}_n^*$, $b \in \mathbb{Z}_n$ (a subgroup of the group $GL_2(\mathbb{Z}_n)$ of all invertible (2×2)-matrices over the ring $\mathbb{Z}_n$).

(c) Give a description of the Galois groups over $\mathbb{Q}$ of the irreducible binomials $X^p - a$, where $a \in \mathbb{Q}$ and p is a prime number.

(d) Give a description of the Galois group over $\mathbb{C}(X)$ of the binomial $T^n - X$.

10.15. Let $\varepsilon_k = e^{\frac{2\pi i}{k}}$ for $k = 1, 2, \ldots$.

(a) Show that the group of all roots of 1 in $K = \mathbb{Q}(\varepsilon_m)$ is ε_m^k, $k = 1, \ldots, m$ when m is even or $\pm\varepsilon_m^k$, $k = 1, \ldots, m$ when m is odd.

(b) Show that $\mathbb{Q}(\varepsilon_m) = \mathbb{Q}(\varepsilon_n)$, where $n \geq m$, if and only if $m = n$ or $n = 2m$ and m is odd.

(c) Show that $\mathbb{Q}(\varepsilon_m) \subseteq \mathbb{Q}(\varepsilon_n)$ if and only if $m \mid n$ or m is even, n is odd and $\frac{m}{2} \mid n$.

10.16. Find the orders of the Galois groups of the following binomials over the field $\mathbb{Q}$:

(a) X^4+1; (b) X^4-3; (c) X^6+3; (d) X^6-3;
(e) X^6+4; (f) X^8+1; (g) X^8+2; (h) X^8-2.

USING COMPUTERS 10

It is not difficult to compute the cyclotomic polynomials over the rational numbers, but in Maple, we get $\Phi_{n,\mathbb{Q}}(X)$ using the command `>cyclotomic(n,x)` preceded by the command `>with(numtheory)`, which loads several commands related to number theory. Below, we suggest some numerical experiments.

10.17. Look at the coefficients of the cyclotomic polynomials $\Phi_{n,\mathbb{Q}}(X)$ and find the first n for which there is a coefficient of `>cyclotomic(n,x)` whose absolute value is bigger than 1. What could be an explanation that such a coefficient finally appears?

10.18. (a) Study the orders of the Galois groups of irreducible binomials X^6-a for some set of integer values of a. What is the size of this group for all possible values of a?

(b) Do the same for binomials X^7-a, X^8-a and X^9-a.

11

Galois modules

If G is an arbitrary group and A an abelian group, then A is called a G-module if to every $a \in A$ and $\sigma \in G$ corresponds an element $\sigma(a) \in A$ in such a way that $\sigma(a+b) = \sigma(a)+\sigma(b)$, $(\sigma\sigma')(a) = \sigma(\sigma'(a))$ and $e(a) = a$ ($a, b \in A$, $\sigma, \sigma' \in G$, e is the unity in G). If $K \subseteq L$ is a Galois extension with $G = G(L/K)$, then both L^+ and L^* can be considered as G-modules, where the action G is given by $(\sigma, x) \mapsto \sigma(x)$ for $\sigma \in G$ and $x \in L^+$ or $x \in L^*$. These two G-modules play a very important role in many applications of Galois theory in algebra, number theory and algebraic geometry. For the general terminology concerning G-modules and more examples see **A.7** (in particular **A.7.4**). In particular, we explain there the notion of the group ring $K[G]$ of a finite group $G = \{\sigma_1 = 1, \sigma_2, \ldots, \sigma_n\}$ over a field (or a commutative ring) K, whose elements are sums $a_1\sigma_1 + a_2\sigma_2 + \cdots + a_n\sigma_n$, where $a_i \in K$. Any G-module A can be considered as a module over this ring and conversely (for details see **A.7.4**).

In this chapter, we gather some results on field extensions, which are concerned with $G(L/K)$-module structures related to L. The first is the **normal basis theorem**, which explains the structure of L^+ as a Galois module. **Hilbert's Theorem 90** (which has number 90 in Hilbert's treatise on algebraic number theory published in 1895) gives an information about the multiplicative group of L considered as a module over $G(L/K)$. Hilbert's theorem and the closely connected to it so called **Noether's equations** showed the way to the general definitions of the **cohomology groups** and found a natural place in their context. We apply Hilbert's Theorem 90 (or rather a consequence of it) to abelian **Kummer theory** concerned with important class of Galois extensions whose elementary description follows a pattern, which is typical in much deeper Class Field Theory – a fundamental part of algebraic number theory of abelian Galois extensions.

T.11.1 *Let $K \subseteq L$ be a Galois extension and $G(L/K) = \{\sigma_1 = 1, \sigma_2, \ldots, \sigma_n\}$ its Galois group. Then the following properties of the extension $K \subseteq L$ hold and are equivalent:*

(a) There exists $\alpha \in L$ such that $\sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_n(\alpha)$ is a basis of L over K.

(b) L^+ is a cyclic $K[G]-$module, that is, there is $\alpha \in L$ such that $L^+ = K[G]\alpha$ for some $\alpha \in L$.

Any basis $\sigma_1(\alpha) = \alpha, \sigma_2(\alpha), \ldots, \sigma_n(\alpha)$ of L over K is called **normal**. Also an element α defining such a basis as well as its minimal polynomial are called **normal**[1]. Thus the last theorem says that every finite Galois extension has a normal basis.

T. 11.2 Hilbert's Theorem 90. *Let $L \supseteq K$ be a cyclic extension of degree n and let σ be a generator of the Galois group $G = G(L/K)$. If $\alpha \in L$, then*

(a) $\mathrm{Nr}_G(\alpha) = 1$ if and only there is $\beta \in L$ such that $\alpha = \frac{\beta}{\sigma(\beta)}$.

(b) $\mathrm{Tr}_G(\alpha) = 0$ if and only if there is $\beta \in L$ such that $\alpha = \beta - \sigma(\beta)$.

One of the applications of Hilbert's Theorem 90 (in the multiplicative version (a)) is a possibility to describe cyclic extensions over a field which contains sufficiently many roots of unity:

T. 11.3 *Let K be a field containing n different n-th roots of unity. If L is a cyclic extension of K of degree n, then there exists $\alpha \in L$ such that $L = K(\alpha)$ and $\alpha^n \in K$.*

For the case of characteristic of K dividing the degree of a cyclic extension see Ex. 11.8.

Remark 11.1 The last result **T.11.3** is often called Lagrange's theorem. It was proved by Lagrange about one century earlier than Hilbert's Theorem 90. It is possible to use Hilbert's result in its proof, which gives a simplification of the argument, so Lagrange's theorem is often considered as an application of Hilbert's Theorem 90. The simplification is obtained when one notes that $\mathrm{Nr}(\varepsilon) = \varepsilon^n = 1$, so that there exists $\alpha \in L$ such that $\varepsilon = \frac{\alpha}{\sigma(\alpha)}$ by **T.11.2** (a). However, it is useful to define α explicitly for practical reasons (even if this could be deduced from the proof of Hilbert's Theorem 90) - see Ex. 11.6.

Remark 11.2 Hilbert's theorem 90 is a specialization to cyclic groups of a more general result on **cohomology groups**. If G is a group and A is a $G-$module, then the first cohomology group $H^1(G, A)$ is the group of functions (with respect to the usual addition of functions) $f : G \to A$ such that $f(\sigma\sigma') = f(\sigma) + \sigma(f(\sigma'))$ called **1-cycles** modulo **1-boundaries**, which are 1-cocyles of the form: $f(\sigma) = a - \sigma(a)$ for some $a \in A$. In multiplicative notations, the 1-cocyles are $f : G \to A$ such that $f(\sigma\sigma') = f(\sigma)\sigma(f(\sigma'))$ and the 1-boundaries $f(\sigma) = \frac{a}{\sigma(a)}$ for some $a \in A$.

If we write $f(\sigma) = \alpha_\sigma$, then we recognize that in the proofs of **T.11.2**, we considered 1-cocycles $f : G \to K^*$ (**T.11.2** (a)) and $f : G \to K^+$ (**T.11.2**(b)) with suitable choices of α. The conditions defining 1-cocyle $a_{\sigma\sigma'} = \alpha_\sigma \sigma(\alpha_{\sigma'})$ are often called **Noether's equations** and Hilbert's Theorem 90 can be considered as a statement about solutions of these equations.

Using the notion of the first cohomology group, the statements of Hilbert's Theorem 90 are simply the claims that $H^1(G, K^*) = 1$ and $H^1(G, K^+) = 1$ (every 1-cocyle is 1-coboundary).

[1] This creates a conflict with the historically older use of the notion normal polynomial, which we introduced in Ex. 7.9. Usually it is possible to easily recognize which notion is discussed.

In fact, the same arguments as those given in the proof of **T.11.2** show that for any finite automorphism group G of K these two groups are trivial. The cohomology groups $H^n(G, A)$ are defined in a natural way for all integer n and the groups $H^n(G, K^+) = 1$ for all $n > 0$, while $H^n(G, K^*)$ are very interesting groups related to the field K.

As an illustration and application of some of the results in this chapter, we shall consider a class of field extensions which are splitting fields of arbitrary families of binomials $X^m - a$ where $a \in K$ and m is fixed. We exclude the case $a = 1$, that is, the case of cyclotomic fields, considered in chapter 10 assuming that the field K contains m *different* m-th roots of 1. This theory is known as (abelian) **Kummer theory**. Notice that the condition concerning roots of 1 simply says that the ground field K has characteristic 0 or its characteristic is relatively prime to m (see Ex. 5.10 (b)).

The **exponent** of any group G is the least positive integer m such that $\sigma^m = 1$ for all $\sigma \in G$. A Galois extension $K \subseteq L$ is called of exponent m if the exponent of its Galois group divides m. A Galois extension $K \subseteq L$ of exponent m is called a **Kummer extension** if it is abelian (that is, its Galois group is abelian) and the field K contains m different m-th roots of 1. The simplest example is a splitting field of a polynomial $X^m - a$ over such a field K. It is $L = K(\alpha)$, where α is any fixed zero of this polynomial (see Ex. 5.10). The Galois group $G(L/K)$ is abelian and $\sigma^m = 1$ for every automorphism $\sigma \in G(L/K)$ (see Ex. 9.20). A zero α of $X^m - a$ will be denoted by $\sqrt[m]{a}$. Even if this symbol may denote any of the m different zeros $\eta\alpha$, where η is m-th root of 1, the field $K(\sqrt[m]{a})$ is uniquely defined, since the factor η belongs to K. We denote by K^{*m} the subgroup of the multiplicative group $K^* = K \setminus \{0\}$ consisting of all $m-$th powers of nonzero elements in K.

The fundamental facts about Kummer extensions of exponent m are contained in the following theorem:

T. 11.4 *Let K be a field containing m different m-th roots of 1.*

(a) If $K \subseteq L$ is a Kummer extension of exponent m, then every subextension of fields $M \subseteq N$, where $K \subseteq M \subseteq N \subseteq L$ is also a Kummer extension.

(b) All Kummer extensions of K of exponent m are exactly the splitting fields of sets of binomial polynomials $X^m - a$ for some $a \in K$. In particular, all finite Kummer extensions of K are $L = K(\sqrt[m]{a_1}, \ldots, \sqrt[m]{a_r})$ for some elements $a_1, \ldots, a_r \in K$.

(c) There is a one-to-one correspondence between the isomorphism classes of finite Kummer extensions of K of exponent m and the subgroups A of K^* containing K^{*m} such that the index $[A : K^{*m}]$ is finite. In this correspondence, to a Kummer extension L of K corresponds the subgroup A of K^* consisting of all $a \in K$ such that $a = \alpha^m$ for some $\alpha \in L$, and to a subgroup A of K^* corresponds any splitting field over K of all binomials $X^m - a$ for $a \in A$. Moreover,

$$|G(L/K)| = [L : K] = [A : K^{*m}]. \tag{11.1}$$

EXERCISES 11

11.1. Construct a normal basis for each of the following field extensions:

(a) $\mathbb{Q}(i)$ over $\mathbb{Q}$;
(b) $\mathbb{Q}(\sqrt{2},\sqrt{3})$ over $\mathbb{Q}$;
(c) $\mathbb{Q}(\varepsilon)$, $\varepsilon^5=1, \varepsilon\neq 1$ over $\mathbb{Q}$;
(d) $\mathbb{F}_2(\gamma)$, $\gamma^3+\gamma^2+1=0$ over $\mathbb{F}_2$.

11.2. (a) Show that in a quadratic Galois extension $K\subset L$ an element $\alpha\in L$ is normal if and only if $\alpha\notin K$ and $\mathrm{Tr}(\alpha)\neq 0$ (see (6.1)).

(b) Show that in a cubic Galois extension $K\subset L$, where K is a real number field, an element $\alpha\in L$ is normal if and only if $\alpha\notin K$ and $\mathrm{Tr}(\alpha)\neq 0$. An open question: Can K in general be replaced by an arbitrary field?

11.3. (a) Let $K\subseteq L$ be a Galois extension and let $\alpha\in L$ be a normal element. Show that $L=K(\alpha)$, that is, a normal element is field primitive. Is the converse true?

(b) Let $K\subseteq L$ be finite fields. Is it true that the group primitive elements (that is, the generators of the cyclic group L^*) are normal? Is the converse true? (see Ex. 8.15).

11.4. (a) Let X,Y,Z be a Pythagorean triple, that is, an integer solution of the equation $X^2+Y^2=Z^2$ with positive and relatively prime X,Y,Z. Consider the complex number $\alpha=x+yi\in\mathbb{Q}(i)$, where $x=X/Z$ and $y=Y/Z$ and notice that $\mathrm{Nr}(\alpha)=1$ in $\mathbb{Q}(i)$. Use this observation together with Hilbert's Theorem 90 in order to find a formula for X,Y,Z.

(b) Find in a similar way a formula for integer solutions of the equation $X^2+2Y^2=Z^2$.

11.5. (a) Let K be a field containing n different n-th roots of 1. Using Kummer theory (**T.11.4**) show that if X^n-a, X^n-b are irreducible polynomials in $K[X]$, then $K(\sqrt[n]{a})=K(\sqrt[n]{b})$ if and only if there is r such that $0<r<n$, $\gcd(r,n)=1$ and $ba^{-r}\in K^{*n}$.

(b) Give a description of all quadratic extensions of the rational numbers $\mathbb{Q}$ using (a).

11.6. (a) Motivate that $E=\mathbb{Q}(\sqrt{-3})$ is the least number field containing the 3rd roots of 1, and show that every cubic Galois extension L of E there is $\alpha\in E$ such that $L=E(\sqrt[3]{\alpha})$. Show also that one can always choose $\alpha\in\mathbb{Z}[\varepsilon]$, where $\varepsilon=\frac{1+\sqrt{-3}}{2}$, that is, $\alpha=a+b\varepsilon$, $a,b\in\mathbb{Z}$.

(b) Show that there is a one-to-one correspondence between cyclic cubic extensions $K\supset\mathbb{Q}$ and the cyclic cubic extensions $L=EK$ of E such that $L\supset\mathbb{Q}$ is Galois with cyclic Galois group $\mathbb{Z}_6$. Show that two two cyclic cubic extensions K_1 and K_2 of $\mathbb{Q}$ are isomorphic if and only if the extensions $L_1=EK_1$ and $L_2=EK_2$ are isomorphic over E.

(c) Show that a cubic extension $L=E(\sqrt[3]{\alpha})$ of E ($\alpha\in E$), is a Galois extension of $\mathbb{Q}$ if and only if $\mathrm{Nr}(\alpha)=\alpha\bar{\alpha}\in\mathbb{Q}^{*3}$ or $\alpha\mathrm{Nr}(\alpha)\in\mathbb{Q}^{*3}$. In the first case the Galois group $G(L/\mathbb{Q})$ is the cyclic group $\mathbb{Z}_6$, and in the second, it is the symmetric group S_3.

(d) Motivate that $\alpha = f\bar{f}^2$, where $f \in \mathbb{Z}[\varepsilon]$ satisfies the condition $\mathrm{Nr}(\alpha) = \alpha\bar{\alpha} \in \mathbb{Q}^{*3}$ in (c). Show that $\mathbb{Q}(\gamma)$, where $\gamma = \sqrt[3]{\alpha} + \sqrt[3]{\bar{\alpha}}$, is a Galois cubic extension of $\mathbb{Q}$ and find the minimal polynomial of γ over $\mathbb{Q}$. Give a few examples of cyclic cubic extensions $K \supset \mathbb{Q}$.

11.7. (a) Let $E = \mathbb{Q}(i)$. Show that for every cyclic quartic Galois extension L of E there is $\alpha \in E$ such that $L = E(\sqrt[4]{\alpha})$. Show also that one can always choose $\alpha \in \mathbb{Z}[i]$, that is, $\alpha = a + bi$, $a, b \in \mathbb{Z}$.

(b) Show that there is a one-to-one correspondence between pairs of cyclic quartic extensions $K_1 \supset \mathbb{Q}$, $K_2 \supset \mathbb{Q}$, where K_1 is a real and K_2 is non-real, and the cyclic quartic extensions $L = EK_1 = EK_2$ of E such that $L \supset \mathbb{Q}$ is Galois with Galois group $\mathbb{Z}_2 \times \mathbb{Z}_4$. Show that two cyclic quartic extensions K_1 and K_2 of $\mathbb{Q}$ are isomorphic if and only if both are real or both are non-real and the extensions $L_1 = EK_1$ and $L_2 = EK_2$ are isomorphic over E.

(c) Show that a quartic extension $L = E(\sqrt[4]{\alpha})$ of E ($\alpha \in E$), is a Galois extension of $\mathbb{Q}$ if and only if $\mathrm{Nr}(\alpha) = \alpha\bar{\alpha} \in \mathbb{Q}^{*4}$ or $\alpha^2\mathrm{Nr}(\alpha) \in \mathbb{Q}^{*4}$. In the first case the Galois group $G(L/\mathbb{Q})$ is the group $\mathbb{Z}_2 \times \mathbb{Z}_4$, and in the second, it is the dihedral group D_4 (the symmetry group of a square).

(d) Motivate that $\alpha = f\bar{f}^3g^2$, where $f \in \mathbb{Z}[i]$ and $g \in \mathbb{Q}^*$ satisfies the condition $\mathrm{Nr}(\alpha) = \alpha\bar{\alpha} \in \mathbb{Q}^{*4}$ from (c). Show that $\mathbb{Q}(\gamma)$, where $\gamma = \sqrt[4]{\alpha} + \sqrt[4]{\bar{\alpha}}$, $\sqrt[4]{\alpha}\sqrt[4]{\bar{\alpha}} = \mathrm{Nr}(f)|g|$, is a cyclic quartic extension of $\mathbb{Q}$ (real if $g > 0$, non-real if $g < 0$) and find the minimal polynomial of γ over $\mathbb{Q}$. Give a few examples of cyclic quartic extensions $K \supset \mathbb{Q}$.

11.8. Let K be a field of prime characteristic p and let L be a Galois field extension of K of degree p. Show that $L = K(\alpha)$, where α is a zero of a polynomial $X^p - X - a$ for some $a \in K$ (compare Ex. 9.24).

Remark. The polynomial $X^p - X - a$ over a field K of characteristic p is often called an **Artin-Schreier polynomial**, and $K \subset L$ is called an **Artin-Schreier extension**. The description of cyclic Galois extensions of degree p given in the exercise above is called Artin-Schreier theorem. Such extensions play an important role, for example, in the Kummer theory and in the study of radical extensions over fields of characteristic p (see Chap. 13 for characteristic 0). See also Ex. XXX.

11.9. Let $K \subset L$ be a finite field extension and L an algebraically closed field. Show that $[L : K] = 2$.

Remark. This is a part of the Artin-Schreier theorem, which says that that not only an algebraically closed field of finite degree > 1 over its subfield has in fact degree 2, but also that K must be a real field (that is, -1 is not a sum of squares in K), which is really closed (that is, there is no bigger real field containing it) and $L = K(i)$, where $i^2 = -1$. For a proof of this last part of the Artin-Schreier theorem see [Lang,xxx]. The best known example of this situation is the extension $\mathbb{R} \subset \mathbb{C}$.

11.10. Use Ex. 11.6, respectively Ex. 11.7, in order to write Maple procedures, which list cubic, respectively quartic, polynomials with integer coefficients whose Galois groups are cyclic of order 3, respectively 4.

12

Solvable groups

As a preparation for the next chapter in which we discuss solvability of equations by radicals, we need som knowledge about solvable groups.

A group G is called **solvable** if there exists a chain of groups:

$$G = G_0 \supset G_1 \supset \ldots \supset G_n = \{e\}$$

such that G_{i+1} is normal in G_i and the quotients G_i/G_{i+1} are abelian for $i = 0, 1, \ldots, n-1$.

T. 12.1 (*a*) *If G is solvable and H is a subgroup of G, then H is solvable.*

(*b*) *If N is a normal subgroup of G and G is solvable, then the quotient group G/N is solvable.*

(*c*) *If N is a solvable normal subgroup of G such that the quotient group G/N is solvable, then G is solvable.*

We look at several examples of solvable and some non-solvable groups in exercises below. In particular, we look at solvable and non-solvable subgroups of the permutation groups. By the permutation group S_n, we mean the group of all bijective functions on a set X with n elements. Usually, we choose $X = \{1, 2, \ldots, n\}$, but sometimes other choices are more suitable. The following result is usually used in the proof that among algebraic equations of degrees at least 5, there are equations not solvable by radicals:

T. 12.2 *The symmetric group S_n is not solvable when $n \geq 5$.*

EXERCISES 12

12.1. Show that the following groups are solvable:

(a) Every abelian group G.

(b) The group $G = S_3$ (this group may be considered as the group of all symmetries of an equilateral triangle – see (c)).

(c) The group $G = S_4$ (this group may be considered as the group of all symmetries of a regular tetrahedron).

(d) The dihedral group D_n of all symmetries of a regular polygon with n sides for $n = 3, 4, \ldots$ (for definition of D_n, see the Remark after Ex. 12.4).

(e) The group $\mathbb{H}^*(\mathbb{Z})$ of quaternion units $\pm 1, \pm i, \pm j, \pm k$, where $i^2 = j^2 = -1, ij = k$ and $ji = -ij$.

Remark. According to the famous Feit-Thompson Theorem (proved by Walter Feit and John G. Thompson in 1962 and conjectured by William Burnside in 1911), every finite group of odd order is solvable. As a rather long exercise, one can prove that every group of order less than 60 is solvable. The least non-solvable group is the group A_5 (of order 60) of all even permutations of numbers $1, 2, 3, 4, 5$ (see Ex. 12.2).

12.2. The aim of this exercise is to show that every alternate group A_n, where $n \geq 5$ is not solvable.

(a) Let G be a subgroup of the group A_n, where $n \geq 5$ and N a normal subgroup of G such that G/N is abelian. Show that if G contains every cycle (a, b, c), then also N contains every such cycle.

(b) Deduce from (a) that the group A_n for $n \geq 5$ is not solvable.

(c) Why the symmetric groups S_n, $n \geq 5$ are not solvable?

12.3. (a) Show that a group G is solvable if and only if there exists a chain of groups:

$$G = G_0 \supset G_1 \supset \ldots \supset G_n = \{e\}$$

such that G_{i+1} is normal in G_i and the quotient group G_i/G_{i+1} is cyclic of prime order for $i = 0, 1, \ldots, n-1$.

(b) Show that a solvable group whose order is not a prime number contains a nontrivial normal subgroup (a normal subgroup different from the identity and the whole group).

12.4. Denote by $\mathcal{G}_n$ the set of all functions $\varphi_{a,b} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, where $\varphi_{a,b}(x) = ax + b$, $a, b \in \mathbb{Z}/n\mathbb{Z}$, $a \in (\mathbb{Z}/n\mathbb{Z})^*$ and by $\mathcal{T}_n$ all translations $\varphi_{1,b}(x) = x + b$.

(a) Motivate that the functions $\varphi_{a,b}(x)$ are bijections on the set $\{0, 1, \ldots, n-1\}$ and as such can be considered as permutations belonging to the group S_n of all permutations of this set (with n elements).

(b) Show that $\mathcal{G}_n$ is a subgroup of S_n of order $n\varphi(n)$, where $\varphi(n)$ is the Euler function.

(c) Define $\Phi : \mathcal{G}_n \to (\mathbb{Z}/n\mathbb{Z})^*$ such that $\Phi(\varphi_{a,b}) = a$. Show that Φ is a surjective group homomorphism, whose kernel is $\mathcal{T}_n$. Motivate that $\mathcal{G}_n$ is solvable.

(d) Let p be a prime number. Show that $\mathcal{G}_p$ is transitive on the set $\{0, 1, \ldots, p-1\}$ and that every $\varphi_{a,b} \in \mathcal{G}_n$, $\varphi_{a,b} \neq \varphi_{1,0}$, has at most one fix point $x \in \mathbb{Z}/p\mathbb{Z}$.

(e) If p is a prime number prove that $\mathcal{G}_p$ has exactly one subgroup of order p – the subgroup $\mathcal{T}_p$ consisting of all translations $\varphi_{1,b}$, $b = 0, 1, \ldots, p-1$, which is generated by $\varphi_{1,1}$. Show that $\mathcal{T}_p$ contains all elements of order p in $\mathcal{G}_p$.

(f) Show that $\mathcal{G}_n$ is isomorphic to the group consisting of the matrices

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix},$$

where $a \in (\mathbb{Z}/n\mathbb{Z})^*$, $b \in \mathbb{Z}/n\mathbb{Z}$ with respect to matrix multiplication. Notice that the determinant:

$$\det : \mathcal{G}_n \to (\mathbb{Z}/n\mathbb{Z})^*$$

is a surjective group homomorphism (in (b) was denoted by Φ) and that the kernel of this homomorphism is the subgroup isomorphic to $\mathcal{T}_n$ and consisting of matrices with $a = 1$. Check that the group $\mathcal{G}_n$ acts on the set of the column vectors $[x, 1]^t, x \in \mathbb{Z}/n\mathbb{Z}$ (that is, maps by matrix multiplication a vector of this type on a vector of this type again) and, when $n = p$ is a prime, then every matrix has at most one fix vector $[x, 1]^t$ (compare to (e)).

Ramark. The subgroup of $\mathcal{G}_n$ ($n > 2$) consisting of matrices with $a = \pm 1$ is called the **dihedral group** (of order $2n$). It is often denoted by D_n.

12.5. Let G be a transitive subgroup of the symmetric group S_p on a set X with p elements. Show that the following conditions are equivalent:

(a) G is solvable;

(b) Each different from identity element of G fixes at most one element of X;

(c) The group G is conjugated to a subgroup of $\mathcal{G}_p$ containing $\mathcal{T}_p$ (for notations see Ex. 12.4).

In order to prove (a)–(c) show the following two facts:

(d) The order of any transitive group G on a set X with p elements is divisible by p.

(e) If H is a subgroup of a transitive group G on a set X with p elements, then H is also transitive on X or every element of H acts as the identity on X.

12.6. Show that every $p-$group, that is, a group whose order is a power of a prime, is solvable.

Remark. A famous result proved by William Burnside in 1904 says that if the order of a finite group is divisible by at most two prime numbers, then the group is solvable.

13

Solvability of equations

Throughout this chapter, we assume that all fields have characteristic 0. A field extension $L \supseteq K$ is called **radical** if there is a chain of fields

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n = L \tag{13.1}$$

such that $K_i = K_{i-1}(\alpha_i)$, where $\alpha_i^{r_i} \in K_{i-1}$ and r_i are positive integers for $i = 1, \ldots, n-1$. We say that an equation $f(X) = 0$, $f \in K[X]$ is **solvable by radicals** over K if the splitting field K_f of $f(X)$ over K is contained in a radical extension $L \supseteq K$. In general, we say that an extension $K \subseteq L$ is **solvable** (by radicals) if L is a subfield of a radical extension of K (so $f(X) = 0$ is solvable by radicals over K says that K_f is a solvable extension of K). We say that an equation $f(X) = 0$, $f \in K[X]$, where K is a subfield of the real numbers $\mathbb{R}$, is **solvable by real radicals** if the splitting field of $f(X)$ over K is contained in a radical extension $L \supseteq K$ such that $L \subset \mathbb{R}$.

T. 13.1 *An equation $f(X) = 0$, $f \in K[X]$ is solvable by radicals if and only if the Galois group of f over K is solvable.*

The **general equation** of degree n over K is

$$f(X) = \prod_{i=1}^{n}(X - X_i) = X^n - s_1 X^{n-1} + s_2 X^{n-2} + \ldots + (-1)^n s_n = 0,$$

where s_i are the elementary symmetric functions of $X_1, X_2, \ldots, X_n$, that is, $s_1 = \sum X_i$, $s_2 = \sum X_i X_j, \ldots, s_n = X_1 X_2 \ldots X_n$.

T. 13.2 *The Galois group over $K(s_1, s_2, \ldots, s_n)$ of the general equation $f(X) = 0$ of n-th degree is S_n, so $f(X) = 0$ is not solvable by radicals when $n \geq 5$.*

This result is a consequence of **T.13.1** taking into account that the symmetric groups S_n are not solvable for $n \geq 5$. It is not difficult to construct rational polynomials $f(X)$ of degree

5 having the symmetric group S_5 as its Galois group. According to the same result, the equations $f(X) = 0$ are not solvable by radicals (see several exercises below).

Another famous result is concerned with a surprising phenomenon related to irreducible (rational) cubic polynomials (and also, polynomials of higher degrees) – even if such a polynomial has real coefficients and 3 real zeros, the formulae expressing these zeros (like Cardano's formulae (1.5) in Chapter 1) can not contain only real radicals. This follows from the following fact:

T. 13.3 (**Casus irredicibilis**) *Let $f(X)$ be an irreducible polynomial having 3 real zeros and coefficients in a real number field K. Then $f(X)$ is not solvable by real radicals over the field K.*

EXERCISES 13

13.1. Show that $L \supset \mathbb{Q}$ is a radical extensions when:

(a) $L = \mathbb{Q}(\sqrt[5]{1+\sqrt{3}})$; (b) $L = \mathbb{Q}(\sqrt[3]{1-\sqrt{5}}, \sqrt[7]{\sqrt{2}+\sqrt{3}})$.

13.2. Argue that the following equations are solvable by radicals over $\mathbb{Q}$ (without solving these equations):

(a) $X^4 - 4X^2 - 21 = 0$; (b) $X^6 - 2X^3 - 2 = 0$.

13.3. Show that in the definition of an equation solvable by radicals, we can always assume that in the chain (13.1) the degrees r_i of the consecutive extensions $K_{i-1} \subset K_i$ are prime numbers.

13.4. Let p be a prime number and K a real number field.

(a) Prove Weber's theorem: If $f \in K[X]$ is an irreducible polynomial of degree p with $p-2$ real and 2 complex non-real zeros, then its Galois group is S_p.

(b) Show that the equation $X^5 - p^2X - p = 0$, p a prime number, is not solvable by radicals over $\mathbb{Q}$.

(c) Show that the polynomial $f(X) = (X^2+4)(X-2)(X-4)\cdots(X-2(p-2)) + 2$ is irreducible and has exactly $p-2$ real zeros (hence its Galois group is S_p according to (a)).

13.5. For every $n \geq 5$ give an example of a polynomial equation $f(X) = 0$ over $\mathbb{Q}$ whose degree is n and which is not solvable by radicals.

13.6. The aim of this exercise is a direct proof (using only the definition of solvability by radicals, but without Galois theory and the relation between solvable equations and solvable groups) that any polynomial equation $f(X) = 0$, where $f(X) \in \mathbb{Q}[X]$ is irreducible and has

3 real and 2 non-real (conjugated) complex roots is not solvable by radicals over $\mathbb{Q}$. Let $f(X)$ be such a polynomial and assume that there is a chain of fields

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n = L$$

such that $K_i = K_{i-1}(\alpha_i)$, where $\alpha_i^{r_i} \in K_{i-1}$, the exponents r_i are prime numbers (see Ex. 13.3) for $i = 1, \ldots, n-1$ and the splitting field of $f(X)$ over $\mathbb{Q}$ is contained in L. Of course, the polynomial $f(X)$ has a factorization over $K_n = L$. Choose the least $i < n$ such that $f(X)$ is irreducible in K_{i-1} but reducible in K_i. In the exercise, we want to show that this is impossible, that is, $f(X)$ must be still irreducible over K_i. This contradiction shows that $f(X) = 0$ can not be solvable by radicals.

(a) Using Nagell's Lemma (see Ex. 4.2) show that $[K_i : K_{i-1}] = 5$, where $K_i = K_{i-1}(\alpha_i)$, $\alpha_i^5 = a_i \in K_{i-1}$.

(b) Show that $f(X)$ is irreducible over K_i.

13.7. Motivate that every equation $f(X) = 0$ of degree $\deg(f) \leq 4$, where $f \in K[X]$, is solvable by radicals.

13.8. Show that the equation $f(X) = 0$ is solvable in radicals over K if and only if the equation $f(X^n) = 0$ is solvable by radicals over K ($n \geq 1$ a natural number).

13.9. Prove Galois' theorem: An irreducible polynomial equation of prime degree p over a number field is solvable by radicals if and only if its splitting field is generated by any two of its zeros.

(a) Let $f(X)$ be a polynomial of degree p over a number field K and let L be its splitting field over K. Show that L is generated by two of the zeros of $f(X)$ if and only if each non-trivial automorphism in $G(L/K)$ has at most one fixed point as a permutation of the zeros of $f(X)$. Motivate that the group $G(L/K)$ is transitive (see Ex. 6.2).

(b) Prove Galois' theorem considering $G(L/K)$ as a subgroup of S_p (see p. 30) and using Ex. 12.5.

13.10. Let $f(X) \in K[X]$ be an irreducible polynomial of prime degree $p > 2$ over a real number field K (that is, $K \subset \mathbb{R}$). Using Galois' Theorem (see Ex. 13.9) show that if the equation $f(X) = 0$ is solvable by radicals, then $f(X)$ has exactly one or p real zeros. Notice that this result gives an alternative solution of Ex. 13.4.

13.11. Let $f(X)$ be an irreducible polynomial of degree 5 over the rational numbers and $\Delta(f)$ its discriminant (see p. 258).

(a) Show that if $\Delta(f) < 0$, then the equation $f(X) = 0$ is not solvable by radicals.

(b) Show that there are both solvable and unsolvable equations $f(X) = 0$ over K with $\Delta(f) > 0$.

13.12. Show that the general cubic equation $f(X) = X^3 - s_1X^2 + s_2X - s_3 = 0$ over the field $K = \mathbb{Q}(\varepsilon, s_1, s_2, s_3)$, where $\varepsilon^3 = 1, \varepsilon \neq 1$, is solvable by radicals constructing a suitable chain of fields (13.1) between $K_0 = K$ and $L = K(X_1, X_2, X_2)$ ($s_1 = X_1 + X_2 + X_3$, $s_2 = X_1X_2 + X_2X_3 + X_3X_1$, $s_3 = X_1X_2X_3$).

13.13. Show that if an equation $f(X) = 0$, $f \in K[X]$, where K is a subfield of the real numbers $\mathbb{R}$, is solvable by real radicals, then the degree of its splitting field $L \subseteq \mathbb{R}$ over K is a power of 2.

13.14. Show that the field of complex numbers is algebraically closed in the following steps:

(a) If K is a Galois extension of $\mathbb{R}$ and the degree $[K : \mathbb{R}]$ is odd, then $K = \mathbb{R}$.

(b) If K is a quadratic extension of $\mathbb{R}$, then $K = \mathbb{C}$, while there are no quadratic extensions of the field $\mathbb{C}$.

(c) If K is a Galois extension of $\mathbb{C}$ (a splitting field of an irreducible polynomial over $\mathbb{C}$), then there is a field containing it, which is a Galois extension over $\mathbb{R}$. Using (a) and (b) show that this field containing K is equal $\mathbb{C}$ (so $K = \mathbb{C}$).

14

Geometric constructions

Let X be an arbitrary set of points in the plane containing $(0,0)$ and $(1,0)$.

- A line is defined by X if it goes through two points belonging to X.
- A circle is defined by X if its center belongs to X and its radius equals to the distance between two points belonging to X.

We say that a point $P=(a,b)$ **can be directly constructed** from X by using a straightedge and a compass (a straightedge-and-compass or ruler-and-compass construction) if P is an intersection point of two lines or two circles or a line with a circle, which are defined by X. Let X_1 be the set of all points in the plane, which can be directly constructed from $X=X_0$, X_2 the set of all points which can be directly constructed from X_1, X_3 the set of all points which can be directly constructed from X_2 ans so on. We say that a point $P=(a,b)$ **can be constructed from** X by a straightedge-and-compass construction if $P\in X^\star=\bigcup_{i=0}^{\infty}X_i$ (that is, $P\in X_i$ for some $i\geq 0$). We say shortly that X^* is the set of points constructible from X.

One also defines **real numbers constructible** from X as such $r\in\mathbb{R}$ that $|r|=$ the distance between two points constructible from X.

Very often one takes $X=\{(0,0),(1,0)\}$. Those numbers which can be constructed from $X=\{(0,0),(1,0)\}$ will be denoted by $\mathbb{K}$. The least number field which contains the coordinates of $(0,0)$ and $(1,0)$ is of course $\mathbb{Q}$. The constructible lines through $(0,0),(1,0)$ and $(0,0),(0,1)$ (it is easy to see that the point $(0,1)$ is constructible from $(0,0)$ and $(1,0)$) are, as usual, called the **axis**.

T. 14.1 *Let K be the least subfield to $\mathbb{R}$ which contains the coordinates of all points belonging to a given set of points X in the plane. A point $P=(a,b)$ can be constructed from X by a straightedge-and-compass construction if and only if there is a chain of fields:*

$$K=K_0\subset K_1\subset\ldots\subset K_n=L\subset\mathbb{R} \qquad (*)$$

such that $a, b \in L$ *and* $[K_{i+1} : K_i] = 2$ *for* $i = 0, 1, \ldots, n-1$. *In particular, the set of numbers which are constructible from* X (*like* $\mathbb{K}$ *when* $X = \{(0,0),(1,0)\}$) *is a field.*

In practise, one uses this theorem when one wants to show that a point $P = (a, b)$ is not constructible – one shows that $[K(a, b) : K]$ is not a power of 2. If one wants to show that a point can be constructed one uses often the following theorem:

T. 14.2 *Let* K *be the least subfield of* $\mathbb{R}$ *which contains the coordinates of all points belonging to a point set* X *in the plane* $\mathbb{R}^2$. *A point* $P = (a, b)$ *can be constructed from* X *by a straightedge-and-compass construction if and only if one of the following equivalent conditions hold:*

(*a*) *There exists a Galois extension* $L \supseteq K$ *such that* $a, b \in L$ *and* $[L : K]$ *is a power of* 2.

(*b*) *There exists a Galois extension* $L \supseteq K$ *such that* $a + bi \in L$ *and* $[L : K]$ *is a power of* 2.

In the following exercises, the terms "to construct" or "can be constructed" should be understood as constructed by using a straightedge and a compass. We always start from a set X, which contains $(0, 0)$ and $(1, 0)$.

EXERCISES 14

14.1. Show that the following geometric constructions are impossible:

(a) to construct a cube of volume 2 when a cube of volume 1 is given, that is, to construct a segment of length $\sqrt[3]{2}$ when a segment of length 1 is given ("doubling of a cube");

(b) to construct the angle $20°$ when the angle $60°$ is given ("trisection of an angle");

(c) to construct a square of area π when a disk of area π (that is, of radius 1) is given ("squaring of a circle").

14.2. Let X be a set of points in the plane. Prove that $P = (a, b)$ can be constructed from X if and only if its coordinates can be constructed from X.

14.3. (a) Is it possible to construct a disk whose area is equal to the sum of the areas of two given disks?

(b) Is it possible to construct a sphere whose volume is equal to the sum of the volumes of two given spheres?

14.4. Is it possible to construct a square whose area is equal to the area of a given triangle?

14.5. Is it possible to construct a cube whose volume is equal to the volume of a regular tetrahedron whose sides are equal to 1?

14.6. Prove the following **theorem of Gauss**: A regular polygon with n sides is constructible (by straightedge-and-compass construction) when a segment of length 1 is given if and only if $n = 2^r$, $r \geq 2$ or $n = 2^r p_1 p_2 \dots p_s$, $r \geq 0$, $s \geq 1$ and p_i are different Fermat primes (p is a Fermat prime when $p = 2^{2^t} + 1$, $t \geq 0$):

(a) If $k|n$ and a regular polygon with n sides is constructible, then a regular polygon with k sides is constructible;

(b) If $n = kl$, where k and l are relatively prime, then a regular polygon with n sides is constructible if and only if regular polygons with k sides and l sides are constructible;

(c) If $n = 2^r$, $r \geq 2$, then a regular polygon with n sides is constructible;

(d) If $n = p^2$, where p is an odd prime, then a regular polygon with n sides is not constructible;

(e) If $n = p$, where p is an odd prime, then a regular polygon with n sides is constructible if and only if p is a Fermat prime.

14.7. Construct a regular polygon with n sides when $(0, 0)$ and $(1, 0)$ are given if

(a) $n = 5$; (b) $n = 15$; (c) $n = 20$.

14.8. Which of the following angles α can be constructed when $(0, 0)$ and $(1, 0)$ are given:

(a) $\alpha = 1°$; (b) $\alpha = 3°$; (c) $\alpha = 5°$.

14.9. Give an example of an angle α which is not constructible when $(0, 0)$ and $(1, 0)$ are given, but which can be trisected when this angle is given (an angle is given if three different points $(0, 0), (1, 0)$ and (a, b) are given defining the rays from $(0, 0)$ through $(1, 0)$ and (a, b)).

15

Computing Galois groups

In earlier chapters, we had several opportunities of finding Galois groups of specific polynomials. In general, computing the Galois group of a given polynomial over a given field is numerically complicated when the degree of the polynomial is already modestly high. For polynomials of (very) low degrees it is possible to specify some numerical invariants, which tell us about the isomorphism type of the Galois group depending on the values of these invariants. For arbitrary polynomials there is a variety of numerical methods, which for not too high degrees make the computational task possible to implement in more or less effective way. There are several computer packages in which Galois groups of irreducible polynomials up to varying degrees can be computed, notably, Maple, GP/Pari, Sage and Magma.

Let K be a field and $F(X_1,\dots,X_n) \in K(X_1,\dots,X_n)$ a rational function in n variables $X_1,\dots,X_n$. The symmetric group S_n acts as an automorphism group of the field $K(X_1,\dots,X_n)$ when for $\sigma \in S_n$:

$$\sigma F(X_1,\dots,X_n) = F(X_{\sigma(1)},\dots,X_{\sigma(n)})$$

and σ is a permutation of $\{1,\dots,n\}$. Let G be a subgroup of S_n. We denote by G_F **the stabilizer of** F **in** G, that is, $G_F = \{\sigma \in G \mid \sigma F = F\}$.

T. 15.1 (*a*) *Let G be a subgroup of S_n. Then for every subgroup H of G there exists a polynomial $F \in K[X_1,\dots,X_n]$ such that $H = G_F$.*

(*b*) *Let $G = \sigma_1 G_F \cup \cdots \cup \sigma_m G_F$ be the presentation of G as a union of different left cosets with respect to G_F. Then $\sigma_i F(X_1,\dots,X_n)$ for $i = 1,\dots,m$ are all different images of F under the permutations belonging to G.*

Let $f(X) \in K[X]$ be a polynomial of degree n and $L = K_f = K(\alpha_1,\dots,\alpha_n)$ its splitting field over K, where α_i are all the zeros of $f(X)$ in L taken in an arbitrarily fixed order. Assume that $\mathrm{Gal}(K_f/K) \subseteq G$, where the Galos group of $f(X)$ over K is considered as a group of permutations of $\{1,\dots,n\}$ in the usual way: $\sigma(\alpha_i) = \alpha_{\sigma(i)}$ (this means that we use the same symbol σ to denote the permutation $\sigma \in \mathrm{Gal}(K_f/K)$ of the zeros of $f(X)$ in K_f

and the corresponding permutation on the set of the indices of these zeros). From now on, we assume that $F(X_1, \ldots, X_n)$ is a polynomial.

By a **general polynomial** with respect to a subgroup $G \subseteq S_n$ and $F(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$, we mean the polynomial:

$$r_{G,F}(T) = \prod_{i=1}^{m} (T - (\sigma_i F)(X_1, \ldots, X_n)), \tag{15.1}$$

where the product is over a set σ_i, $i = 1, \ldots, m$, of representants of all left cosets of G_F in G. Of course, $\sigma_i F$ does not depend on the choice of a representant of $\sigma_i G_F$, since $\sigma_i \tau F = \sigma_i F$, when $\tau \in G_F$. We usually omit G in $r_{G,F} \in K[X_1, \ldots, X_n, T]$, when $G = S_n$. If $G = S_n$ and $F(X_1, \ldots, X_n) = X_1$, then $r_{G,F}(T)$ is the general polynomial of degree n as defined on p. 67.

Let $f(X) \in K[X]$ be a polynomial with the zeros $\alpha_1, \ldots, \alpha_n$ in a field extension of K. By a **resolvent polynomial** of $f(X)$ with respect to a subgroup $G \subseteq S_n$ and $F(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$, we mean the polynomial

$$r_{G,F}(f)(T) = \prod_{i=1}^{m} (T - (\sigma_i F)(\alpha_1, \ldots, \alpha_n)). \tag{15.2}$$

The values $(\sigma_i F)(\alpha_1, \ldots, \alpha_n))$ are obtained by a homomorphism of $K[X_1, \ldots, X_n]$ onto $K[\alpha_1, \ldots, \alpha_n]$ sending X_i onto α_i. Notice that these values need not be different. They generate over K a subfield of K_f, which plays an important role in studies of the Galois group $\mathrm{Gal}(K_f/K)$, in particular, through the following result:

T. 15.2 *Let $f(X) \in K[X]$, $F(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$ and assume that $\mathrm{Gal}(K_f/K) \subseteq G$, where G is a subgroup of S_n. Then:*

(a) The resolvent polynomial $r_{G,F}(f)$ has its coefficients in K;

(b) If all the zeros of $r_{G,F}(f)$ are different, then $\mathrm{Gal}(K_f/K)$ is conjugated in G to a subgroup of G_F if and only if at least one of the zeros of $r_{G,F}(f)$ belongs to K.

Even if the assumptions above are not satisfied, the splitting field of the resolvent $r_{G,F}(f)$ in K_f and the degrees of irreducible factors of the resolvent very often give information about the Galois group $\mathrm{Gal}(K_f/K)$ (see the exercises below).

Remark 15.1 If in **T.15.2**, we have $K = \mathbb{Q}$, $F(X_1, \ldots, X_n) \in \mathbb{Z}[X_1, \ldots, X_n]$ and $f(X) \in \mathbb{Z}[X]$ has the highest coefficient 1, then $r_{G,F}(f)(T)$ is a polynomial with integer coefficients. A proof of this property can be given in broader context of integers in arbitrary (number) fields but, unfortunately, we can not present it here (troszke rozwinac, czy potrzebne?).

There exists a general algorithmic procedure for finding the isomorphism type of the Galois group $\mathrm{Gal}(K_f/K)$, which uses **T.15.2** and was already known to Galois. Unfortunately,

the value of this procedure for practical computations is rather limited. We describe it for two reasons. First of all, it shows that the Galois group of any polynomial can be found if the zeros of it are known (over number fields, it is often sufficient to know the zeros with appropriate precision). On the other hand, we will use it in the proof of Dedekind's Theorem (**T.15.4**), which gives a very good method for computing of Galois groups in many situations.

Consider a field k and let $K = k(Y_1, \ldots, Y_n)$ be the field of rational functions of Y_i. In the field $K(X_1, \ldots, X_n)$ of rational functions of X_i take the polynomial

$$F(X_1, \ldots, X_n) = X_1Y_1 + \cdots + X_nY_n.$$

Let $f(X) \in k[X]$ and let $k_f = k(\alpha_1, \ldots, \alpha_n)$ be a splitting field of $f(X)$ over k. Then $K_f = k_f(Y_1, \ldots, Y_n)$ is a splitting field of $f(X) \in K[X]$ over K and $\mathrm{Gal}(K_f/K) \cong \mathrm{Gal}(k_f/k)$ (see Ex. 15.9). In the notations of **T.15.2**, choose $G = S_n$. It is clear that $G_F \subset S_n$ consists of only the identity permutation. The resolvent of $f(X)$ with respect to $G = S_n$ and $F(X_1, \ldots, X_n)$ is:

$$r_{G,F}(f)(T) = \prod_{\sigma \in S_n} (T - (\alpha_{\sigma(1)}Y_1 + \cdots + \alpha_{\sigma(n)}Y_n))$$

This polynomial has degree $n!$ and is a product of irreducible polynomials $r_i(T, Y_1, \ldots, Y_n)$ in $k[T, Y_1, \ldots, Y_n]$:

$$r_{G,F}(f)(T) = r_1(T, Y_1, \ldots, Y_n) \cdots r_t(T, Y_1, \ldots, Y_n). \tag{15.3}$$

The polynomials r_i are called **Galois resolvents** of $f(X)$. We will assume that r_1 is the polynomial having $\theta = \alpha_1Y_1 + \cdots + \alpha_nY_n$ as its zero.

T. 15.3 *The Galois group* $\mathrm{Gal}(k_f/k)$ *is isomorphic to any group* G_{r_i} *of those permutations of* $Y_1, \ldots, Y_n$ *which map* $r_i(X, Y_1, \ldots, Y_n)$ *onto itself for* $i = 1, \ldots, t$. *Moreover, all* $r_i(T, Y_1, \ldots, Y_n)$ *have the same degree* $[k_f : k]$ *with respect to* T *and they have a common splitting field* $K_f = k_f(Y_1, \ldots, Y_n)$ *over* $K = k(Y_1, \ldots, Y_n)$.

Another, often very effective technique for description of the Galois groups of polynomials, in particular, over number fields, uses a result proved by Dedekind. This is also a very general method, but in the case of number fields there is usually a lot of arithmetical information, which can be used in order to determine the Galois groups. Therefore, we formulate a special case of Dedekind's theorem in the case of the integers $\mathbb{Z}$.

Let $\varphi : R \to R^*$ be a ring homomorphism mapping an integral domain R into an integral domain R^*. Let K and K^* be fields of quotients of R and R^*, respectively. Let $f \in R[X]$ be separable (that is, without multiple zeros). Denote by f^* the image of f under the homomorphism extending φ to $R[X]$ by applying φ to the coefficients of the polynomials in $R[X]$. Such an extension is sometimes called **reduction modulo** φ, since the simplest example is the homomorphism $\varphi : \mathbb{Z} \to \mathbb{F}_p$ of reduction modulo a prime p.

T. 15.4 (**Dedekind**) (*a*) *Let* $f \in R[X]$ *be a separable monic polynomial and assume that its image* $f^* \in R^*[X]$ *is also separable and* $\deg(f) = \deg(f^*) = n$. *Then the Galois group of* f^* *over* K^* *has an embedding into the Galois group of* f *over* K.

(*b*) *Let in* (*a*), $R = \mathbb{Z}$, $R^* = \mathbb{F}_p$ *and let* $\varphi : \mathbb{Z} \to \mathbb{F}_p$ *be the reduction modulo a prime number* p. *If* $f \in \mathbb{Z}[X]$ *and*

$$f^* = f_1^* \cdots f_k^*,$$

where f_i^* *are irreducible over* $\mathbb{F}_p$, *then* $\mathrm{Gal}(\mathbb{Q}_f/\mathbb{Q})$ *considered as a permutation subgroup of* S_n *contains a permutation which is a product of cycles of length* $\deg(f_i{}^*)$ *for* $i = 1, \ldots, k$.

Usual proofs of the first part of this theorem use the relation between Galois groups and the Galois resolvents of f and f^*. Even if it is possible to give a proof relying on the properties of rings, we choose the "old fashioned" proof using Galois' resolvents (see **T.15.3**). A proof in the modern language can be found in [L], Chap.VII, §2.

EXERCISES 15

15.1. Consider $f(X) = X^3 + pX + q \in K[X]$ with zeros $\alpha_1, \alpha_2, \alpha_3$ in some extension of the field K, where $\mathrm{char}(K) \neq 2$. Let $\Delta = \Delta(f) = (\alpha_1 - \alpha_2)^2(\alpha_2 - \alpha_3)^2(\alpha_3 - \alpha_1)^2 = -4p^3 - 27q^2$ be the discriminant of $f(X)$ (see Ex. 1.3).

(a) Show that $K_f = K(\alpha_1, \alpha_2, \alpha_3) = K(\sqrt{\Delta}, \alpha_1)$ and if $f(X)$ is irreducible in $K[X]$, then its Galois group is isomorphic to C_3 or S_3 depending on $\sqrt{\Delta} \in K$ or $\sqrt{\Delta} \notin K$.

(b) In the notations of **T.15.2**, choose $G = S_3$ and $F(X_1, X_2, X_3) = (X_1 - X_2)(X_2 - X_3)(X_3 - X_1)$. Show that $G_F = A_3$ and $r_{G,F}(f) = X^2 - \Delta(f)$. Assume that $f(X)$ is irreducible over K and deduce the description of the Galois group of $f(X)$ in (a) from **T.15.2**.

15.2. (a) Let K be a field of characteristic different from 2, $L = K(X_1, \ldots, X_n)$, $F(X_1, \ldots, X_n) = \prod_{1 \leq i < j \leq n}(X_i - X_j)$ and $G = S_n$. Show that $r_{G,F}(T) = T^2 - F^2$ and $G_F = A_n$.

(b) Let $f(X) \in K[X]$ be an irreducible polynomial with zeros $\alpha_1, \ldots, \alpha_n$ in an extension of K and $\Delta(f) = \prod_{1 \leq i < j \leq n}(\alpha_i - \alpha_j)^2$ its discriminant (see Ex. 9.23). Use (a) and **T.15.2** in order to show that the Galois group $\mathrm{Gal}(K_f/K)$ is contained in A_n if and only if $\sqrt{\Delta(f)} \in K$.

15.3. Let $f(X) = X^4 + pX^2 + qX + r$, where $p, q, r \in K$ and $\mathrm{char}(K) \neq 2, 3$. Show that $f(X) = X^4 + pX^2 + qX + r = (X^2 + aX + b)(X^2 + a'X + b')$ for a, b, a', b' in some field containing K, if and only if a^2 is a zero of the polynomial

$$r(f)(T) = T^3 + 2pT^2 + (p^2 - 4r)T - q^2$$

.

Remark. The polynomial $r(f)(T) = T^3 + 2pT^2 + (p^2 - 4r)T - q^2$ is usually called the resolvent of $f(X) = X^4 + pX^2 + qX + r$ and, in fact, it is a resolvent in the context of the general definition of this notion in (15.2) (see Ex. 15.5). This exercise gives a somewhat different method of solving quartic equations than the method described in Chap. 1 on p. 4: It is possible to factorize the polynomial $f(X)$ by solving the cubic equation $r(f)(T) = 0$ (this gives a, a', b, b'). The zeros of $f(X)$ are the zeros of the two quadratic factors of $f(X)$.

15.4. Denote by $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ the zeros of a separable polynomial $f(X) = X^4 + pX^2 + qX + r$ in its splitting field K_f over K.

(a) Show that the zeros of its resolvent $r(f)(T)$ (see Ex. 15.3) are $(\alpha_1+\alpha_4)^2, (\alpha_2+\alpha_4)^2, (\alpha_3+\alpha_4)^2$.

(b) Show that the discriminants of the polynomials f and $r(f)$ are equal (see Ex. 15.2 and p. 258). In particular, if a quartic polynomial $f(X)$ is separable, then its resolvent $r(f)(X)$ is also separable.

(c) Show that the splitting field K_f of f can be obtained from the splitting field $K_{r(f)}$ of its resolvent $r(f)$ over K by adjunction of one arbitrary solution of the equation $f(X) = 0$, that is,

$$K_f = K(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = K_{r(f)}(\alpha_i),$$

where $i = 1, 2, 3, 4$.

15.5. (a) Let K be a field of characteristic different from 2 and $F(X_1, X_2, X_3, X_4) = \frac{1}{2}((X_1+X_2)^2 + (X_3+X_4)^2) \in K[X_1, X_2, X_3, X_4]$. Show that $G_F = D_4 = V_4 \cup \{(1,3,2,4), (1,4,2,3), (1,2), (3,4)\}$, where $V_4 = \{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ if $G = S_4$ and $G_F = V_4$ if $G = A_4$. Motivate that $r_{G,F}(T)$ is the same for both $G = S_4$ and $G = A_4$.

(b) Let $f(X) = X^4 + pX^2 + qX + r$ and let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ be the zeros of $f(X)$ in its splitting field K_f over K. Motivate that the resolvent defined in Ex. 15.3 equals the resolvent $r_{G,F}(f)(T) = r(f)(T) = T^3 + 2pT^2 + (p^2 - 4r)T - q^2$.

Remark. Very often one meets a somewhat simpler choice $F(X_1, X_2, X_3, X_4) = X_1X_2 + X_3X_4$ for which $G_F = D_4$ (when $G = S_4$). The choice of F in the text of the exercise is adjusted to the "ad hoc" resolvent obtained in a natural way from factorization of a quartic polynomial as a product of two quadrics in Ex. 15.3. The coefficients of $r_{G,F}(f)$ for the "simpler" choice of F are: $r_{G,F}(f)(T) = T^3 - pT^2 - 4rT + 4pr - q^2$

15.6. (a) Assume that $f(X) = X^4 + pX^2 + qX + r$ is irreducible over K. Let

$$\Delta = \Delta(f) = \Delta(r(f)) = -4p^3q^2 - 27q^4 + 16p^4r - 128p^2r^2 + 144pq^2r + 256r^3$$

be the discriminant of f and $r(f)$ (see Ex 15.4(b)) and $\delta = p^2 - 4r$. Using Ex. 15.4 (with or without Ex. 15.5) show that

$$G(K_f/K) = \begin{cases} S_4 \text{ if } [K_{r(f)} : K] = 6, \\ A_4 \text{ if } [K_{r(f)} : K] = 3, \\ D_4 \text{ if } [K_{r(f)} : K] = 2 \text{ and } f \text{ is irreducible over } K_{r(f)}, \\ C_4 \text{ if } [K_{r(f)} : K] = 2 \text{ and } f \text{ is reducible over } K_{r(f)}, \\ V_4 \text{ if } [K_{r(f)} : K] = 1. \end{cases}$$

(b) Show that:

$$G(K_F/K) = \begin{cases} S_4 \text{ when } r(f) \text{ does not have zeros in } K \text{ and } \sqrt{\Delta} \notin K, \\ A_4 \text{ when } r(f) \text{ does not have zeros in } K \text{ and } \sqrt{\Delta} \in K, \\ D_4 \text{ when } r(f) \text{ has only one zero } \beta \in K \text{ and } \sqrt{\beta\Delta} \notin K \\ \qquad \text{if } \beta \neq 0 \text{ and } \sqrt{\delta\Delta} \notin K \text{ if } \beta = 0, \\ C_4 \text{ when } r(f) \text{ has only one zero } \beta \in K \text{ and } \sqrt{\beta\Delta} \in K \\ \qquad \text{if } \beta \neq 0 \text{ and } \sqrt{\delta\Delta} \in K \text{ if } \beta = 0, \\ V_4 \text{ when } r(f) \text{ has all its zeros in } K. \end{cases}$$

In each case give an example of a polynomial f over $\mathbb{Q}$ with the corresponding Galois group.

15.7. Let $f(X) = X^4 + pX^2 + qX + r$ be reducible in K but without zeros in K. Then

$$G(K_f/K) = \begin{cases} V_4 \text{ when } r(f) \text{ has only one zero in } K \\ C_2 \text{ when } r(f) \text{ has all its zeros in } K \end{cases}$$

15.8. (a) Show that the resolvent $r(f)$ of $f(X) = X^4 + pX^2 + r$ has always one of the zeros in K and it has all three zeros in K if and only if $\sqrt{r} \in K$ (K a field of characteristic $\neq 2$). Check also that the discriminant of $f(X)$ (and $r(f)$ – see Ex. 15.4(b)) is

$$\Delta = \Delta(f) = 16r(p^2 - 4r)^2,$$

so $K(\sqrt{\Delta}) = K(\sqrt{r})$.

(b) Show that if $f(X) = X^4 + pX^2 + r$ is irreducible in $K[X]$, where K is a field of characteristic different from 2, then

$$G(K_f/K) = \begin{cases} V_4 \text{ if } r \text{ is a square in } K, \\ C_4 \text{ if } r \text{ is not a square in } K \text{ and } r(p^2 - 4r) \text{ is a square in } K, \\ D_4 \text{ if } r \text{ and } r(p^2 - 4r) \text{ are not squares in } K. \end{cases}$$

15.9. Show that the splitting fields of irreducible trinomials $X^4 + qX + r$ over $\mathbb{Q}$ may give all possible types of Galois groups which appear in Ex. 15.6, that is, S_4, A_4, D_4, C_4 and V_4.

15.10. (a) Let $K = k(Y_1, \ldots, Y_n)$ be the field of rational functions of Y_i over a field k. Let k' be a finite Galois extension of k. Show that $K' = k'(Y_1, \ldots, Y_n)$ is a Galois extension K and $\mathrm{Gal}(K'/K) \cong \mathrm{Gal}(k'/k)$.

(b) Compute the resolvent $r_{G,F}(f)$ in (15.3) when $n = 2$, $k = \mathbb{Q}$ and $f(X) = X^2 + pX + q$ has zeros α_1, α_2. When $r_{G,F}(f)$ is irreducible?

15.11. Using Dedekind's Theorem **T.15.4** show that the Galois groups over $\mathbb{Q}$ of the given polynomials are

(a) S_5 for $f(X) = X^5 + X^2 + 1$;
(b) S_5 for $f(X) = X^5 - X - 1$;
(c) A_5 for $f(X) = X^5 + 20X + 16$;
(d) A_5 for $f(X) = X^5 - 55X + 88$.

15.12. (a) Using Dedekind's Theorem **T.15.4** show that for every n the symmetric group S_n is the Galois group of a field extension of $\mathbb{Q}$.

(b) Construct polynomials in $\mathbb{Z}[X]$ with Galois groups S_6 and S_8.

16

Supplementary problems

In this chapter, we give

16.1. (a) Consider $K = \mathbb{Q}(\sqrt{1+\sqrt[3]{2}})$. Show that $\alpha = \sqrt{1+\sqrt[3]{2}}$ is a zero of $f(X) = X^6 - 3X^4 + 3X^2 - 3$, $[K : \mathbb{Q}] = 6$ and K does not contain any quadratic extension of $\mathbb{Q}$.

(b) Let $K = \mathbb{Q}(\sqrt[3]{1+\sqrt{3}})$. Show that K does not contain a cubic extension but contains a quadratic extension of $\mathbb{Q}$.

16.2. (a) Call a number field (that is, a subfield of the complex numbers) normal if it is normal over the rational numbers. Show that two isomorphic normal subfields of the complex numbers are equal.

(b) Show that for every $n > 2$ there exists n isomorphic but different subfields of the complex numbers.

16.3. Write down multiplication tables for given finite field defining it as a splitting field of $f(X)$ over K if

(a) $f(X) = X^2 + X + 1$ and $K = \mathbb{F}_2$; (b) $f(X) = X^3 + 2X + 1$ and $K = \mathbb{F}_3$;

16.4. Show that there exists a polynomial in $\mathbb{Z}[X]$ of degree 6 whose Galois group is A_5.

Hint. Take a Galois extension of $\mathbb{Q}$ with group A_5 and consider the fix field of a subgroup of order 10 in A_5.

16.5. Show that over a finite field every irreducible polynomial is normal (see Ex. 7.9 for the definition of normal polynomial).

16.6. Find the order of the Galois group of $X^{10} - 5$ over $\mathbb{Q}$. (F_{20}).

16.7. Let $K \subseteq L$ be a finite Galois field extension. Show that if a prime number p divides $[L : K]$, then there is a subfield M of L containing K such that $[L : M] = p$.

16.8. (a) Let $\alpha = \sqrt{2} + \sqrt{3} + \cdots + \sqrt{n}$ $(n \geq 2)$. Show that $[\mathbb{Q} : \mathbb{Q}] = 2^{\pi(n)}$, where $\pi(n)$ denotes the number of primes less or equal n.

(b) Find a primitive element of $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ over $\mathbb{Q}$.

(c) Using (a) show that $\alpha = \sqrt{2}+\sqrt{3}+\cdots+\sqrt{n}$ is a primitive element of $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \ldots, \sqrt{n})$ over $\mathbb{Q}$.

(d) Assume that $[K(\sqrt{a_1}, \ldots, \sqrt{a_n}) : K] = 2^n$. Show that $K(\sqrt{a_1}, \ldots, \sqrt{a_n}) = K(\sqrt{a_1} + \ldots + \sqrt{a_n})$.

(e) Show that $\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}) = 2^n$ when $p_1, \ldots, p_n$ are different prime numbers.

16.9. Let k be a field of characteristic, $L = k(X_1, \ldots, X_n)$ and $K = k(s_1, \ldots, s_n)$, where s_i are the elementary symmetric polynomials of the variables $X_1, \ldots, X_n$. Show that $\alpha = X_1 + 2X_2 + \cdots + nX_n$ is a primitive element of the extension $K \subset L$.

16.10. Let $f(X)$be an irreducible polynomial of degree 4 with two real and two nonreal zeros. Show that the Galois group of $f(X)$ is either D_4 or S_4.

16.11. Show that $\mathbb{Q}(\varepsilon_m, \varepsilon_n) = \mathbb{Q}(\varepsilon_m + \varepsilon_n)$, where $\varepsilon_m, \varepsilon_n$ are m-th and n-th primitive rooth of 1.

16.12. Let $\mathbb{F}$ be a finite field of characteristic p. Find the following degrees:

(a) $[\mathbb{F}(X) : \mathbb{F}(X^p)]$; (b) $[\mathbb{F}(X, Y) : \mathbb{F}(X^p, Y^p)]$.

16.13. (prel) (a) Show that a polynomial $X^{2n+1} - a$, $a \in \mathbb{Q}$, never is normal.

(b) Show that a polynomial $X^4 - a$, $a \in \mathbb{Q}$ is normal if and only if $a = b^2$, $b \in \mathbb{Q}$.

(c) If a polynomial $X^n - a$, $a \in \mathbb{Q}$ which is irreducible over $\mathbb{Q}$ is normal then $n = 2^k$ or $n = 2^k 3^l$, whee $k > 0$.

16.14. Show that if $f(X)$ is a polynomial of odd degree whose reduction modulo one prime p is a product of a first degree polynomial by an irreducible polynomial, and for another prime q its reduction is a product of a quadratic polynomial by an irreducible polynomial, then the Galois group of $f(X)$ over $\mathbb{Q}$ is the symmetric group S_n.

16.15. Find Galois groups of the Taylor polynomials $T_n(X) = \sum_{i=0}^{n} \frac{X^i}{i!}$ for $n > 0$. (Tsche?)

16.16. Let $K = \mathbb{Q}(\sqrt[r]{a})$ where a is a positive integer be such that $[K : \mathbb{Q}] = n$. Show that if M is a subfield of K and $[M : \mathbb{Q}] = d$, then $E = \mathbb{Q}(\sqrt[d]{a})$.

16.17. Show that $\mathbb{C}(X)$ is a Galois extension of $\mathbb{C}(X^n + X^{-n})$, $n \geq 1$. Find the degree and the Galois group of this extension (the Galois group is the dihedral group D_n generated by $\sigma(X) = -X$ and $\tau(X) = \varepsilon X$, where $\varepsilon = e^{\frac{2\pi i}{n}}$ – see also Ex. 12.4).

16.18. Let $\mathbb{F}$ be a finite field with $q = p^n$ elements. Show that $\mathbb{F}(X)$ is a Galois extension of $\mathbb{F}(X^q - X)$. Find the degree and give a description of the Galois group.

16.19. (Verma) Let $\mathbb{F}$ be a finite field with q elements and let $G = G(\mathbb{F}(X)/\mathbb{F})$ be the group of all Möbius transformations over $\mathbb{F}$(see Ex. 6.6). Show that

(a) $|G| = q^3 - q$.

(b) $\mathbb{F}(X)^G = \mathbb{F}(Y)$, where $Y = \frac{(X^{q^2}-X)^{q+1}}{(X^q-X)^{q^2+1}}$.

(c) If H_1 is the subgroup of G consisting of $\sigma(X) = aX + b, a, b \in \mathbb{F}, a \neq 0$, then $\mathbb{F}(X)^{H_1} = \mathbb{F}((X^q - X)^{q-1})$.

(d) If H_2 is the subgroup of G consisting of $\sigma(X) = X + b, b \in \mathbb{F}$, then $\mathbb{F}(X)^{H_2} = \mathbb{F}(X^q - X)$.

(d) Find all subfields of $\mathbb{F}(X)$ containing $\mathbb{F}(X)^G$ when $\mathbb{F}$ has 2 or 3 elements.

16.20. Show that a finite group is solvable if and only if every nontrivial subgroup H of G contains a normal subgroup N such that H/N is a notrivial abelian group.

16.21. Let $K \subseteq L$ be a Galois extension and let $G(L/K) = G$. Show that if G contains a subgroup H such that H does not contain any normal subgroups of G other than the unit subgroup, then there is a polynomial of degree $|H|$ for which the field L is a splitting field.

16.22. (a) Let K be an algebraically closed field (see p. 18) containing a finite field $\mathbb{F}_p$. Show that the algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$ in K (see p. 25) is equal to the union $\bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$. Show also that $\overline{\mathbb{F}}_p = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^{n!}}$.

16.23. Let $\mathbb{F}$ be a finite field and $\mathbb{F} \subset K \subset \overline{\mathbb{F}}$, where K is a field and $\overline{\mathbb{F}}$ an algebraic closure of $\mathbb{F}$ (see p. 25). Show that if K is not finite, then the order of each nontrivial automorphism $\sigma \in A(K/\mathbb{F})$ is not finite.

16.24. Let L be an algebraically closed field and K a subfield of L such that $[L : K] > 1$ is finite. Show that the characteristic of L is 0, $[L : K] = 2$ and $L = K(i)$, where $i^2 = -1$.

16.25. Let $K \subseteq L$ be a Galois extension and $G = G(L/K)$ its Galois group. Show that if L is finite, then both functions $\mathrm{Tr}_G : L \to K$ and $\mathrm{Nr}_G : L \to K$ are surjective. Give an example showing that this is not true for Nr_G when L is infinite (see p. 29 and Ex. 9.11).

16.26. Show that the field $K = \mathbb{Q}(\alpha)$, where $\alpha = \sqrt{(2+\sqrt{2})(3+\sqrt{3})}$ is Galois and show that the Galois group $G(K/\mathbb{Q})$ is the quaternion group of order 8 (see Ex. 12.1(e)).

16.27. Let $K \subseteq L$ be a Galois extension. Show that L is a splitting field of normal polynomials over K (see the definition of a normal polynomial in Ex. 7.9).

16.28. Assume that an irreducible polynomial $f(X) = a_nX^n + \cdots + a_1X + a_0 \in \mathbb{Q}[X]$ has a zero of absolute value 1. Show that the degree of $f(X)$ is even and the polynomial is symmetric, that is, $a_i = a_{n-i}$ for $i = 0, 1, \ldots, n$.

16.29. Let K be a field of characteristic different from 2.

(a) Motivate that if the group of roots of 1 in K is finite, then its order is even.

(b) Show that the group of roots of 1 in a number field K of finite degree over $\mathbb{Q}$ is finite.

(c) Find the groups of roots of 1 in the quadratic fields $\mathbb{Q}(\sqrt{d})$ and in the biquadratic fields $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ ($d, d_1, d_2 \neq 1$ square-free integers not equal 1 and $d_1 \neq d_2$).

16.30. Show that if K is a field and X a variable, then there is infinitely many fields M such that $K \subseteq M \subseteq K(X)$.

16.31. (a) Find the degree of the extension $K(X_1, \ldots, X_n) \supseteq K(X_1^{d_1}, \ldots, X_n^{d_n})$, where $X_1, \ldots, X_n$ are variables and $d_1, \ldots, d_n$ are positive integers (K any field).(Bergman,Verma)

(b) Let K be a field and let k, l, m, n be nonnegative integers such that $kn - lm \neq 0$. Find the degree $[K(X, Y) : K(X^kY^l, X^mY^n)]$, where X, Y are variables.

(c) Choose in (a), $K = \mathbb{C}$. Show that the extension $K(X^kY^l, X^mY^n) \subseteq K(X, Y)$ is Galois and describe its Galois group.

16.32. Let $K \subseteq L$ be a field extension and M_1, M_2 two subfields containing K and contained in L.

(a) Let M_1, M_2 both have one of the properties: separable, normal, Galois over K. What can be said about the same property of M_1M_2 and $M_1 \cap M_2$ over K?

(b) Let L have one of the properties: separable, normal, Galois over both M_1 and M_2. What can be said about the same property of L over M_1M_2 and $M_1 \cap M_2$?

16.33. (George M. Bergman gbergmanmath.berkeley.edu) Let $K \subseteq L$ be an algebraic field extension and let $f(X) \in L[X]$. Show that there exists a nonzero polynomial $g(X) \in L[X]$ such that $f(X)g(X) \in K[X]$.

16.34. Let $K \subseteq L$ bea finite field extension. Show that $K(X) \subseteq L(X)$ is also finite and $[L : K] = [L(X) : K(X)]$.

16.35. Let $L_i \supseteq K$, $i = 1, 2$, be finite field extensions. Show that there exists a normal extension L of K such that $L_i \subseteq L$ for $i = 1, 2$. If $L_i \supseteq K$ are separable, then there exists a Galois extension L of K containing both.

16.36. Let ε be a zero of the polynomial $f(X) = \frac{X^{25}-1}{X^5-1}$. Motivate that $K = \mathbb{Q}(\varepsilon)$ is the splitting field of $f(X)$ over $\mathbb{Q}$ and find all subfields of K (a primitive element for each such subfield expressed as a polynomial of ε).

16.37. Let $f(X) \in K[X]$ be a nonzero polynomial. Show that for every positive integer d there exists $g(X) \in K[X]$ such that $f(X)$ divides $g(X^d)$.

16.38. (Calcut) Let $n > 2$ be a natural number and k an integer such that $\gcd(k, n) = 1$. Then, we have:

(a) $[\mathbb{Q}(\cos \frac{2k\pi}{n}) : \mathbb{Q}] = \frac{\varphi(n)}{2}$;

(b) $[\mathbb{Q}(\sin \frac{2k\pi}{n}) : \mathbb{Q}] = \begin{cases} \varphi(n) & \text{if } 4 \nmid n; \\ \frac{\varphi(n)}{2} & \text{if } n \equiv 0 \pmod 8; \\ \frac{\varphi(n)}{4} & \text{if } n \equiv 4 \pmod 8, n > 4; \end{cases}$

(c) $[\mathbb{Q}(\tan \frac{2k\pi}{n}) : \mathbb{Q}] = \begin{cases} \varphi(n) & \text{if } 4 \nmid n; \\ \frac{\varphi(n)}{4} & \text{if } n \equiv 0 \pmod 8; \\ \frac{\varphi(n)}{2} & \text{if } n \equiv 4 \pmod 8, n > 4. \end{cases}$

16.39. Let G be a group and let G' denote the commutator subgroup of G (see p. 230).

(a) Show that a finite group G is solvable if and only if for each subgroup $H \neq 1$ of G, we have $H' \neq H$.

(b) Show that if H is a normal subgroup of a solvable group G, then H' is also normal in G.

Remark. Notice that this exercise shows that in the definition of solvable group it is possible to choose a chain $G = G_0 \supset G_1 \supset \ldots \supset G_n = \{e\}$ such that G_{i+1} is normal in G_i and G_i/G_{i+1} is abelian in such a way that G_{i+1} is normal in G (and not only in in G_i) for $i = 0, 1, \ldots, n-1$.

16.40. (a) Let K be a field and $f(X) = X^n + pX + q \in K[X]$ a trinomial such that $q \neq 0$. Show that the splitting field of $f(X)$ over K is the same as the splitting field of the trinomial $g(X) = X^n + tX + t$, where $t = \frac{p^n}{q^{n-1}}$.

(b) Show that the Galois group of an irreducible trinomial $g(X) = X^3 + tX + t$ is cyclic of order 3 if and only if there is $a \in K$ such that $t = -\frac{a^2+27}{4}$ (notice that the discriminant $\Delta(g(X)) = -4t^3 - 27t^2$).

(c) Let $x_1 = x$ be a zero of an irreducible trinomial $g(X)$ (in (b)) in its splitting field. Show that the two other zeros are:

$$x_2 = \frac{6x^2 - 9x - ax - a^2 - 27}{2a}, \qquad x_3 = -\frac{6x^2 - 9x + ax - a^2 - 27}{2a}.$$

(d) Let $r(X) \in K[X]$ be such that $x_2 = r(x)$. Motivate that $f(r(X)) = f(X)g(X)$ for some polynomial $g(X) \in K[X]$. Find $g(X)$.

16.41. The normal core of a subgroup H in a group G is the biggest subgroup of H which is normal in G.

(a) Show that the normal core of H in G is

$$H_G = \bigcap_{g \in G} gHg^{-1}.$$

(b) Let $K \subseteq M \subseteq L$ be field extensions such that L is a Galois extension of K and let $H = G(L/M)$, so that $M = L^H$. Show that the normal closure M^* of M in L is the fixed field of the normal core H_G.

16.42. Let $K \subseteq L$ be a Galois extension of degree n. Show that L is not a splitting field of a polynomial of degree less than n if and only if the core of each subgroup of $G(L/K)$ is nontrivial.

16.43. Let G be a group and K a field. Assume that G is a Galois group of a Galois extension of K and call the **Galois index** of G over K the least degree of the polynomials with coefficients in K whose splitting field has G as its Galois group.

Show that the Galois index of G over K is equal to the minimal index of subgroups of G whose core is trivial.

16.44. What are the degrees of irreducible polynomials whose splitting field over $\mathbb{Q}$ has Galois group S_4? Answer the same question for S_5.

16.45. Let $K \subseteq L$ be a Galois extension of degree n whose Galois group $G(L/K)$ is abelian. What is the degree of irreducible polynomials in $K[X]$ having L as its splitting field? Answer the same question when $G(L/K)$ is the quaternion group (of order 8 – see Ex. 12.1(e)).

16.46. Let $K \subseteq L$ be a separable field extension and let N be a normal closure of $K \subseteq L$. Show that the group $G(N/L)$ does not contain nontrivial normal subgroups of the group $G(L/K)$. Notice that $K \subseteq N$ is a Galois extension by Ex. 8.4(b).

Remark. Another way of expressing the situation in the exercise is to say that the core of $G(N/L)$ in $G(N/K)$ is trivial (see Ex. 16.41).

16.47. Find the orders of the Galois groups for the following polynomials:

(a) $X^6 - 3X^2 + 6$; (b) $X^6 + 5X^2 - 10$; (c) $X^6 + 3X^3 + 3$; (d) $X^6 - 7X^2 + 7$.

16.48. Let $K \subseteq L$ be a Galois extension and let $\sigma \in G(L/K)$ be an involution of L (that is, an element of order 2 i $G(L/K)$). Show that $K \subseteq L^\sigma$ is Galois if and only if σ is in the center of $G(L/K)$.

(b) Let $K = \mathbb{Q}$ and $L \subset \mathbb{C}$ in (a). Explain when $L_0 = L \cap \mathbb{R}$ is Galois over $\mathbb{Q}$ (see Ex. 9.21).

16.49. Let $K \subseteq L$ be a field extension and $\alpha, \beta \in L$ be elements such that $\alpha^m, \beta^n \in K$ for some positive integers m, n. Find conditions assuring that $K(\alpha, \beta) = K(\alpha\beta)$. What can be said about $K(\alpha, \beta) = K(\alpha + \beta)$?

16.50. Let $f(X)$ be a polynomial of degree n over a field K whose Galois group is S_n. Show that any splitting field of $f(X)$ over K can not be generated by less than $n-1$ of its zeros. Is it true that if $f(X)$ has the Galois group A_n over K, then its splitting field can not be generated by less than $n-2$ of its zeros?

16.51. Let $N \supset L$ be a normal closure of a finite separable field extension $L \supset K$. Show that $G(N/K)$ is not abelian if $L \supset K$ is not normal.

16.52 (XXXBerg, 22.11(b)). Let $f(X)$ be an irreducible polynomial of prime degree p over a field K and let M be a subfield of a splitting field of $f(X)$ over K. Show that $f(X)$ is still irreducible over M if and only if p does not divide $[M : K]$. (Suggestion: use Ex. 4.2(a) and Ex. 5.3.)

16.53. Let $G = G(L/K)$ be the Galois group of a Galois field extension $K \subseteq L$ and let G' be the commutator subgroup of G (see p. 230). Show that $L^{G'} \supseteq K$ is an abelian Galois extension of K (that is, $L^{G'}$ is a Galois extension of K and the Galois group $G(L^{G'}/K)$ is an abelian group). Show also that for every Galois extension $M \supseteq K$ such that $G(M/K)$ is abelian, we have $M \subseteq L^{G'}$ (thus $L^{G'}$ is the maximal abelian extension of K, which is contained in L).

16.54. Let L be a splitting field of an irreducible polynomial $f(X) \in K[X]$ and let $f(\alpha) = 0$ for $\alpha \in L$. If $K \subseteq M$ is a Galois extension, where $M \subseteq L$, then

(a) the polynomial $f(X)$ is irreducible over M if and only if $M \cap K(\alpha) = K$;

(b) all irreducible factors factors of $f(X)$ in $M[X]$ have the same degree (see Ex. 7.8) and the number of them equals $[M \cap K[\alpha] : K]$.

16.55. Let K be field and $f(X), g(X) \in K[X]$ two irreducible polynomials. Let L be a splitting field of $f(X)g(X)$ over K. Let α be a zero of $f(X)$ and β a zero of $g(X)$ in L.

(a) Show that $f(X)$ is irreducible over $K(\beta)$ if and only if $g(X)$ is irreducible over $K(\alpha)$;

(b) Generalize (a): If $f(X) = f_1(X) \cdots f_r(X)$, where $f_i(X)$ are irreducible in $K(\beta)[X]$, and $g(X) = g_1(X) \cdots g_s(X)$, where $g_j(X)$ are irreducible in $K(\alpha)[X]$, then $r = s$. Moreover, it is possible to number f_i, g_j in such a way that if $\alpha_i \in L$ is a zero of $f_i(X)$ and $\beta_i \in L$ is a zero of $g_i(X)$, then $K(\alpha, \beta_i)$ is isomorphic to $K(\beta, \alpha_i)$ for $i = 1, \ldots, r$. Motivate that $\deg f \deg g_i = \deg g \deg f_i$.

Remark. This correspondence between pairs of irreducible polynomials over fields was first observed by Richard Dedekind (see [XXX]).

16.56. (a) Show that the number of roots of 1 in a finite extension field K of the rational numbers is finite.

(b) Find all roots of 1 in a cyclotomic field $\mathbb{Q}(\varepsilon)$, where ε is a primitive n-th root of 1.

16.57. Let $K \subset L$ be a finite field extension and R a subring of L containing K. Show that R is also a field.

16.58. Find all n such that for any given angle α, the angle $\frac{\alpha}{n}$ is constructible (by using a straightedge and a compass).

16.59. Let K be an arbitrary field and let $L = K(X)$ be the field of rational functions over K. Show that the six functions $X \mapsto X$, $X \mapsto 1 - X$, $X \mapsto 1/X$, $X \mapsto 1/(1 - X)$, $X \mapsto X/(X - 1)$, $X \mapsto (X - 1)/X$ form an automorphism group G of $L = K(X)$ over K, which is isomorphic to S_3. Show also that $L^G = K(g)$, where

$$g(X) = \frac{(X^2 - X + 1)^3}{X^2(X - 1)^2}.$$

Compare Ex. 6.7 and Ex. 16.19.

16.60. Let L be a splitting field of a polynomial $f(X)$ of degree n with coefficients in a field K. By Ex. 5.3, we know that $[L : K] \leq n!$. Show that $[L : K]$ always divides $n!$.

16.61. (a) Let $K \subseteq L$ be a separable field extension and assume that there is n such that $[K(\alpha) : K] \leq n$ for every $\alpha \in L$. Show that the extension $K \subseteq L$ is finite and $[L : K] \leq n$.

(b) Show that (a) need not be true when $K \subseteq L$ is not separable.

16.62. Let L be a separable extension of K and $[L : K] = n$. Show that there are at most 2^{n-1} fields M such that $K \subseteq M \subseteq L$.

16.63. Show that if L is a simple and algebraic extension of a field K, then every intermediate field M between K and L also is simple over K (L need not be algebraic over K in which case the claim is Lüroth's theorem – see Ex. 4.10).

16.64. Let $L = K(\alpha, \beta)$ be a field extension such that α is algebraic and β is transcendent over K. Show that the extension $K \subset L$ is not simple.

16.65. Let $K \subset M \subset L$ be three fields and let L be algebraic over K. Is it true that the degree of $\alpha \in L$ over M divides the degree of α over K?

16.66. Let $K \subset M \subset L$ be three fields and let L be algebraic over K. Show that $[M : K]$ and $[M(\alpha) : M]$ are relatively prime for $\alpha \in L$, then the minimal polynomial of α over M has its coefficients in K.

16.67. Give an example of a polynomial $f(X) \in \mathbb{Z}[X]$ of degree n with n real zeros whose Galois group over $\mathbb{Q}$ is S_n for $n = 3, 4, 5$.

16.68. Let M_1, M_2 be two finte extensions of a field K contained in a field L. Show that $[M_1M_2 : K] = [M_1 : K][M_2 : K]$ implies that $M_1 \cap M_2 = K$.

16.69. Show that the multiplicative group K^* of a field K is cyclic if and only if K is a finite field.

16.70. Show that a finite extension over its prime subfield contains only finitely many roots of 1.

16.71. Let $K \subseteq L$ be a finite field extension. Show that K is perfect if and only if L is perfect (see p. 39 and Ex. 8.3).

16.72. Show that the splitting field of the polynomial $X^4 - 7X^2 + 3X + 1$ is real and its Galois group is A_4.

17

Proofs of the theorems

Theorems of Chapter 2

For the proof of Theorem **T.2.1** see **A.3.8**.

Theorems of Chapter 3

For the proofs of the Theorems **T.3.1** and **T.3.2** see **A.6.1** and **A.6.2**, respectively.

T. 3.3 Gauss's Lemma. *A nonconstant polynomial with integer coefficients is reducible in* $\mathbb{Z}[X]$ *if and only if it is reducible in* $\mathbb{Q}[X]$*. More exactly, if* $f \in \mathbb{Z}[X]$ *and* $f = gh$*, where* $g, h \in \mathbb{Q}[X]$*, then there are rational numbers* r, s *such that* $rg, sh \in \mathbb{Z}[X]$ *and* $rs = 1$*, so* $f = (rg)(sh)$*.*

Proof. We start with a definition. A polynomial with integer coefficients $f(X)$ is called **primitive** if the greatest divisor of its coefficients is equal 1. The product of two primitive polynomials $f(X)g(X)$ is also primitive. In fact, if there is a prime number p dividing all the coefficients of $f(X)g(X)$ then we can take the reduction of the product modulo p. The result will be a zero polynomial so that $\bar{f}(X)\bar{g}(X) = 0$ in the ring $\mathbb{F}_p[X]$. But a product of two polynomials with coefficients in a field is zero only if one of the factors is 0. If, say, $\bar{f}(X) = 0$, then all the coefficients of $f(X)$ are divisible by p, which is impossible ($f(X)$ is primitive). This proves that the product of primitive polynomials is primitive.

Note now that if $f(X)$ is an arbitrary polynomial with rational coefficients, then $f(X) = c(f)f_0(X)$, where $f_0(X)$ is primitive and $c(f)$ is a rational number. In fact, we can find the least positive integer l such that the coefficients of $lf(X)$ are integers an then divide $lf(X)$ by the greatest common divisor k of its coefficients. This is $f_0(X)$. Thus defining $c(f) = \frac{k}{l}$, we have $f(X) = c(f)f_0(X)$. The rational number $c(f)$ is called the **contents** of $f(X)$.

Of course, if a polynomial $f \in \mathbb{Z}[X]$ is reducible in $\mathbb{Z}[X]$, then it is reducible in $\mathbb{Q}[X]$. Conversely, suppose that $f \in \mathbb{Z}[X]$ and $f = gh$, where $g, h \in \mathbb{Q}[X]$. We have $g = c(g)g_0$ and $h = c(h)h_0$, where $g_0, h_0 \in \mathbb{Z}[X]$ are primitive polynomials. Hence $f = c(g)c(h)g_0h_0$. Let $c(g)c(h) = \frac{m}{n}$, where m, n are relatively prime integers. Assume that $n \neq 1$ and choose a prime p dividing n. Then the equality $nf = mg_0h_0$ shows that p divides the right hand side and since p does not divide m, it must divide all the coefficients of the product g_0h_0. But this is clearly impossible, since the product is a primitive polynomial. The conclusion is that p can not exist and consequently $n = 1$. Hence, we have a decomposition $f(X) = (mg_0)(h_0)$ into a product of two integer polynomials. Now taking $r = \frac{m}{c(g)}$ and $s = \frac{1}{c(h)}$, we have two rational numbers such that $rg, sh \in \mathbb{Z}[X]$ and $rs = 1$. □

Theorems of Chapter 4

T. 4.1 *Let $\alpha \in L \supseteq K$ be algebraic over K.*

(a) Any minimal polynomial of α over K is irreducible and divides every polynomial in $K[X]$ which has α as its zero.

(b) An irreducible polynomial $f \in K[X]$ such that $f(\alpha) = 0$ is a minimal polynomial of α over K.

(c) All minimal polynomials of α over K can be obtained by multiplying one of them by nonzero elements in K.

Proof. (a) Let p be a minimal polynomial of α over K. If $p = p_1p_2$, where $\deg(p_1) < \deg(p)$ and $\deg(p_2) < \deg(p)$, then $p(\alpha) = 0$ implies $p_1(\alpha) = 0$ or $p_2(\alpha) = 0$, which contradicts the choice of p as a polynomial of the least possible degree having α as its zero.

(b) We have, $f(X) = p(X)q(X) + r(X)$, where $\deg(r) < \deg(p)$ or $r = 0$. $f(\alpha) = 0$ and $p(\alpha) = 0$ imply that also $r(\alpha) = 0$, so r must be the zero polynomial according to the definition of p, that is, $p \mid f$.

(c) Let both p and p' be minimal polynomials of α over K. According to (a), they divide each other, so $p' = cp$, where c is a nonzero element of K. □

T. 4.2 Simple extension theorem. *(a) If $\alpha \in L \supseteq K$ is algebraic over K, then each element in $K(\alpha)$ can be uniquely represented as $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$, where $a_i \in K$ and n is the degree of the minimal polynomial of α over K. Thus $[K(\alpha) : K] = n$ and $1, \alpha, \ldots, \alpha^{n-1}$ is a basis of $K(\alpha)$ over K.*

(b) If $\alpha \in L \supseteq K$ is transcendental over K, then $K[\alpha] \cong K[X]$, where $K[X]$ is the ring of polynomials over K.

Proof. Consider the ring homomorphism

$$\varphi : K[X] \longrightarrow K[\alpha],$$

where $\varphi(f(X)) = f(\alpha)$. We have

$$\operatorname{Ker}\varphi = \{f \in K[X] : \varphi(f) = f(\alpha) = 0\} = (p(X)),$$

since every polynomial having α as its zero is a multiple of $p(X)$ by **T.4.1** (b). It is clear that the image of φ is the whole ring $K[\alpha]$. By the Main Theorem on ring homomorphisms, we get $K[X]/(p(X)) \cong K[\alpha]$. As we know, each class in $K[X]/(p(X))$ can be uniquely represented by a polynomial

$$a_0 + a_1X + \cdots a_{n-1}X^{n-1},\ a_i \in K,$$

so that each element in $K[\alpha]$ can be uniquely written as the image

$$a_0 + a_1\alpha + \cdots a_{n-1}\alpha^{n-1}, a_i \in K,$$

of such a polynomial. Finally, we observe that $K[\alpha]$ is a field, since the polynomial $p(X)$ is irreducible (by an earlier theorem, $K[X]/(p(X))$ is a field if and only if $p(x)$ is irreducible).

If α is transcendental, then it is clear that the kernel of the homomorphism φ is (0), since by the definition of α, the equality $\varphi(f(X)) = f(\alpha) = 0$ implies that f must be the zero polynomial. Of course, φ is surjective. Thus φ is an isomorphism of the rings $K[X]$ and $K[\alpha]$. Notice that the field of quotients of these rings $K(X)$ and $K(\alpha)$ are also isomorphic. □

T. 4.3 Tower law. *Let $M \supseteq L$ and $L \supseteq K$ be finite field extensions. Then $M \supseteq K$ is a finite extension and $[M : K] = [M : L][L : K]$.*

Proof. Let e_i, $i = 1, \ldots, l$, be a basis of L over K, and f_j, $j = 1, \ldots, m$, a basis of M over L. If $x \in M$, then there is a unique presentation $x = \sum_{j=1}^{m} l_j f_j$, where $l_j \in L$. For each j there is a unique presentation $l_j = \sum_{i=1}^{l} a_{ij}e_i$, where $a_{ij} \in K$. Therefore,

$$x = \sum_{j=1}^{m} l_j f_j = \sum_{j=1}^{m}\sum_{i=1}^{l} a_{ij}e_i f_j$$

and the presentation of x as a linear combination of $e_i f_j$ with coefficients $a_{ij} \in K$ is unique. This shows that lm products $e_i f_j$ form a basis of M over K, that is, $[M : K] = [M : L][L : K]$. □

T. 4.4 *A field extension $L \supseteq K$ is finite if and only if it is algebraic and finitely generated.*

Proof. Assume that $L \supseteq K$ is a finite extension. Then there is a basis $e_1, \ldots, e_n$ of L over K, so $L = K(e_1, \ldots, e_n)$, that is, L is finitely generated over K. Take $x \in L$ and consider the powers $1, x, x^2, \ldots, x^n \in L$. Since the number of these elements is $n+1$, they must be linearly dependent over K, that is, $a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = 0$, where not all coefficients $a_i \in K$ are equal to 0. Thus x is an algebraic element over K, that is, L is an algebraic extension of K.

Assume now that $L \supseteq K$ is algebraic and finitely generated. This means that $L = K(\alpha_1, \alpha_2, \ldots, \alpha_r)$ and we have the following tower of fields:

$$K \subseteq K(\alpha_1) \subseteq K(\alpha_1, \alpha_2) \subseteq \cdots \subseteq K(\alpha_1, \ldots, \alpha_r).$$

For each $i = 0, \ldots, n-1$, we have α_{i+1} algebraic over K, so it is algebraic over $K(\alpha_1, \alpha_2, \ldots, \alpha_i)$. Hence the extension $K(\alpha_1, \alpha_2, \ldots, \alpha_i) \subseteq K(\alpha_1, \alpha_2, \ldots, \alpha_i, \alpha_{i+1})$ is finite. Consequently the extension $K \subseteq L$ is finite as its degree is the product of the degrees $[K(\alpha_1, \alpha_2, \ldots, \alpha_i, \alpha_{i+1}) : K(\alpha_1, \alpha_2, \ldots, \alpha_i)]$ □

T. 4.5 *If $K \subseteq M \subseteq L$ are field extensions such that M is algebraic over K and $\alpha \in L$ is algebraic over M, then it is algebraic over K.*

Proof. Let α be a zero of a polynomial $f(X) = X^n + \alpha_{n-1} X^{n-1} + \cdots + \alpha_1 X + \alpha_0$, where $\alpha_i \in M$ for $i = 0, 1, \ldots, n-1$. Consider the tower of field extensions:

$$K \subseteq K(\alpha_0, \ldots, \alpha_{n-1}) \subseteq K(\alpha_0, \ldots, \alpha_{n-1}, \alpha).$$

Since the elements $\alpha_0, \ldots, \alpha_{n-1}$ are algebraic over K, the first extension is finite by **T.4.4**. Since α is algebraic over the field $K(\alpha_0, \ldots, \alpha_{n-1})$, the second extension is finite by the same theorem. Thus, the extension $K(\alpha_0, \ldots, \alpha_{n-1}, \alpha) \supseteq K$ is finite by **T.4.3**, the element α is algebraic over K by **T.4.4**

□

T. 4.6 *Let $L \supseteq K$. All elements in L algebraic over K form a field.*

Proof. Let $\alpha, \beta \in L$ be two elements algebraic over K. Then the extensions $K(\alpha, \beta) \supseteq K(\alpha) \supseteq K$ are finite. Hence according to theorem **T.4.4** they are algebraic. But $\alpha \pm \beta$, $\alpha\beta \in K(\alpha, \beta)$, and $\alpha/\beta \in L$, when $\beta \neq 0$. Hence the set of algebraic elements in L is closed with respect to the four arithmetical operations, that is, the elements of L algebraic over K form a field. □

Theorems of Chapter 5

T. 5.1 *(a) If f is an irreducible polynomial over K, then there exists a field $L \supseteq K$ such that $L = K(\alpha)$ and $f(\alpha) = 0$.*

(*b*) *If* $\tau : K \to K'$ *is a field isomorphism,* f *an irreducible polynomial over* $K, L = K(\alpha)$, *where* $f(\alpha) = 0$ *and* $L' = K'(\alpha')$, *where* $\tau(f)(\alpha') = 0$, *then there is an isomorphism* $\sigma : K(\alpha) \to K'(\alpha')$ *such that in the diagram:*

$$\begin{array}{ccc} K(\alpha) & \xrightarrow[\sigma]{} & K'(\alpha') \\ \uparrow & & \uparrow \\ K & \xrightarrow[\tau]{} & K' \end{array} ,$$

we have $\sigma(\alpha) = \alpha'$ *and* $\sigma|_K = \tau$.

In particular, if $K = K'$ *and* $\tau = id$, *then* σ *is an isomorphism over* K (*that is, the isomorphism* σ *maps each element in* K *on itself*) *of the two simple extensions of* K *by two arbitrary roots of* $f(X) = 0$.

Proof. (a) As we know from the proof of **T.4.2**, the quotient $L = K[X]/(f(X))$ is a field, since $f(X)$ is irreducible in $K[X]$. The class $[X] = \alpha$ is a solution in L of the equation $f(X) = 0$ and $L = K(\alpha)$.

(b) The isomorphism $\tau : K \to K'$ can be extended to an isomorphism of the polynomial rings $\tau : K[X] \to K'[X]$ (just applying τ on K to the coefficients of the polynomials). This isomorphisms maps the irreducible polynomial $f(X)$ onto the irreducible polynomial $\tau(f)(X)$ in $K'[X]$. Thus we have an isomorphism of the the quotient rings:

$$\tau^* : K[X]/(f(X)) \to K'[X]/(\tau(f)(X))$$

such that the class of $[X] = \alpha$ in the first ring maps onto the class of $[X] = \alpha'$ in the second one. Since $K[X]/(f(X)) = K(\alpha)$ and $K'[X]/(\tau(f)(X)) = K'(\alpha')$, $\sigma = \tau^*$ is the required extension of τ. □

T. 5.2 (*a*) *Every polynomial* $f \in K[X]$ *has a splitting field over* K.

(*b*) *If* $\tau : K \to K'$ *is an isomorphism of fields,* L *is a splitting field of a polynomial* $f \in K[X]$ *and* L' *is a splitting field of the polynomial* $\tau(f) \in K'[X]$, *then there exists an isomorphism* $\sigma : L \to L'$

$$\begin{array}{ccc} L & \xrightarrow[\sigma]{} & L' \\ \uparrow & & \uparrow \\ K & \xrightarrow[\tau]{} & K' \end{array}$$

which extends τ (*that is* $\sigma|_K = \tau$). *In particular, if* $K = K'$ *and* $\tau = id$, *then two splitting fields for* f *over* K *are* K*-isomorphic* (*that is, the isomorphism* σ *maps each element in* K *on itself*).

Moreover, if f is separable, then there are exactly $[L : K]$ different possibilities for σ when τ is given.

Proof. (a) We apply induction with respect to the $\deg f = n$ and an arbitrary field K. If $\deg f = 1$, then of course $L = K$. If $\deg f > 1$ and f_1 is an irreducible factor of f, then according to **T.5.1** (a), there is a field $L_1 = K(\alpha_1)$ in which $f_1(X) = 0$ has a solution α_1. Thus $f(X) = (X - \alpha_1)g(X)$, where the $\deg g = \deg f - 1$ and the highest coefficients a of f and g are the same. The polynomial g has a splitting field L over L_1, that is, $g(X) = a(X - \alpha_2)\cdots(X - \alpha_n)$ and $L = L_1(\alpha_2, \ldots, \alpha_n)$, so $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ and $f(X) = a(X - \alpha_1)(X - \alpha_2)\cdots(X - \alpha_n)$.

(b) Let $L = K(\alpha_1, \ldots, \alpha_n)$ and $L' = K(\alpha'_1, \ldots, \alpha'_n)$, where $f(X) = a(X - \alpha_1)\cdots(X - \alpha_n)$, $a \in K$, and $\tau(f)(X) = a'(X - \alpha'_1)\cdots(X - \alpha'_n)$, $a' \in K'$.

We apply induction with respect to the degree $[L : K]$ for arbitrary pairs of fields K and L. If $[L : K] = 1$, then $f(X) = a(X - \alpha_1)(X - \alpha_2)\cdots(X - \alpha_n)$, $\alpha_i \in K$, so $\tau(f)(X) = a(X - \alpha'_1)(X - \alpha'_2)\cdots(X - \alpha'_n)$ and $\alpha'_i \in K$, that is, $L' = K'$. We take $\sigma = \tau$.

Assume now that $[L : K] > 1$. Then there exists i such that $\alpha_i \notin K$. Ma may assume that $i = 1$, so α_1 is a solution to the equation $f_1(X) = 0$, where $f_1(X)$ is an irreducible factor of $f(X)$ and $\deg f_1 > 1$. Let α'_1 be a zero of $\tau(f_1)(X)$, which is an irreducible factor of $\tau(f)(X)$. According to **T.5.1** (b), we have an extension σ_1 of τ to an isomorphism of $K(\alpha_1)$ onto $K(\alpha'_1)$. Now L is a splitting field of f over $K(\alpha_1)$ and $[L : K(\alpha_1)] = [L : K]/[K(\alpha_1) : K] < [L : K]$. According to the inductive assumption, there exists an isomorphism $\sigma : L \to L'$, which extends σ_1. Of course, σ extends τ, since σ_1 extends τ.

If $f(X)$ is separable and α is a zero of $f_1(X)$ then $\sigma(\alpha)$ is a zero of $\tau(f_1)(X)$, since $0 = \sigma(f_1(\alpha)) = \tau(f_1)(\sigma(\alpha))$. Thus $\tau(f_1)(X)$ has d different zeros, where $d = \deg f_1$. Hence we can choose σ_1 in exactly d different ways. Since $f(X)$ is separable over $K(\alpha_1)$, we can use induction as above to the extension L of $K(\alpha_1)$. Each choice of σ_1 gives $[L : K(\alpha_1)] = [L : K]/[K(\alpha_1) : K] = [L : K]/d$ different choices of σ. Thus the total number of extensions σ of τ equals $d \cdot [L : K]/d = [L : K]$.

When $K = K'$ and $\tau = id$, it is now evident that two splitting fields of $f(X)$ over K are isomorphic. □

T. 5.3 *A polynomial $f \in K[X]$ has no multiple zeros in any extension $L \supseteq K$ if and only if* $\gcd(f, f') = 1$.

Proof. Let $\alpha \in L$ be a multiple zero of $f(X)$, that is, $f(X) = (X-\alpha)^2 q(X)$ (the multiplicity of α is at least 2), where $q(X) \in L[X]$. Then $f'(X) = 2(X - \alpha)q(X) + (X - \alpha)^2 q'(X)$, so $f(\alpha) = f'(\alpha) = 0$. Hence $\gcd(f(X), f'(X)) \neq 1$ as it is divisible by $X - \alpha$.

Conversely, let $d = \gcd(f, f')$ be not a constant polynomial and let α be a zero of $d(X)$ in some field containing K (here we use **T.5.1**). We have $f(\alpha) = f'(\alpha) = 0$. Hence $f(X) = (X - \alpha)q(X)$, so $f'(X) = q(X) + (X - a)q'(X)$. The last equality shows that $q(\alpha) = 0$. Hence $q(X) = (X - \alpha)q_1(X)$ and $f(X) = (X - \alpha)^2 q_1(X)$, that is, the polynomial $f(X)$ has multiple zeros. □

T.5.4 *(a) The number of elements in a finite field is a power of a prime number.*

(b) If p is a prime number and $n \geq 1$, then the splitting field for $X^{p^n} - X$ over $\mathbb{F}_p$ is a finite field with p^n element.

(c) Two finite fields with the same number of elements are isomorphic. More exactly, every finite field with p^n element is a splitting field of $X^{p^n} - X$ over $\mathbb{F}_p$.

Proof. (a) Let K be a finite field. The prime subfield of K is of course also finite, so let $\mathbb{F}_p$ for a prime number p be the prime subfield contained in K (see Chapter 2). Let $\alpha_1, \ldots, \alpha_n$ be a basis of K over $\mathbb{F}_p$. Each element of K is uniquely represented as $a_1\alpha_1 + \cdots + a_n\alpha_n$, where $a_i \in \mathbb{F}_p$, so the number of elements of K equals the number of such linear combinations, that is, it is equal p^n.

(b) Let K be a splitting field of the polynomial $X^q - X$, where $q = p^n$, over $\mathbb{F}_p$. The existence of K follows from **T.5.2**. Let

$$M = \{\alpha \in K \mid \alpha^q = \alpha\}$$

be the set of all solutions of the equation $X^q = X$ in K. If $\alpha, \alpha_1, \alpha_2 \in M$, then

$$(\alpha_1 + \alpha_2)^q = \alpha_1^q + \alpha_2^q = \alpha_1 + \alpha_2, \qquad (\alpha_1\alpha_2)^q = \alpha_1^q\alpha_2^q = \alpha_1\alpha_2,$$

and

$$\left(\frac{1}{\alpha}\right)^q = \frac{1}{\alpha^q} = \frac{1}{\alpha} \quad \text{if} \quad \alpha \neq 0,$$

so the elements of M form a subfield of K. The subfield M is of course a splitting field of the polynomial $X^q - X$ over $\mathbb{F}_p$, so by **T.5.2** it is isomorphic to K. In particular, the fields M and K have the same number of elements which equals $q = p^n$, since all zeros of the polynomial $f(X) = X^q - X$ are different. In fact, we have $f'(X) = qX^{q-1} - 1 = -1$, that is, the polynomials $f(X)$ and $f'(X)$ are relatively prime (see **T.5.3**). This proves that $M = K$, so K is a field consisting of p^n.

(c) Let K be any field with $q = p^n$ elements. Since all nonzero elements of K form a group with respect to multiplication and the order of this group is $q-1$, we have $\alpha^{q-1} = 1$ for each nonzero $\alpha \in K$. Hence all elements of K including 0 satisfy the equation $X^q = X$. Thus K is the splitting field of the polynomial $X^q - X$ over $\mathbb{F}_p$. □

T.5.5 *For every field K there exists an algebraic closure $\overline{K}$ and two algebraic closures of the same field K are K-isomorphic.*

Proof. As a first step, we prove that for every field K, there exists a field $K_1 \supseteq K$ such that every irreducible polynomial $f(X) \in K[X]$ has a zero in K_1.

Let $\mathcal{S}$ denote the set of all irreducible polynomials $f \in K[X]$. For each $f \in \mathcal{S}$, we take a variable X_f and form the polynomial ring $R = K[\ldots X_f \ldots]$ generated over K by all the varaiables X_f. Consider the ideal $\mathcal{I}$ in this polynomial ring generated by all $f(X_f)$, where $f \in \mathcal{S}$. We claim that this ideal is proper, since $1 \notin \mathcal{I}$. If this is not true, then there are polynomials $f_i(X_{f_i})$ such that

$$1 = g_1 f_1(X_{f_1}) + \cdots + g_r f_r(X_{f_r})$$

for some polynomials $g_i \in R$. The polynomials g_i depend on some finite number of variables X_f. Let M be an extension of K in which each polynomial $f(X_{f_i})$ has a zero α_i. Take a ring homomorphism mapping each variable X_{f_i} on α_i and all remaining variables X_f on 0. The equality above maps then onto $1 = 0$, which is impossible. Hence 1 can not belong to the ideal $\mathcal{I}$.

Since $\mathcal{I}$ is a proper ideal, we have a maximal ideal $\mathcal{M}$ containing $\mathcal{I}$ (see **A.15.1**) and we have the natural surjection of the ring R onto its quotient $R/\mathcal{M}$, which is a field K_1 by **A.4.4**. Notice now that the field K is mapped into the field K_1, since the kernel of the surjection of R onto K_1 is zero when restricted to the field K (a field has only two ideals (0) and itself, but in this case the kernel is (0), since 1 is not in the kernel – see **A.4.6**). Thus, we can identify K with a subfield of K_1. Moreover, every polynomial $f(X_f)$ has a zero in K_1, since the image of X_f is a zero of this polynomial ($f(X_f)$ equals zero in K_1). This proves the first assertion of our proof.

Now we repeat the process and construct a chain of fields

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_n \subseteq \cdots$$

such that each polynomial over K_1 has a zero in K_2, each polynomial over K_2 has a zero in K_3 and so on. Define $\overline{K} = \bigcup_{i=0}^{\infty} K_i$. We claim that $\overline{K}$ is an algebraic closure of K.

In fact, if $f(X) \in \overline{K}$ is an irreducible polynomial, then the coefficients of $f(X)$ are already in some field K_i. Hence, this polynomial has a zero in K_{i+1}, that is, it has a zero in $\overline{K}$. As $f(X)$ is irreducible in $\overline{K}[X]$ and has a zero in $\overline{K}$, it has degree 1. Thus the field $\overline{K}$ is algebraically closed, since the only irreducible polynomials over $\overline{K}$ have degree 1 (see p. 18).

Now we prove that two algebraic closures $\overline{K}$ and $\overline{K'}$ of the same field K are isomorphic. Consider the set of all pairs (L, φ) such that L is a subfield of $\overline{K}$ containing K and φ an injection of L into $\overline{K'}$ over K. This set is not empty, since we have the pair consisting of K and the identity as φ. Such pairs are ordered when we declare a pair (L, φ) less or equal (L', φ') when $L \subseteq L'$ and φ' restricted to L is equal φ. If $\mathcal{Y}$ is a set of pairs (L, φ) such that for two pairs (L_1, φ_1) and (L_2, φ_2), we have $L_1 \subseteq L_2$ or $L_2 \subseteq L_1$, then taking $L^0 = \bigcup_{L \in \mathcal{Y}} L$ and defining φ_0 on L_0 so that its restriction to L is φ (for $(L, \varphi) \in \mathcal{Y}$), we get an upper bound of the set $\mathcal{Y}$. Thus, we can apply Zorn's Lemma (see **A.14.1**), which says that there exist a maximal pair. Let (M, φ) be such a maximal pair and let $M' = \varphi(M)$ be the corresponding subfield of $\overline{K'}$. We want to prove that $M = \overline{K}$ and $M' = \overline{K'}$. If not, then there is $\alpha \in \overline{K}$ such that $\alpha \notin M$. The element α is algebraic over M (since it is algebraic over K), so let us take

its minimal polynomial $f(X)$ over M. Since $f(X) \in M[X]$, we can take the image of this polynomial applying φ to its coefficients. This polynomial, as a polynomial with coefficients in M', has a zero $\alpha' \in \overline{K'}$. By **T.5.1**, there is an isomorphism $\psi : M(\alpha) \to M'(\alpha')$ which restricted to M is equal to φ. Thus the pair (M, φ) is not maximal if α could be chosen outside of M. This contradiction shows that $M = \overline{K}$. Now the image $\varphi(\overline{K})$ is an algebraically closed subfield of $\overline{K'}$, which is algebraic over it. But this is only possible when $\overline{K'} = \varphi(\overline{K})$, since an algebraically closed field has not nontrivial algebraic extensions. □

Theorems of Chapter 6

T. 6.1 *All K-automorphisms of L form a group with respect to the composition of automorphisms.*

Proof. If $\sigma, \tau \in G(L/K)$ are automorphisms of L over K, then one easily checks that their composition $\sigma\tau$ also is an automorphism of L over K. The inverse σ^{-1} is an automorphism of L over K, which also can be easily checked. □

T. 6.2 *If G is a group of automorphisms of L (finite or infinite), then L^G is a subfield of L and $[L : L^G] = |G|$.*

Proof. First we show that $[L : L^G] \geq |G|$. Let $G = \{\sigma_1, \ldots, \sigma_n\}$. Here G need not to be a group – simply a set of different automorphisms of L. Assume that L has dimension $m < n$ over L^G and let $e_1, \ldots, e_m$ be a basis of L over L^G. Consider the following system of m homogeneous linear equations:

$$\begin{aligned} \sigma_1(e_1)x_1 + \cdots + \sigma_n(e_1)x_n &= 0 \\ &\ldots \\ \sigma_1(e_i)x_1 + \cdots + \sigma_n(e_i)x_n &= 0 \\ &\ldots \\ \sigma_1(e_m)x_1 + \cdots + \sigma_n(e_m)x_n &= 0. \end{aligned}$$

Since the number of equations m is less than the number of variables n, the system has a nontrivial solution $(x_1, \ldots, x_n) \in L^n$. Let $x = \sum_{i=1}^{m} a_i e_i$, where $a_i \in L^G$, be an arbitrary element of L. Multiply the $i-th$ equation in the system by a_i for $i = 1, \ldots, m$ and notice that for every $j = 1, \ldots, n$, we have $a_i\sigma_j(e_i) = \sigma_j(a_i e_i)$, since $a_i \in L^G$. Then add all the equations. The result is the following equality:

$$\sigma_1(x)x_1 + \cdots + \sigma_n(x)x_n = 0,$$

which holds for every $x \in L$. But it contradicts to the Dedekind's Lemma, since $(x_1, \ldots, x_n) \neq (0, \ldots, 0)$. Hence $[L : L^G] \geq |G|$. Notice that the proof implies that the degree $[L : L^G]$ is

always at least equal to the number of automorphisms in any set (not necessarily a group) G. In particular, if there exists an infinite group of automorphisms of L, then the dimension of L over L^G is not finite.

Now we prove that $[L : L^G] \leq |G|$, when G is a finite group of automorphisms of L. Let $G = \{\sigma_1, \ldots, \sigma_n\}$ and assume that $m = [L : L^G] > |G| = n$. Assume that $e_1, \ldots, e_m$ is a basis of L over L^G and consider the homogeneous linear system:

$$\begin{aligned} x_1\sigma_1^{-1}(e_1) + \cdots + x_m\sigma_1^{-1}(e_m) &= 0 \\ &\ldots \\ x_1\sigma_i^{-1}(e_1) + \cdots + x_m\sigma_i^{-1}(e_m) &= 0 \\ &\ldots \\ x_1\sigma_n^{-1}(e_1) + \cdots + x_m\sigma_n^{-1}(e_m) &= 0. \end{aligned}$$

Since the number of equations n is less than the number of variables m, the system has a nontrivial solution $(x_1, \ldots, x_m) \in L^m$. Assume that $x_1 \neq 0$. Since the system is homogeneous, any multiple $c * (x_1, \ldots, x_m)$, where $c \in L$, is also a solution of the system. Therefore, we can choose x_1 arbitrarily in L. Let's do it in such a way that

$$\sigma_1(x_1) + \cdots + \sigma_n(x_1) \neq 0.$$

Such a choice is possible by Dedekind's Lemma (the sum to the left can not be 0 for all $x_1 \in L$). With this choice of x_1, we map the $i - th$ equation of the system $(*)$ by the automorphism σ_i and we get:

$$\begin{aligned} \sigma_1(x_1)e_1 + \cdots + \sigma_1(x_m)e_m &= 0 \\ &\ldots \\ \sigma_i(x_1)e_1 + \cdots + \sigma_i(x_m)e_m &= 0 \\ &\ldots \\ \sigma_m(x_1)e_1 + \cdots + \sigma_m(x_m)e_m &= 0. \end{aligned}$$

Adding all the equations above, we get the following equality:

$$\mathrm{Tr}_G(x_1)e_1 + \cdots + \mathrm{Tr}_G(x_m)e_m = 0,$$

where $\mathrm{Tr}_G(x_1) = \sigma_1(x_1) + \cdots + \sigma_n(x_1) \neq 0$. This gives a contradiction, since $e_1, \ldots, e_m$ are linearly independent over L^G and $\mathrm{Tr}_G(x_i) \in L^G$. Hence $[L : L^G] \leq |G|$. □

T. 6.3 Dedekind's Lemma. *If $\sigma_1, \sigma_2, \ldots, \sigma_n$ are different automorphisms of a field L and the equality $a_1\sigma_1(x) + a_2\sigma_2(x) + \ldots + a_n\sigma_n(x) = 0$, where $a_i \in L$, holds for every $x \in L$, then $a_1 = a_2 = \ldots = a_n = 0$.*

Proof. We prove the Lemma by induction on the number of automorphisms n. If $n = 1$, then the equality $a_1\sigma_1(x) = 0$ for every $x \in L$, implies that $a_1\sigma_1(1) = a_1 = 0$.

Assume now that the Lemma is true when the number of automorphisms is less than $n > 1$ and let

$$a_1\sigma_1(x) + a_2\sigma_2(x) + \ldots + a_n\sigma_n(x) = 0 \tag{2}$$

for every $x \in L$, where $a_i \in L$. Since the last equality holds for every $x \in L$, we may choose an arbitrary $\alpha \in L$ and replace x by αx. Then we get:

$$a_1\sigma_1(\alpha)\sigma_1(x) + a_2\sigma_2(\alpha)\sigma_2(x) + \ldots + a_n\sigma_n(\alpha)\sigma_n(x) = 0 \tag{3}$$

Now we multiply the equality (2) by $\sigma_n(\alpha)$ and subtract from it the equality (3):

$$a_1(\sigma_n(\alpha)-\sigma_1(\alpha))\sigma_1(x)+a_2(\sigma_n(\alpha)-\sigma_2(\alpha))\sigma_2(x)+\ldots+a_{n-1}(\sigma_n(\alpha)-\sigma_{n-1}(\alpha))\sigma_{n-1}(x) = 0$$

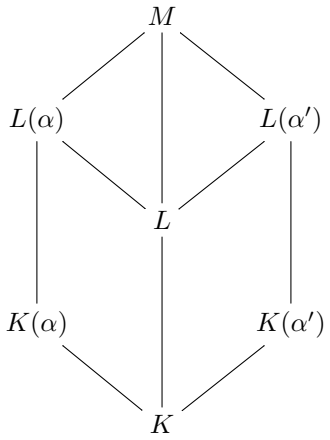
Using the inductive assumption, we get that all the coefficients in the last equality are equal to 0, that is, $a_i(\sigma_n(\alpha) - \sigma_i(\alpha)) = 0$ for $i = 1, \ldots, n-1$. Since the automorphisms $\sigma_1, \ldots, \sigma_n$ are different, for every $i = 1, \ldots, n-1$ there is an element $\alpha_i \in L$ such that $\sigma_n(\alpha_i) \neq \sigma(\alpha_i)$. Choosing $\alpha = \alpha_i$, the equality $a_i(\sigma_n(\alpha) - \sigma_i(\alpha)) = 0$ implies that $a_i = 0$ for $i = 1, \ldots, n-1$. Now we go back to the equality (2), which gives $a_n\sigma_n(x) = 0$ for every $x \in L$. When $x = 1$, we get $a_n = 0$ and the proof is complete. □

Theorems of Chapter 7

T. 7.1 *A finite extension $L \supseteq K$ is normal if and only if L is a splitting field of a polynomial with coefficients in K.*

Proof. Let $L = K(\alpha_1, \ldots, \alpha_n)$ and let f_i be the minimal polynomial of α_i over K for $i = 1, \ldots, n$. According to the definition of a normal extension, every polynomial f_i splits into linear factors in L. The same is true about the product $f = f_1 \cdots f_n$, so L is a splitting field of f over K, since it contains all its zeros and is generated over K by some of them: $\alpha_1, \ldots, \alpha_n$.

Conversely, assume that L is a splitting field of a polynomial $f \in K[X]$. Wa want to show that if an irreducible polynomial $g \in K[X]$ has a zero $\alpha \in L$, then g splits in L into linear factors. Let M be a splitting field of the polynomial g over L and let α' be any zero of g in M. We want to show that $\alpha' \in L$, which will show that g already splits in L. Consider the following chain of field extensions:



Since L is a splitting field of f over K, both $L(\alpha)$ and $L(\alpha')$ are splitting fields of f over $K(\alpha)$ and $K(\alpha')$, respectively. Since $K(\alpha) \cong K(\alpha')$, there is an isomorphism of the splitting fields $L(\alpha)$ and $L(\alpha')$ of f extending an isomorphism of $K(\alpha)$ and $K(\alpha')$. Hence $[L(\alpha) : K(\alpha)] = [L(\alpha') : K(\alpha')]$. Of course, $[K(\alpha) : K] = [K(\alpha') : K]$. Thus

$$[L(\alpha) : L] = \frac{[L(\alpha) : K]}{[L : K]} = \frac{[L(\alpha) : K(\alpha)][K(\alpha) : K]}{[L : K]} =$$
$$\frac{[L(\alpha') : K(\alpha')][K(\alpha') : K]}{[L : K]} = \frac{[L(\alpha') : K]}{[L : K]} = [L(\alpha') : L].$$

But $[L(\alpha) : L] = 1$, since $\alpha \in L$, so $[L(\alpha') : L] = 1$, which means that $L(\alpha') = L$, that is, $\alpha' \in L$. □

T. 7.2 *Let $L = K(\alpha_1, \ldots, \alpha_n)$ be a finite extension. Then a normal closure to $L \supseteq K$ is unique up to a K-isomorphism. More exactly, every normal closure of $L \supseteq K$ is a splitting field over K of $f = f_1 \cdots f_n$, where f_i is the minimal polynomial of α_i over K.*

Proof. Let f_i be the minimal polynomial of α_i over K. If N is a normal closure of $L \supseteq K$, then f_i splits in N. Hence N contains a splitting field of f_i. Let $f = f_1 \cdots f_n$. Then N also contains a splitting field of f. But this splitting field of f is normal, so N coincides with it.

□

Theorems of Chapter 8

T. 8.1 (*a*) *All fields of characteristic* 0 *and all finite fields are perfect.*

(*b*) *If char $(K) = p$, then an irreducible polynomial $f \in K[X]$ is not separable if and only if $f' \equiv 0$, which is equivalent to $f(X) = g(X^p)$, where $g \in K[X]$.*

Proof. (a) Let K be a field of characteristic 0 and let $f(X) = a_nX^n + \cdots + a_1x + a_0 \in K[X]$ be an irreducible polynomial. Let $\gcd(f, f') = d$. Since $\deg f > 0$ and $\mathrm{char}(K) = 0$, we have $f' \neq 0$ (zero polynomial). We have $d \mid f$ and $\deg d \leq \deg f' < \deg f$, so d must be a constant polynomial as a divisor of an irreducible polynomial f. Hence d is a constant polynomial, so by **T.5.3**, the polynomial f is separable.

Assume now that K is a finite field of characteristic p. First note that the function $\sigma(x) = x^p$ is an automorphism of the field K (see Ex. 6.5 (b)) and since K is finite, we have $\sigma(K) = K$ (the number of elements in $\sigma(K)$ and K is the same). This equality says that each element of K is a $p-$th power. Let now $f(X)$ be a minimal polynomial of an algebraic element over K in an extension of this field. We want to show that $f(X)$ is separable. If not, then according to (b) below, there is a polynomial $g \in K[X]$ such that $f(X) = g(X^p) = b_mX^{pm} + \cdots + b_1X^p + b_0$ for same $b_i \in K$. But all b_i are $p-$powers in K, so we have $b_i = c_i^p$ for some $c_i \in K$. Hence

$$f(X) = b_mX^{pm} + \cdots + b_1X^p + b_0 = c_m^pX^{pm} + \cdots + c_1^pX^p + c_0^p = (c_mX^m + \cdots + c_1X + c_0)^p,$$

which shows that $f(X)$ is not irreducible contrary to the assumption. Hence $f(X)$ is separable, which proves our claim concerning the finite field K.

(b) Assume that $f \in K[X]$ is irreducible and not separable. Hence by **T.5.3**, we have $\gcd(f, f') = d$, where d is not a constant polynomial. Since $d|f$ is irreducible, we have $d = f$ (up to a constant), so $f|f'$. This is only possible when f' is identically equal to zero. Since $f'(X) = na_nX^{n-1} + \cdots + 2a_2X + a_1$, we get that the only nonzero coefficients a_i in $f(X)$ may be those, which correspond to X^i for i divisible by p – if X^i has nonzero coefficient in $f(X)$ and $p \nmid i$, then the coefficient of X^{i-1} in the derivative is also nonzero, so the derivative is nonzero. Hence $f(X)$ is a polynomial in X^p, that is, $f(X) = g(X^p)$ for some $g(X) \in K[X]$. Conversely, it is clear that an irreducible polynomial $f(X) = g(X^p)$ is not separable, since $f'(X) \equiv 0$ so $\gcd(f, f') = f$, which means that $f(X)$ has multiple zeros in an extension of K. □

T. 8.2 Primitive element theorem. *If $L = K(\alpha_1, \ldots, \alpha_n)$, where $\alpha_1, \ldots, \alpha_n$ are algebraic and all with possibly one exception are separable over K, then there is a primitive element of L over K. In particular, every finite separable extension has a primitive element.*

Proof. First we assume that K is an infinite field. It suffices if we show that if $L = K(\alpha, \beta)$, then $L = K(\theta)$ for a suitable $\theta \in L$. Let f and g be the minimal polynomials of α and β over K and let

$$f(X) = (X - \alpha_1) \ldots (X - \alpha_n),$$
$$g(X) = (X - \beta_1) \ldots (X - \beta_m),$$

where $\alpha_1 = \alpha$, $\beta_1 = \beta$. According to the assumption all zeros of f or g are different (f or g is separable polynomial). Assume that g is separable. Choose $c \in K$ so that

$$\alpha_i + c\beta_j \neq \alpha_1 + c\beta_1$$

for all $(i,j) \neq (1,1)$. The existence of c follows from the fact that

$$\alpha_i + x\beta_j = \alpha_1 + x\beta_1$$

holds for finitely many $x \in K$ (less than mn "bad" x). Define:

$$\theta = \alpha + c\beta$$

We have $K(\theta) \subseteq K(\alpha,\beta)$. We want to show that $K(\alpha,\beta) \subseteq K(\theta)$. It suffices if we show that $\beta \in K(\theta)$, since then $\alpha = \theta - c\beta \in K(\theta)$. Consider the polynomials:

$$f(\theta - cX) \quad \text{and} \quad g(X).$$

These polynomials have coefficients in $K(\theta)$ and they have a common zero β, since

$$f(\theta - c\beta) = f(\alpha) = 0 \quad \text{and} \quad g(\beta) = 0.$$

They do not have any other common zeros, since if $f(\theta - c\beta_j) = 0$ for some j, then $\theta - c\beta_j = \alpha_i$ for some i. Thus $\alpha_i + c\beta_j = \theta = \alpha + c\beta$, which occurs only if $i = j = 1$. This shows that

$$GCD(f(\theta - cX),\, g(X)) = X - \beta$$

But the greatest common divisor of two polynomials with coefficients in $K(\theta)$ is a polynomial with coefficients in $K(\theta)$, so $\beta \in K(\theta)$.

If K is a finite field[1], then L is a finite field as well and its multiplicative group of nonzero elements is cyclic (see Ex. 5.7). Any generator of this group is a (field) primitive element of L over K. □

Theorems of Chapter 9

T. 9.1 *Let $L \supseteq K$ be a finite field extension and $G(L/K)$ its Galois group. Then the following conditions are equivalent:*

(*a*) $[L : K] = |G(L/K)|$;

(*b*) $L^{G(L/K)} = K$;

(*c*) *There is a group G of K-automorphisms of L such that $K = L^G$ and then, $G = G(L/K)$;*

(*d*) *$L \supseteq K$ is normal and separable;*

(*e*) *L is a splitting field of a separable polynomial over K.*

Proof. (*a*) ⇒ (*b*) We have the following chain of fields:

[1] There exists a proof of the theorem on primitive element, which works for both finite and infinite fields K. See [BR].

$$K \subseteq L^{G(L/K)} \subseteq L$$

and according to **T.6.2**, we get $[L : L^{G(L/K)}] = |G(L/K)|$. Since also $[L : K] = |G(L/K)|$, by **T.4.3**, we get $[L^{G(L/K)} : K] = [L : K]/[L : L^{G(L/K)}] = 1$, that is, $L^{G(L/K)} = K$.

$(b) \Leftrightarrow (c)$ is evident, since taking $G = G(L/K)$, we get that (b) implies (c). The converse follows if we note that $G \subseteq G(L/K)$ gives $K \subseteq L^{G(L/K)} \subseteq L^G \subseteq L$. Since $L^G = K$, we get $L^{G(L/K)} = K$, which gives (b). Moreover, if $L^G = K$, then Artin's Lemma **T.6.2** and the inclusion $G \subseteq G(L/K)$ imply that $G = G(L/K)$.

$(b) \Rightarrow (d)$ We have to show that if $f(X) \in K[X]$ is an irreducible polynomial such that $f(\alpha) = 0$ for some $\alpha \in L$, then $f(X)$ splits in L as a product of linear factors (normality) and all solutions of the equation $f(X) = 0$ in L are different (separability).

Let $G = \{\sigma_1, \ldots, \sigma_n\}$ and let $X = \{\alpha_1, \ldots, \alpha_r\}$ be the set of all diffrent images $\sigma_i(\alpha)$ for $i = 1, \ldots, n$. We assume that $\sigma_1 = id$, so $\alpha_1 = \alpha$. Notice that by the definition of X, if $\alpha_i \in X$, then $\sigma(\alpha_i) \in X$ for $\sigma \in G$, so every $\sigma \in G$ gives a permutation of the elements of X.

Consider the polynomial

$$g(X) = (X - \alpha_1) \cdots (X - \alpha_r).$$

We claim that $g(X) \in K[X]$. In fact, the coefficients of this polynomial are $\alpha_1 + \cdots + \alpha_r$, $\alpha_1\alpha_2 + \cdots + \alpha_{r-1}\alpha_r$, ..., $\alpha_1 \cdots \alpha_r$ (all fundamental symmetric expressions in $\alpha_1, \ldots, \alpha_r$) and every $\sigma \in G$ permutes all the α_i leaving the coefficients unchanged:

$$\sigma(\alpha_1 + \cdots + \alpha_r) = \sigma(\alpha_1) + \cdots + \sigma(\alpha_r) = \alpha_1 + \cdots + \alpha_r$$

$$\sigma(\alpha_1\alpha_2 + \cdots + \alpha_{r-1}\alpha_r) = \sigma(\alpha_1\alpha_2) + \cdots + \sigma(\alpha_{r-1}\alpha_r) = \alpha_1\alpha_2 + \cdots + \alpha_{r-1}\alpha_r$$

$$\cdots$$

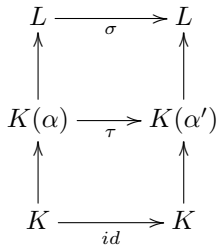
$$\sigma(\alpha_1 \cdots \alpha_r) = \sigma(\alpha_1) \cdots \sigma(\alpha_r) = \alpha_1 \cdots \alpha_r$$

Thus by (b), the coefficients of $g(X)$ belong to $L^{G(L/K)} = K$. Since $f(X)$ is irreducible in $K[X]$, has a zero α, and $g(X)$ is a polynomial in $K[X]$ which also has a zero α, we get that $f(X)$ divides $g(X)$. Hence all zeros of $f(X)$ are in L and are different.

$(d) \Rightarrow (e)$ Let $L = K(\alpha_1, \ldots, \alpha_n)$ be finite, normal and separable. Let $f_i(X)$ be the minimal polynomial of α_i over K for $i = 1, \ldots, n$. Then $f_i(X)$ is irreducible and has a zero in L, so it is separable and has all its zeros in L. Thus $f(X) = f_1(X) \cdots f_n(X)$ is separable and L is its splitting field over K.

$(e) \Rightarrow (a)$ Let $L = K(\alpha_1, \ldots, \alpha_n)$ be a splitting field of a separable polynomial $f(X) = a(X - \alpha_1) \cdots (X - \alpha_n)$, $a \in K$. We use induction with respect to the degree $[L : K]$. If $[L : K] = 1$, then of course, $|G(L/K)| = 1$. Assume that $[L : K] > 1$. Then there exists i such that $\alpha_i \notin K$. We may assume that $i = 1$, so $\alpha = \alpha_1$ is a solution to the equation $f_1(X) = 0$, where $f_1(X)$ is an irreducible factor of $f(X)$ and $\deg f_1 = d > 1$. Since f is separable, $f_1(X) = 0$ has d different solutions in L. Let α' be any of the solutions to $f_1(X) = 0$ in L. As we know, there is an isomorphism $\tau : K(\alpha) \to K(\alpha')$ such that $\tau(\alpha) = \alpha'$ and τ is the identity on K. The number of such τ is exactly d since $\tau(f_1(\alpha)) = f_1(\tau(\alpha)) = 0$, so there are exactly d possibilities for $\tau(\alpha)$ as solutions to the equation $f_1(X) = 0$ in L.

We have the following field extensions:



Now consider $f(X)$ as a separable polynomial with coefficients in $K(\alpha)$. Then L is its splitting field. $[L : K(\alpha)] = [L : K]/[K(\alpha) : K] < [L : K]$, so we can use the inductive assumption. Each choice of τ gives $[L : K(\alpha)] = [L : K]/[K(\alpha) : K] = [L : K]/d$ different choices of σ. Thus the total number of extensions σ of $id : K \to K$ equals $d \cdot [L : K]/d = [L : K]$. □

If $L \supseteq K$ is a field extension, $\mathcal{F}$ the set of all fields between K and L and $\mathcal{G}$ the set of all subgroups to $G(L/K)$, then we define two functions:

$$f : \mathcal{G} \to \mathcal{F} \quad \text{and} \quad g : \mathcal{F} \to \mathcal{G}$$

in the following way:

$$f(H) = L^H = \{x \in L : \forall_{\sigma \in H} \sigma(x) = x\}$$

and

$$g(M) = G(L/M) = \{\sigma \in G(L/K) : \forall_{x \in M} \sigma(x) = x\}.$$

T. 9.2 The main theorem of Galois theory. *If $L \supseteq K$ is a finite Galois extension, then f and g are the inverse anti-automorphisms between partially ordered by inclusion sets $\mathcal{F}$ of all fields between K and L and the set $\mathcal{G}$ of all subgroups to $G(L/K)$, that is, $f \circ g = id_{\mathcal{F}}$, $g \circ f = id_{\mathcal{G}}$ and $f(H_1) \supseteq f(H_2)$ if $H_1 \subseteq H_2$, and $g(M_1) \supseteq g(M_2)$ if $M_1 \subseteq M_2$.*

Proof. We show $fg = id_{\mathcal{F}}$ and $gf = id_{\mathcal{G}}$, which says that f and g are mutually inverse bijections. We have

$$fg(M) = f(G(L/M)) = L^{G(L/M)} = M$$

according to **T.9.1** (b), since by **T.9.3** (a) the extension $L \supseteq M$ is Galois. We have also

$$gf(H) = g(L^H) = G(L/L^H) = H,$$

where the last equality is a direct consequence of **T.9.1** (c).

The last statement concerning inverting of inclusions follows immediately from the definitions of $f(H)$ and $g(M)$. □

T. 9.3 *Let $K \subseteq L$ be a Galois extension and M a field between K and L.*

(a) The extension $L \supseteq M$ is a Galois extension.

(b) The extension $M \supseteq K$ is a Galois extension if and only if $G(L/M)$ is normal in $G(L/K)$. If this holds, then $G(M/K) \cong G(L/K)/G(L/M)$.

Proof. (a) Since $K \subseteq L$ is a Galois extension, it is a splitting field of a separable polynomial $f(X) \in K[X]$. L is a splitting field of the same polynomial over M. Thus $M \subseteq L$ is a Galois extension.

(b) Let $K \subseteq M$ be a Galois extension and let $\sigma \in G(L/K)$. We claim that the restriction of σ to M belongs to the Galois group $G(M/K)$. In fact, if $\alpha \in M$ and $g(X)$ is the minimal polynomial of α over K, then $g(\sigma(\alpha)) = \sigma(g(\alpha)) = 0$, so $\sigma(\alpha) \in M$, since all solutions of $g(X) = 0$ belong to M (since M is Galois over K, $g(X)$ is irreducible in K and has one zero α in M). Consider the group homomorphism

$$\varphi : G(L/K) \to G(M/K)$$

such that $\varphi(\sigma) = \sigma_{|M}$. The kernel of this homomorphism consists of all automorphisms $\sigma \in G(L/K)$ which map onto the identity $\sigma_{|M} = id_M$, that is, the kernel is $G(L/M)$. Thus $G(L/M)$ is a normal subgroup of $G(L/K)$.

Conversely, assume that $G(L/M)$ is a normal subgroup of $G(L/K)$. Then for every $\sigma \in G(L/K)$ and every $\tau \in G(L/M)$, we have $\sigma^{-1}\tau\sigma \in G(L/M)$. Let $\alpha \in M$. Then $\sigma^{-1}\tau\sigma(\alpha) = \alpha$, that is, $\tau\sigma(\alpha) = \sigma(\alpha)$. Hence $\sigma(\alpha) \in M$ as an element fixed by all automorphisms $\tau \in G(L/M)$ (remember that $M \subseteq L$ is Galois by (a)). Hence, the homomorphism φ is defined – it maps every K-automorphism of L onto its restriction to M. It follows from Theorem **T.5.2** (b) that φ is surjective, since every automorphism $\tau \in G(M/K)$ can be extended to an automorphism $\sigma \in G(L/K)$ (that is, σ restricted to M equals τ). According to the main theorem on group homomorphisms, we have

$$\frac{G(L/K)}{G(L/M)} \cong \varphi(G(L/K)) = G(M/K).$$

This gives:

$$|G(M/K)| = \left|\frac{G(L/K)}{G(L/M)}\right| = \frac{|G(L/K)|}{|G(L/M)|} = \frac{[L:K]}{[L:M]} = [M:K],$$

that is, $K \subseteq M$ is a Galois extension. □

Theorems of Chapter 10

T. 10.1 *(a) The degree* $[\mathbb{Q}(\varepsilon):\mathbb{Q}] = \varphi(n)$*, where* ε *is a primitive* $n-$*th root of unity and* φ *is the Euler function.*

(b) Each automorphism σ *in the Galois group* $G(\mathbb{Q}(\varepsilon)/\mathbb{Q})$ *is given by* $\sigma_k(\varepsilon) = \varepsilon^k$*, where* $k \in \{1,\dots,n\}$ *and* $\gcd(k,n) = 1$*. The mapping* $\sigma_k \mapsto k \pmod n$ *gives an isomorphism* $G(\mathbb{Q}(\varepsilon)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$.

Proof. (a) Let ε be any primitive n-th root of unity. Let $f(X)$ be the minimal polynomial of ε. Since $\varepsilon^n = 1$, the polynomial $f(X)$ divides $X^n - 1$. Let $X^n - 1 = f(X)q(X)$. Hence the field $\mathbb{Q}(\varepsilon)$ is the splitting field of $f(X)$ as well as of $X^n - 1$, since all zeros of these polynomials are the powers ε^k for $k = 0, 1, \dots, n-1$. The polynomial $f(X)$ is monic, has rational coefficients and divides $X^n - 1$. Hence, it has integer coefficients by Ex. 3.11. We want to prove that the zeros of $f(X)$ are exactly all $\varphi(n)$ primitive n-th roots of unity ε^k, where $\gcd(k,n) = 1$.

First we show that every zero of $f(X)$ is $n-$th primitive root of unity. Let ε^k be a zero of $f(X)$ in $\mathbb{Q}(\varepsilon)$. According to **T.5.1**, there is an automorphism σ of this field such that $\sigma(\varepsilon) = \varepsilon^k$. The automorphism σ maps $n-$th roots of unity onto $n-$th roots of unity and since the powers of ε are all such roots, so even all the powers of ε^k must be all of them. Hence k must be relatively prime to n, so that ε^k is a primitive $n-$th root of unity. (This argument shows that if a primitive n-th root of unity is a zero of an irreducible polynomial, then all other zeros of this polynomial are also primitive n-th roots of unity.)

Now we prove that any primitive $n-$th root of unity is among the zeros of $f(X)$. Let p be an arbitrary prime relatively prime to n. We want to show that ε^p is also a zero of $f(X)$. If it is true, then it will follow that all ε^k for k relatively prime to n are zeros of $f(X)$. In fact, the exponent $k = p_1 \cdots p_r$ is a product of prime numbers, so starting with ε as a zero of $f(X)$, we get ε^{p_1}, $\varepsilon^{p_1 p_2}, \dots$ as zeros of $f(X)$. After r steps, we get ε^k as a zero of $f(X)$.

Assume that ε^p is not a zero of $f(X)$ and let $g(X)$ be its minimal polynomial. Observe that $f(X)$ and $g(X^p)$ have a common zero ε. Since $f(X)$ is irreducible, it divides $g(X^p)$. Let $g(X^p) = f(X)h(X)$, where $h(X)$ is a monic integer polynomial.

Now we want to prove that $f(X)$ and $g(X)$ have a common zero. The zeros of both these polynomials are n-th roots of 1, so if all these zeros are different, then $X^n - 1 = f(X)g(X)q(X)$ for some polynomial $q(X) \in \mathbb{Z}[X]$. Reduce the equalities:

$$X^n - 1 = f(X)g(X)q(X) \qquad \text{and} \qquad g(X^p) = f(X)h(X)$$

modulo p, that is, consider the images of all involved polynomials in $\mathbb{F}_p[X]$. Since $p \nmid n$, the derivative nX^{n-1} of $X^n - 1$ is nonzero, so all zeros of this polynomial are different (see **T.5.3**). Hence the zeros of $f(X)$ and $g(X)$ are also different when considered over $\mathbb{F}_p$. But the second equality says that $g(X)^p = f(X)h(X)$, since $g(X^p) = g(X)^p$ over $\mathbb{F}_p$. Hence the zeros of $f(X)$ are among the zeros of $g(X)$. This contradiction shows that $f(X)$ and $g(X)$ have common zeros already over $\mathbb{Q}$. Since both f and g are monic and irreducible with common zero, they are equal. Hence $f(\varepsilon) = 0$ implies $f(\varepsilon^p) = 0$ for each $p \nmid n$. As we noted above, this implies that all $\varphi(n)$ primitive n-th roots of 1 are the zeros of $f(X)$, so $f(X) = \Phi_n(X)$ proving that this polynomial is irreducible.

(b) Let ε be a primitive n-th root of unity. We already know that $\Phi_n(X)$ is the minimal polynomial of ε and its zeros are ε^k for k such that $\gcd(k, n) = 1$ and $k \in \{1, \ldots, n-1\}$. By **T.5.1**, all automorphisms of $\mathbb{Q}(\varepsilon)$ are defined by the images of ε, that is, $\sigma_k(\varepsilon) = \varepsilon^k$ for all k as above. Now notice that $\sigma_k\sigma_l(\varepsilon) = \sigma_k(\sigma_l(\varepsilon)) = \sigma_k(\varepsilon^l) = \varepsilon^{kl} = \sigma_{kl}(\varepsilon)$, where the index kl (in σ_{kl}) is taken modulo n, since $\varepsilon^{kl} = \varepsilon^{kl \pmod n}$ as $\varepsilon^n = 1$. Notice also that $\gcd(kl, n) = 1$, when $\gcd(k, n) = \gcd(l, n) = 1$. Thus the mapping $\varphi : G(\mathbb{Q}(\varepsilon)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^*$, where $\varphi(\sigma_k) = k$ is a bijection and $\varphi(\sigma_k\sigma_l) = \varphi(\sigma_{kl}) = kl \pmod n = \varphi(\sigma_k)\varphi(\sigma_l)$ is a group isomorphism. □

T. 10.2 *Let K be a field whose characteristic does not divide n.*

(a) We have:

$$X^n - 1 = \prod_{d|n} \Phi_{d,K}(X) \qquad \textit{and} \qquad \Phi_{n,K}(X) = \prod_{d|n} (X^d - 1)^{\mu(\frac{n}{d})},$$

where μ denotes the Möbius function (see Ex. 5.6).

(b) The cyclotomic polynomials $\Phi_{n,K}(x)$ are monic and their coefficients are integer multiples of the unity in K.

(c) All irreducible factors of $\Phi_{n,K}(X)$ are of the same degree.

(d) If $K = \mathbb{Q}$, then $\Phi_n(X) = \Phi_{n,\mathbb{Q}}(X)$ is irreducible over $\mathbb{Q}$.

Proof. (a) Since the characteristic of K does not divide n, the polynomial $X^n - 1$ has n different zeros, as its derivative nX^{n-1} is relatively prime to it (see **T.5.3**). Every $n-$th root of unity is a zero of exactly one polynomial $\Phi_{d,K}(X)$ for $d \mid n$. This proves the first identity in (a).

The second identity follows immediately from the first one and **A.10.3** if we choose $G = K(X)^*$, the group of rational functions $p(X)/q(X)$, where $p(X), q(X) \in K[X]$ with multiplication as group operation and $f(n) = X^n - 1$, $g(n) = \Phi_{n,K}(X)$.

(b) We prove the claim by induction. If $n = 1$, the $\Phi_{1,K}(X) = X - 1$ so (b) is true in this case. Assume that it is true for all positive integers $m < n$. Hence the coefficients of the

polynomial $\prod \Phi_{d,K}(X)$, where $d \mid n$ and $d < n$ are all integer multiples of the unit in the field K. According to (a), we have

$$\Phi_{n,K}(X) = \frac{X^n - 1}{\prod_{d<n, d|n} \Phi_{d,K}(X)}$$

so the division algorithm shows that also the coefficients of $\Phi_{n,K}(X)$ are all integer multiples of the unity in K.

It is easy to deduce (b) from Gauss's Lemma (see **T.3.3**) when $K = \mathbb{Q}$. In fact, since the zeros of $\Phi_{n,\mathbb{Q}}(X)$ are n-th roots of 1, it is a divisor of $X^n - 1$, which is a polynomial with integer coefficients. According to Gauss's Lemma, there exists a rational number r such that $r\Phi_{n,\mathbb{Q}}(X)$ has integer coefficients and divides $X^n - 1$. The polynomials $X^n - 1$ and $\Phi_{n,\mathbb{Q}}(X)$ are monic. Hence the polynomial $r\Phi_{n,\mathbb{Q}}(X)$ is also monic (as an integer divisor of $X^n - 1$) and $r = 1$. Thus $\Phi_{n,\mathbb{Q}}(X)$ has integer coefficients.

(c) Let ε be any primitive $n-$th root of unity and let $f(X)$ be its minimal polynomial over K. Then $K(\varepsilon)$ is the splitting field of $f(X)$ as well as of the polynomial $X^n - 1$ whose all zeros are in $K(\varepsilon)$, since they are powers of ε. If η is any other primitive $n-$th root of unity, then $K(\varepsilon) = K(\eta)$, so the minimal polynomial of η over K has the same degree as the degree of $f(X)$ (see **T.4.2**).

(d) This was proved in **T.10.1** (a). □

Theorems of Chapter 11

T.11.1 *Let $K \subseteq L$ be a Galois extension and $G(L/K) = \{\sigma_1 = 1, \sigma_2, \ldots, \sigma_n\}$ its Galois group. Then the following properties of the extension $K \subseteq L$ hold and are equivalent:*

(a) There exists $\alpha \in L$ such that $\sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_n(\alpha)$ is a basis of L over K.

(b) L^+ is a cyclic $K[G]-$module, that is, there is $\alpha \in L$ such that $L^+ = K[G]\alpha$ for some $\alpha \in L$.

In order to prove the existence of normal bases, we need two auxiliary results:

Lemma 11.1. *Let $K \subseteq L$ be a Galois extension and $G(L/K) = \{\sigma_1 = id, \sigma_2, \ldots, \sigma_n\}$. The elements $\alpha_1, \ldots, \alpha_n \in L$ form a basis of L over K if and only if* $\det[\sigma_i(\alpha_j)] \neq 0$.

Proof. The given elements are linearly dependent if and only if there are elements $a_1, \ldots, a_n \in K$ not all equal to 0 such that $a_1\alpha_1 + \cdots + a_n\alpha_n = 0$. Letting all σ_i act on this equality, we get

$$
\begin{aligned}
&a_1\sigma_1(\alpha_1) + \cdots + a_n\sigma_1(\alpha_n) = 0\\
&a_1\sigma_2(\alpha_1) + \cdots + a_n\sigma_2(\alpha_n) = 0\\
&\cdots\\
&a_1\sigma_n(\alpha_1) + \cdots + a_n\sigma_n(\alpha_n) = 0.
\end{aligned}
$$

The above system of linear equations has a non-zero solution $a_1, \ldots, a_n$ if and only if the determinant of the coefficient matrix (consisting of $\sigma_i(\alpha_j)$) equals 0. □

Lemma 11.2. *Let $f(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$ be a non-zero polynomial and let A be an infinite subset of K. Then there exist $a_1, \ldots, a_n \in A$ such that $f(a_1, \ldots, a_n) \neq 0$.*

Proof. We use induction with respect to n. If $n = 1$, then some element of A is not a zero of $f(X)$, since the number of zeros of $f(X)$ is finite. Assume that $n > 1$ and the statement is true for polynomials whose number of variables is less than n. Write $f(X_1, \ldots, X_n)$ as a polynomial with respect to X_n with coefficients depending on $X_1, \ldots, X_{n-1}$, that is,

$$
f(X_1, \ldots, X_n) = a_k(X_1, \ldots, X_{n-1})X_n^k + \cdots + a_1(X_1, \ldots, X_{n-1})X_n + a_0(X_1, \ldots, X_{n-1})
$$

Let $a(X_1, \ldots, X_{n-1})$ be the product of those $a_i(X_1, \ldots, X_{n-1})$ for $i = 0, 1, \ldots, k$, which are non-zero. By the inductive assumption, we can find $a_1, \ldots, a_{n-1} \in A$ such that $a(a_1, \ldots, a_{n-1}) \neq 0$. We consider then $f(a_1, \ldots, a_{n-1}, X_n)$ which is a non-zero polynomial in the variable X_n. Hence we can find $a_n \in A$ such that $f(a_1, \ldots, a_{n-1}, a_n) \neq 0$ by the case $n = 1$. Thus we have $a_1, \ldots, a_n \in A$ satisfying our requirement.

Proof of NBT in the infinite case. Let $e_1, \ldots, e_n$ be any basis of L over K and consider n linear forms in the polynomial ring $L[X_1, \ldots, X_n]$ given by:

$$
\begin{aligned}
X_{\sigma_1} &= \sigma_1(e_1)X_1 + \cdots + \sigma_1(e_n)X_n\\
X_{\sigma_2} &= \sigma_2(e_1)X_1 + \cdots + \sigma_2(e_n)X_n\\
&\cdots\\
X_{\sigma_n} &= \sigma_n(e_1)X_1 + \cdots + \sigma_n(e_n)X_n
\end{aligned}
\qquad (*)
$$

Look at X_{σ_i} as functions of $X_1, \ldots, X_n$. Define $f(X_1, \ldots, X_n) = \det[X_{\sigma_i\sigma_j}]$. We claim that this polynomial is non-zero. In fact, we can choose $X_{\sigma_1} = 1, X_{\sigma_2} = 0, \ldots, X_{\sigma_n} = 0$ and find the suitable values of $X_1, \ldots, X_n$ solving the system $(*)$. Such a solution exists (and is unique), since $\det[\sigma_i(e_j)] \neq 0$ (see Lemma **11.1**). For these values of $X_1, \ldots, X_n$ the determinant defining $f(X_1, \ldots, X_n)$ has elements 0 or 1 with exactly one 1 in each row and each column. Thus the value of $f(X_1, \ldots, X_n)$ is ± 1, which implies that this is a non-zero polynomial.

As K is an infinite subset of L, using Lemma **11.2**, we choose $a_1, \ldots, a_n \in K$ such that $f(a_1, \ldots, a_n) \neq 0$ and define $\alpha = a_1e_1 + \cdots + a_ne_n$. Then by $(*)$ and the definition of $f(X_1, \ldots, X_n)$, we get

$$f(a_1, \ldots, a_n) = \det[\sigma_i \sigma_j(\alpha)] \neq 0.$$

Thus, $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ are linearly independent over K by Lemma **11.1**, so these elements form a normal basis of L over K. ■

Proof of NBT in the finite case. Let $K \subseteq L$ be a field extension of finite fields. Now we want to prove the normal basis theorem in this case. As we know, the field L is a cyclic Galois extension of K. In fact, the argument given below applies to any cyclic Galois extension $K \subseteq L$ (not necessarily finite), so it gives an alternative proof of the theorem in this case.

Let $G = G(L/K) = \langle \sigma \rangle$ be the Galois group, where σ is any of its generators and $[L : K] = |G(L/K)| = n$, so σ has order n. The field L can be considered as a module over the polynomial ring $K[X]$ when we define $X\alpha = \sigma(\alpha)$ for $\alpha \in L$ (see **A.7**). As all modules over $K[X]$ having finite dimension over K, the module L is a direct sum of modules of the form $K[X]/(f)$, where f is a nonzero polynomial in $K[X]$ dividing the annihilator of L (see **A.7.3**). Since $\sigma^n = 1$, we have $(X^n - 1)\alpha = \sigma^n(\alpha) - \alpha = 0$ for all $\alpha \in L$, so $X^n - 1$ belongs to the annihilator of L. Thus the annihilator of L divides $X^n - 1$ (see **A.7.3**). If the annihilator is generated by a polynomial $a_0 + a_1 X + \cdots + a_{n-1}X^{n-1} \in K[X]$ of degree less than n, then

$$(a_0 + a_1 X + \cdots + a_{n-1}X^{n-1})\alpha = a_0\alpha + a_1\sigma(\alpha) + \cdots + a_{n-1}\sigma^{n-1}(\alpha) = 0$$

for any $\alpha \in L$. But according to Dedekind's Lemma **T.6.3**, the automorphisms $\sigma^0 = 1, \sigma, \ldots, \sigma^{n-1}$ are linearly independent over L and consequently over K, so all $a_i = 0$. Thus $X^n - 1$ must be the annihilator of L and L is isomorphic to $K[X]/(X^n - 1)$ as $K[X]$-module. If $\varphi : K[X]/(X^n - 1) \to L$ is an isomorphism and $\varphi(1) = \alpha$, then every element of L is of the form

$$(a_0 + a_1 X + \cdots + a_{n-1}X^{n-1})\alpha = a_0\alpha + a_1\sigma(\alpha) + \cdots + a_{n-1}\sigma^{n-1}(\alpha),$$

since every element of $K[X]/(X^n - 1)$ is of the form $(a_0 + a_1 X + \cdots + a_{n-1}X^{n-1}) \cdot 1$. Thus $\alpha, \sigma(\alpha), \ldots, \sigma^{n-1}(\alpha)$ form a basis of L over K, since the number of these elements is n and they generate L over K. □

T. 11.2 Hilbert's Theorem 90. *Let $L \supseteq K$ be a cyclic extension of degree n and let σ be a generator of the Galois group $G = G(L/K)$. If $\alpha \in L$, then*

(a) $\mathrm{Nr}_G(\alpha) = 1$ *if and only there is* $\beta \in L$ *such that* $\alpha = \frac{\beta}{\sigma(\beta)}$.

(b) $\mathrm{Tr}_G(\alpha) = 0$ *if and only if there is* $\beta \in L$ *such that* $\alpha = \beta - \sigma(\beta)$.

Proof. (a) First recall that $\mathrm{Nr}_G(\alpha) = \alpha\sigma(\alpha)\cdots\sigma^{n-1}(\alpha)$. Define

$$\alpha_{\sigma^i} = \alpha\sigma(\alpha)\cdots\sigma^{i-1}(\alpha)$$

for $i = 1, \ldots, n$ and observe that $\alpha_{\sigma^n} = 1$ and $\sigma(\alpha_{\sigma^i}) = \frac{1}{\alpha}\alpha_{\sigma^{i+1}}$. Since $\alpha_\sigma = \alpha \neq 0$, by Dedekind's Lemma **T.6.3**, we can find $x \in L$ such that

$$\beta = \alpha_\sigma \sigma(x) + \alpha_{\sigma^2}\sigma^2(x) + \cdots + \alpha_{\sigma^{n-1}}\sigma^{n-1}(x) + \alpha_{\sigma^n}\sigma^n(x) \neq 0.$$

Now observe that $\sigma(\beta) = \frac{1}{\alpha}\beta$, which proves the result as $\sigma(\beta) \neq 0$.

(b) The proof is similar. Using Dedekind's Lemma **T.6.3**, we can find $x \in L$ such that $\mathrm{Tr}_G(x) = x + \sigma(x) + \cdots + \sigma^{n-1}(x) \neq 0$. Define

$$\alpha_{\sigma^i} = \alpha + \sigma(\alpha) + \cdots + \sigma^{i-1}(\alpha)$$

for $i = 1, \ldots, n$ and observe that $\alpha_{\sigma^n} = \mathrm{Tr}_G(\alpha) = 0$ and $\sigma(\alpha_{\sigma^i}) = \alpha_{\sigma^{i+1}} - \alpha$. As in (a), consider

$$\gamma = \alpha_\sigma \sigma(x) + \alpha_{\sigma^2}\sigma^2(x) + \cdots + \alpha_{\sigma^{n-1}}\sigma^{n-1}(x) + \alpha_{\sigma^n}\sigma^n(x)$$

and notice that $\sigma(\gamma) = \gamma - \mathrm{Tr}_G(x)\alpha$. Hence $\alpha = \frac{1}{\mathrm{Tr}_G(x)}(\gamma - \sigma(\gamma))$. Now we choose $\beta = \frac{\gamma}{\mathrm{Tr}_G(x)}$ and obtain $\alpha = \beta - \sigma(\beta)$. □

T. 11.3 *Let K be a field containing n different n-th roots of unity. If L is a cyclic extension of K of degree n, then there exists $\alpha \in L$ such that $L = K(\alpha)$ and $\alpha^n \in K$.*

We give two proofs of this theorem. The first depends on Dedekind's Lemma **T.6.3**. The second is more direct, but needs a little more knowledge of linear algebra.

First proof. Let σ be a generator of the Galois group $G(L/K)$. According to Dedekind's Lemma **T.6.3**, there exists $x \in L$ such that

$$\alpha = x + \varepsilon\sigma(x) + \cdots + \varepsilon^{n-1}\sigma^{n-1}(x) \neq 0.$$

Notice now that $\sigma(\alpha) = \varepsilon^{n-1}\alpha$ (this says that α is an eigenvector belonging to the eigenvalue $\varepsilon^{n-1} = \varepsilon^{-1}$ of σ). Hence $\sigma^i(\alpha) = \varepsilon^{i(n-1)}\alpha^n$ for $i = 1, \ldots, n$, which shows that the images of α by all automorphisms of the Galois group are different. Hence, by Ex. 9.22, we have $L = K(\alpha)$. Moreover, we have $\sigma(\alpha^n) = (\sigma(\alpha))^n = (\varepsilon^{n-1}\alpha)^n = \alpha^n$, so $\alpha^n \in L^{G(L/K)} = K$. □

Second proof. Let σ be a generator of the Galois group of L over K. Since $\sigma^n = id$, the eigenvalues of σ as a linear mapping of L over K satisfy the equation $X^n - 1 = 0$. In fact, if $\sigma(\alpha) = \varepsilon\alpha$ for $\alpha \in L, \alpha \neq 0$, then $\sigma^n(\alpha) = \varepsilon^n\alpha$, that is, $\varepsilon^n = 1$. But $\varepsilon \in K$, so we can choose ε in K as a generator of the cyclic group of all solution of $X^n - 1 = 0$ and find an eigenvector $\alpha \in L$ belonging to it. We have $\sigma^i(\alpha) = \varepsilon^i\alpha$ for $i = 1, \ldots, n$, so α is fixed only by the identity automorphism of L over K (if $i \neq n$, then $\varepsilon^i\alpha \neq \alpha$). Hence $L = K(\alpha)$. Moreover, $\sigma^i(\alpha^n) = \varepsilon^{in}\alpha^n = \alpha^n$. Thus, α^n is fixed by all the elements of the Galois group of L over K, that is, $\alpha^n = a \in K$. □

T. 11.4 *Let K be a field containing m different m-th roots of 1.*

(a) If $K \subseteq L$ is a Kummer extension of exponent m, then every subextension of fields $M \subseteq N$, where $K \subseteq M \subseteq N \subseteq L$ is also a Kummer extension.

(b) All Kummer extensions of K of exponent m are exactly the splitting fields of sets of binomial polynomials $X^m - a$ for some $a \in K$. In particular, all finite Kummer extensions of K are $L = K(\sqrt[m]{a_1}, \ldots, \sqrt[m]{a_r})$ for some elements $a_1, \ldots, a_r \in K$.

(c) There is a one-to-one correspondence between the isomorphism classes of finite Kummer extensions of K of exponent m and the subgroups A of K^* containing K^{*m} such that the index $[A : K^{*m}]$ is finite. In this correspondence, to a Kummer extension L of K corresponds the subgroup A of K^* consisting of all $a \in K$ such that $a = \alpha^m$ for some $\alpha \in L$, and to a subgroup A of K^* corresponds any splitting field over K of all binomials $X^m - a$ for $a \in A$. Moreover,

$$|G(L/K)| = [L : K] = [A : K^{*m}]. \tag{11.1}$$

Proof. (a) It is clear that the field M contains m different m-th roots of 1. Since the Galois group $G(L/K)$ is abelian, the Galois group $G(N/M)$ is also abelian as the quotient $G(L/M)/G(L/N)$ (see **T.9.3**). Since every element of $G(L/M)$ has order dividing m, the same is true about the elements of the quotient, that is, the elements of $G(M/N)$.

(b) Let L be a splitting field of a set of binomials $X^m - a$ for $a \in K$. We shall prove that L is a Kummer extension of K of exponent m. According to the assumptions, the field K contains m different m-th roots of 1, so we have to prove that L is an abelian Galois extension of K and $\sigma^m = 1$ for each $\sigma \in G(L/K)$.

The extension $K \subseteq L$ is normal as a splitting field of polynomials over K (see **T.7.1**) and separable, since every polynomial $X^m - a$, where $a \in K$, $a \neq 0$, is separable. In fact, as we noted earlier, such a binomial has m different zeros. Thus L is a Galois extension of K. Since L is generated by the zeros of binomials $X^m - a$ for $a \in K$, every automorphism $\sigma \in G(L/K)$ is uniquely defined by its action on the generators of this form. So let $\sigma, \tau \in G(L/K)$ and let $\alpha, \beta \in L$ be such that $\alpha^m = a, \beta^m b$, where $a, b \in K$. Then we have $\sigma(\alpha) = \varepsilon\alpha$ and $\sigma(\beta) = \eta\beta$, where ε, η are m-th roots of 1. Hence $\sigma\tau(\alpha) = \sigma(\eta\alpha) = \varepsilon\eta\alpha = \tau\sigma(\alpha)$, which shows that the group $G(L/K)$ is abelian. Moreover, we have $\sigma^m(\alpha) = \varepsilon^m\alpha = \alpha$, so $\sigma^m = 1$, which implies that the order of each element of $G(L/K)$ divides m.

Now we prove by induction with respect to the degree of L over K that every finite Kummer extension of K of exponent m is a splitting field of a finite number of binomials $X^m - a$, where $a \in K$. The claim is trivial for K (degree over K equal to 1). Assume that the claim is true for fields of degree less than n and let L be a field of degree $n > 1$ over K. Let H be a non-trivial cyclic subgroup of the Galois group $G(L/K)$ such that $G(L/K) = H \times H'$ for a subgroup H' of $G(L/K)$, which may be trivial if $G(L/K)$ is already cyclic. Such subgroups H and H' exist by the fundamental theorem on abelian groups (see **A.7.2**). Let $M = L^H$ and $M' = L^{H'}$. We have $G(M/K) = H'$ and $G(M'/K) = H$ (see Ex. 9.14). The order of the cyclic group H divides m, since L is a Kummer extension of exponent m. By

Hilbert's Theorem 90, we have $M' = K(\alpha)$, where $\alpha^{m'} \in M$ for some divisor m' of m. Hence $\alpha^m = a' \in K$ and M' is a splitting field of $X^m - a'$. The degree of M over K is less than the degree of L over K so using the inductive assumption, we get that M is a splitting field of a finite number of binomials $X^n - a$, where $a \in K$. The whole extension L is a splitting field of these binomials together with the binomial $X^m - a'$ whose zero is α.

(c) Let $\mathcal{F}_m$ denote all Kummer field extensions L of K of exponent m, and $\mathcal{A}_m$ all subgroups of K^* containing K^{*m}. We have two functions:

$$f : \mathcal{A}_m \to \mathcal{F}_m \quad \text{and} \quad g : \mathcal{F}_m \to \mathcal{A}_m$$

such that $f(A) =$ a splitting field of all binomials $X^m - a$ for $a \in A$ and $g(L) =$ the group of all $a \in K^*$ such that $a = \alpha^m$ for some $\alpha \in L^*$. We want to prove that $f \circ g$ and $g \circ f$ are identities on $\mathcal{F}_m$ and $\mathcal{A}_m$, so f and g are bijective functions between these two sets (see **A.8.1**).

If $L \in \mathcal{F}_m$, then L is a splitting field of some set of binomials $X^m - a$ with $a \in K$. The group $g(L)$ contains all these $a \in K$, so we certainly have $f(g(L)) = L$, since L is defined as a splitting field of some $X^n - a$ with $a \in g(L)$ and for each $a \in g(L)$, the field L contains a splitting field of $X^m - a$. Thus the composition $f \circ g$ is the identity on $\mathcal{F}_m$ (so that g is injective and f surjective - see **A.8.1**).

Let A be a subgroup of K^* containing K^{*m}. Then, of course, $A \subseteq g(f(A))$, since each element of A is an m-th power of an element of the field $f(A)$ corresponding to A. But A and $g(f(A))$ define the same field, that is, $f(g(f(A))) = f(A)$ by what we already has explained for $L = f(A)$, so

$$[A : K^{*m}] = [g(f(A)) : K^{*m}] = [L : K]$$

by (11.1). Since $A \subseteq g(f(A))$, the last equalities imply $g(f(A) = A$, that is, the composition $g \circ f$ is the identity on $\mathcal{F}_m$ (so that f is injective and g surjective - see **A.8.1**).

Let L be a Kummer extension of K defined by a subgroup A of K^* containing K^{*m}. We define a bilinear function

$$\varphi : G(L/K) \times A \to \mathbb{C}^*$$

in the following way. If $(\sigma, a) \in G(L/K) \times A$, then there is $\alpha \in L$ such that $a = \alpha^m$. Hence $\sigma(\alpha) = \varepsilon\alpha$, where ε is m-th root of 1. Notice that ε is independent on the choice of a solution of the equation $X^m = a$. In fact, if also $\beta^m = a$, then $\beta = \eta\alpha$, where $\eta \in K$ is an m-th root of 1. Thus, we have $\sigma(\beta) = \sigma(\eta\alpha) = \eta\varepsilon\alpha = \varepsilon\beta$. Now we define $\varphi(\sigma, a) = \varepsilon = \sigma(\alpha)/\alpha$. We check that φ is bilinear. If $\alpha^m = a$, $\sigma(\alpha) = \varepsilon\alpha$, $\beta^m = b$, $\tau(\beta) = \eta\beta$, then

$$\varphi(\sigma, ab) = \frac{\sigma(\alpha\beta)}{\alpha\beta} = \frac{\sigma(\alpha)}{\alpha}\frac{\sigma(\beta)}{\beta} = \varphi(\sigma, a)\varphi(\sigma, b)$$

and

$$\varphi(\sigma\tau, a) = \varepsilon\tau = \frac{\sigma(\alpha)}{\alpha}\frac{\tau(\beta)}{\beta} = \varphi(\sigma, a)\varphi(\tau, a).$$

The left kernel of φ are all $\sigma \in G(L/K)$ such that $\varphi(\sigma, a) = 1$ for each $a \in A$, that is, $\sigma(\alpha) = \alpha$ for each solution of $X^m - a = 0$ when $a \in A$. But such α generate L, so σ is the identity of $G(L/K)$. The right kernel of φ are all $a \in A$ such that $\varphi(\sigma, a) = 1$ for each $\sigma \in G(L/K)$. Hence $\sigma(\alpha) = \alpha$ for each $\sigma \in G(L/K)$, which means that $\alpha \in K$, that is, $a = \alpha^m \in K^{*m}$. Now by **A.15.1**, we get an isomorphism $A/K^{*m} \cong G(L/K)^*$. In particular, we have $[A : K^{*m}] = |G(L/K)^*| = |G(L/K)| = [L : K]$. □

Theorems of Chapter 12

T. 12.1 *(a) If G is solvable and H is a subgroup of G, then H is solvable.*

(b) If N is a normal subgroup of G and G is solvable, then the quotient group G/N is solvable.

(c) If N is a solvable normal subgroup of G such that the quotient group G/N is solvable, then G is solvable.

Proof. (a) If G is solvable, then there exists a chain

$$G = G_0 \supset G_1 \supset \ldots \supset G_n = \{e\}$$

such that G_{i+1} is normal in G_i and the quotient group G_i/G_{i+1} is abelian for $i = 0, 1, \ldots, n-1$. We claim that

$$H = G = G_0 \cap H \supset G_1 \cap H \supset \ldots \supset G_n \cap H = \{e\} \tag{12.2}$$

is the corresponding chain of subgroups of H. In fact, it is clear that the subgroup $G_{i+1} \cap H$ is normal in $G_i \cap H$ as G_{i+1} is normal in G_i. The quotient $(G_i \cap H)/(G_{i+1} \cap H)$ is abelian, since we have an embedding of pairs $(G_{i+1} \cap H, G_i \cap H) \to (G_{i+1}, G_i)$ for $i = 0, 1, \ldots, n-1$, which induces (see **A.2.7**) an injective homomorphism $(G_{i+1} \cap H)/(G_i \cap H) \to G_{i+1}/G_i$. Thus $(G_{i+1} \cap H)/(G_i \cap H)$ is abelian, since it is isomorphic to a subgroup of the abelian group G_{i+1}/G_i.

(b) Let (12.2) be a chain giving solvability of G and consider the following chain of subgroups of G/N:

$$G/N = G_0N/N \supset G_1N/N \supset \ldots \supset G_nN/N = \{e\}.$$

One checks immediately that $G_{i+1}N/N$ is normal in G_iN/N, since G_{i+1} is normal in G_i for $i = 0, 1, \ldots, n-1$. We have a mapping of pairs $(G_{i+1}, G_i) \to (G_{i+1}N/N, G_iN/N)$ such that $(g', g) \mapsto (g'N, gN)$ for $g \in G_{i+1}, g' \in G_i$ (see **A.2.7**). Since the coset gN, $g \in G_i$ is the image of $g \in G_i$, it is clear that the mapping of the pairs induces a surjective homomorphism $G_i/G_{i+1} \to (G_{i+1}N/N)/(G_iN/N)$. Hence, the quotient $(G_{i+1}N/N)/(G_iN/N)$ is abelian, since G_i/G_{i+1} is an abelian group.

(c) Let

$$N = N_0 \supset N_1 \supset \ldots \supset N_k = \{e\}$$

and

$$G/N = G_0/N \supset G_1/N \supset \ldots \supset G_l/N = \{e\}$$

be chains of subgroups of N and G/N, which existence follows from the assumption that these groups are solvable. We use the fact that each subgroup of G/N is the image H/N of a subgroup H of G containing N (see **A.2.8**), so

$$G = G_0 \supset G_1 \supset \ldots \supset G_l = N = N_0 \supset N_1 \supset \ldots \supset N_k = \{e\}$$

is a chain of subgroups of G such that each quotient G_i/G_{i+1} for $i = 0, 1, \ldots, l-1$ and N_j/N_{j+1} for $j = 0, 1, \ldots, k-1$ is abelian. This shows that the group G is solvable. □

T. 12.2 *The symmetric group S_n is not solvable when $n \geq 5$.*

Proof. We shall prove that the alternate group A_n consisting of the even permutations in S_n is not solvable when $n \geq 5$. By **T.12.1** (a), it follows that the group S_n is also not solvable. The group A_n contains each cycle (a, b, c), since such a permutation is even. In fact, we have $(a, b, c) = (a, b)(b, c)$, that is, a cycle of length 3 is a composition of two transpositions. Assume that

$$G_0 = A_n \supset G_1 \supset G_2 \supset \cdots \supset G_k = \{(1)\}$$

is a chain such that each G_{i+1} is normal in G_i and G_i/G_{i+1} is abelian.

First, we show that if a subgroup G of A_n contains every cycle of length 3 and H is a normal subgroup of G such that G/H is abelian, then H also contains each cycle of length 3. This proves that A_n is not solvable, since A_n contains each cycle of length 3, so its subgroup G_1 also contains every such cycle. Now the same is true about G_2 and so on. All groups G_i contain every cycle of length 3 and G_k can not consist of only the unit.

In order to prove the claim about G and H, we take an arbitrary cycle (a, b, c) of length 3. Let $x = (a, b, d) \in G$ and $y = (c, e, a) \in G$. We use the fact that the number of permuted elements is at least 5, so we can choose c, d different from a, b, c. We have

$$xyx^{-1}y^{-1} = (a,b,d)(c,e,a)(d,b,a)(a,e,c) = (a,b,c).$$

But $xyx^{-1}y^{-1} \in H$, since $HxHy = HyHx$ (G/H is abelian by our assumption) gives $Hxy = Hyx$, that is, $Hxyx^{-1}y^{-1} = H$, so $xyx^{-1}y^{-1} \in H$. Hence H contains arbitrary cycle (a,b,c). □

Theorems of Chapter 13

In the proof of **T.13.1**, we refer to a number of auxiliary results, which we prove below.

T. 13.1 *If char $(K) = 0$, then an equation $f(X) = 0$, $f \in K[X]$ is solvable by radicals if and only if the Galois group of f over K is solvable.*

Proof. First we prove that if K_f is a solvable extension of K, then its Galois group $G(K_f/K)$ is solvable. Let $K_f \subseteq L$, where L is a radical extension of K. According to Lemma 13.1.3, we can assume that L is a Galois extension of K. Thus we have a chain of fields $K \subseteq K_f \subseteq L$ in which L radical Galois extension of K. By Lemma 13.1.4, the group $G(L/K)$ is solvable, and since $K \subseteq K_f$ is a Galois extension, its Galois group $G(K_f/K)$ is a quotient of $G(L/K)$. Hence this group is also solvable.

Now we prove that if the Galois group $G(K_f/K)$ is solvable, then the extension $K \subseteq K_f$ is solvable. Denote by L any Galois extension of K whose Galois group is solvable (in the theorem, $L = K_f$). Using induction with respect to the degree $[L : K] > 1$, we prove that the extension $L \supset K$ is solvable.

If $[L : K]$ is a prime number, then the Galois group $G(L/K)$ is cyclic, so it is, of corse, solvable. Assume that $[L : K] \neq 1$ is not a prime number. Then the solvable group $G(L/K)$ contains a normal subgroup H such that $|G(L/K)| > |H| > 1$ (see Ex. 12.3). We have the corresponding tower of extensions $K \subset L^H \subset L$ and both extensions $L^H \subset L$ and $K \subset L^H$ are Galois with solvable Galois groups, since the first has a subgroup H of $G(L/K)$ as its Galois group, and the second, the quotient group $G(L/K)/H$. Both are solvable of orders less than $|G(L/K)| = [L : K]$. By the inductive assumptions, there exist radical extensions $L^H \subset L \subseteq L'$ and $K \subset L^H \subseteq L''$. Hence by Lemma 13.1.2(b), $K \subseteq L \subseteq L'L''$ is a radical extension of K (where $L'L''$ is taken in any field containing both L' and L''). □

Lemma 13.1.1 *Let L be a splitting field of a polynomial $X^n - a$ over a field K. Then the Galois group $G(L/K)$ is solvable.*

Proof. By Ex. 5.10, we have $L = K(\varepsilon, \alpha)$, where α is a zero of $X^n - a$ and ε generates the group of all zeros of $X^n - 1$. Consider the chain of fields:

$$K \subseteq K(\varepsilon) \subseteq K(\varepsilon, \alpha) = L$$

and the corresponding chain of groups:

$$G(L/K) \supseteq G(L/K(\varepsilon)) \supseteq \{id\}.$$

Of course, the extension $K(\varepsilon) \supseteq K$ is Galois as a splitting field of the polynomial $X^n - 1$ over K. Thus the Galois group $G(L/K(\varepsilon))$ is normal in $G(L/K)$ and $G(L/K)/G(L/K(\varepsilon)) \cong G(K(\varepsilon)/K)$. The last group is abelian. In fact, let σ be an automorphism of $K(\varepsilon)$ over K. Then $\sigma(\varepsilon) = \varepsilon^i$ for some i (notice that $\varepsilon^n = 1$ gives $\sigma(\varepsilon)^n = 1$). If now τ is another automorphism of $K(\varepsilon)$ over K and $\tau(\varepsilon) = \varepsilon^j$, then $\sigma(\tau(\varepsilon)) = \varepsilon^{ij} = \tau(\sigma(\varepsilon))$, that is, $\sigma\tau = \tau\sigma$.

Now notice that the group $G(L/K(\varepsilon))$ is abelian. Let $\sigma, \tau \in G(L/K(\varepsilon))$. Then $\sigma(\alpha) = \varepsilon^i\alpha$ and $\tau(\alpha) = \varepsilon^j\alpha$, for some i, j. Thus $\sigma(\tau(\alpha))) = \varepsilon^{i+j}\alpha = \tau(\sigma(\alpha))$, that is, $\sigma\tau = \tau\sigma$. Hence the group $G(L/K)$ is solvable. □

We say that L is a **radical m-extension** of K if

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n = L$$

are such that $K_i = K_{i-1}(\alpha_i)$, $\alpha_i^{r_i} \in K_{i-1}$ and $r_i \leq m$ are natural numbers for $i = 1, \ldots, n$.

Lemma 13.1.2 *Let $K \subseteq L$ and $K \subseteq L'$ be field extensions.*

(a) If $\sigma : L \to L'$ is a $K-$isomorphism and $K \subseteq L$ is radical, then also $K \subseteq L'$ is radical.

(b) If L is a radical m-extension of K, and L' is a radical m-extensions of K', where $K \subseteq K' \subseteq L$, both L, L' contained in a field M, then the compositum LL' is a radical m-extension of K.

Proof. (a) Let $L = K(\alpha_1, \ldots, \alpha_n)$, where

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n = L$$

are such that $K_i = K_{i-1}(\alpha_i)$, $\alpha_i^{r_i} \in K_{i-1}$ and r_i are natural numbers for $i = 1, \ldots, n$. Then $L' = \sigma(L) = K(\sigma(\alpha_1), \ldots, \sigma(\alpha_n))$ and

$$K = K_0 \subseteq \sigma(K_1) \subseteq \ldots \subseteq \sigma(K_n) = L',$$

where $\sigma(K_i) = \sigma(K_{i-1})(\sigma(\alpha_i))$, $\sigma(\alpha_i)^{r_i} \in \sigma(K_{i-1})$, so L' is a radical extension of K.

(b) Let L be as above and $L' = K'(\alpha'_1, \ldots, \alpha'_n)$, where

$$K' = K'_0 \subseteq K'_1 \subseteq \ldots \subseteq K'_n = L',$$

$K'_i = K'_{i-1}(\alpha'_i)$, $(\alpha'_i)^{s_i} \in K'_{i-1}$ and s_i are natural numbers for $i = 1, \ldots, m$. Then

$$K = K \subseteq K(\alpha_1) \subseteq \cdots \subseteq K(\alpha_1, \ldots, \alpha_n) =$$

$$L \subseteq K(\alpha_1, \ldots, \alpha_n, \alpha'_1) \subseteq \cdots \subseteq K(\alpha_1, \ldots, \alpha_n, \alpha'_1, \ldots, \alpha'_m) = LL'$$

is a corresponding chain of extensions showing that LL' is a radical extension of K. □

Lemma 13.1.3 *Let L be a radical extension of a field K. Then the normal closure N of $L \supseteq K$ is also a radical extension of K. Moreover, if L is a radical m-extension of K, then N is also a radical m-extension.*

Proof. Let $L = K(\alpha_1, \ldots, \alpha_n)$, where

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n = L$$

are such that $K_i = K_{i-1}(\alpha_i)$, $\alpha_i^{r_i} \in K_{i-1}$ and $r_i \leq m$ are natural numbers for $i = 1, \ldots, n$. Thus $K_i = K(\alpha_1, \ldots, \alpha_i)$ for $i = 1, \ldots, n$. Let f_i be the minimal polynomial of α_i over K. Of course, N is a splitting field of $f = f_1 \cdots f_n$ over K. Let β_i be any zero of f_i in N and let $\tau : K(\alpha_i) \to K(\beta_i)$ be the isomorphism over K such that $\tau(\alpha_i) = \beta_i$. Since N is a splitting field of f over $K(\alpha_i)$ and $K(\beta_i)$, there is an automorphism $\sigma : N \to N$, which extends τ. This automorphism maps L onto $\sigma(L)$ which according to Lemma **13.1.2**(a) is also a radical m-extension of K. It is clear that N as a splitting field of f is the compositum of all the fields $\sigma(L)$ obtained for all the choices of τ. Thus N is a radical m-extension of K according to Lemma **13.1.2**(b). □

Lemma 13.1.4 *Let L be a radical Galois extension of K. Then the Galois group $G(L/K)$ is solvable.*

Proof. Let $L = K(\alpha_1, \ldots, \alpha_n)$, where

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n = L$$

are such that $K_i = K_{i-1}(\alpha_i)$, $\alpha_i^{r_i} \in K_{i-1}$ and r_i are natural numbers for $i = 1, \ldots, n$. Thus $K_i = K(\alpha_1, \ldots, \alpha_i)$ for $i = 1, \ldots, n$. We prove the claim by induction on the number n of root extensions between two arbitrary fields K and L.

If $n = 1$, then $L = K(\alpha_1)$, where $\alpha_1^{r_1} = a \in K$. Denote $r_1 = r$ and consider the splitting field $K(\alpha_1, \varepsilon)$ of $X^r - a$ over K, where $\varepsilon^r = 1$. By Lemma **13.1.1**, the Galois group $G(K(\alpha_1, \varepsilon)/K)$ is solvable. Since $K(\alpha_1)$ is Galois over K, its Galois group $G(K(\alpha_1)/K)$ is solvable as a quotient of the solvable Galois group $G(K(\alpha_1, \varepsilon)/K)$. (Observe that $K(\alpha_1)$ needs not be a splitting field of $X^r - a$ even if it is Galois and contains a zero of this polynomial – the polynomial may be reducible. Take as an example $X^4 - 4$ over the rational numbers and $L = \mathbb{Q}(\sqrt{2})$).

Assume now that the claim is true when the number of elementary radical extensions between two fields is less than $n > 1$. Consider the following chain of field extensions:

$$\begin{array}{ccccc} K = K_0 & \subseteq & K_1 & \subseteq \ldots & \subseteq K_n = L \\ & & \downarrow & & \downarrow \\ & & K_1(\varepsilon) & \subseteq \ldots & \subseteq K_n(\varepsilon) = L(\varepsilon) \end{array}$$

Then it is clear that $L(\varepsilon)$ is a radical Galois extension of K and as well as of $K_1(\varepsilon)$. The number of elementary radical extensions between $K_1(\varepsilon)$ and $L(\varepsilon)$ is $n-1$. Thus by the inductive

assumption, the Galois group $G(L(\varepsilon)/K_1(\varepsilon))$ is solvable. According to Lemma **13.1.1**, the Galois group $G(K_1(\varepsilon)/K)$ is solvable. Hence the Galois group $G(L(\varepsilon)/K)$ is solvable since its normal subgroup $G(L(\varepsilon)/K_1(\varepsilon))$ and the quotient group $G(L(\varepsilon)/K)/G(L(\varepsilon)/K_1(\varepsilon)) \cong G(K_1(\varepsilon)/K)$ are solvable. Now, we obtain that the Galois group $G(L/K)$ is isomorphic to $G(L(\varepsilon)/K)/G(L(\varepsilon)/L)$ and as a quotient of a solvable group, is solvable. □

Lemma 13.1.5 *Let L be a Galois extension of K with a cyclic Galois group $G(L/K)$. Then L is a solvable extension of K.*

Proof. Let $[L : K] = n$ and let $K' = K(\varepsilon)$ be a splitting field of $X^n - 1$ over K. Then $L' = L(\varepsilon)$ is a Galois extension of $K' = K(\varepsilon)$ whose Galois group is cyclic as isomorphic to a subgroup of the Galois group $G(L/K)$ (of order n) according to Ex. 9.20. Moreover, the field K' contains all roots of 1 of degree $[L' : K']$, since this degree divides n and all roots of 1 of degree n are in K'. Thus according to **T.11.3**, $K' \subseteq L'$ is a radical extension. $K \subseteq K'$ is also a radical extension. Hence $K \subseteq L'$ is a radical extension, so $K \subseteq L$ is a solvable extension. □

T. 13.2 *The Galois group over $K(s_1, s_2, \ldots, s_n)$ of the general equation $f(X) = 0$ of degree n is S_n, so $f(X) = 0$ is not solvable by radicals when $n \geq 5$.*

Proof. It is clear that each elementary symmetric function s_i of $X_1, \ldots, X_n$ is fixed by all elements of $\sigma \in S_n$, that is, by all permutations $\sigma(X_i) = X_{\sigma(i)}$. Hence we have the tower of fields:

$$K(s_1, s_2, \ldots, s_n) \subseteq K(X_1, X_2, \ldots, X_n)^{S_n} \subset K(X_1, X_2, \ldots, X_n).$$

We have $[K(X_1, X_2, \ldots, X_n) : K(X_1, X_2, \ldots, X_n)^{S_n}] = |S_n| = n!$ and $[K(X_1, X_2, \ldots, X_n) : K(s_1, s_2, \ldots, s_n)] \leq n!$, since the splitting field $K(X_1, X_2, \ldots, X_n)$ of the polynomial of degree n

$$f(X) = X^n - s_1 X^{n-1} + s_2 X^{n-2} + \ldots + (-1)^n s_n = 0,$$

over the field $K(s_1, s_2, \ldots, s_n)$ has at most degree $n!$, so $K(X_1, X_2, \ldots, X_n)^{S_n} = K(X_1, X_2, \ldots, X_n)$. Thus, the Galois group of $K(X_1, X_2, \ldots, X_n)$ over $K(s_1, s_2, \ldots, s_n)$ is S_n by Theorem **T.9.1**. □

T. 13.3 Casus irreducibilis. *Let $f(X) \in \mathbb{Q}[X]$ be an irreducible polynomial of degree 3 whose all zeros x_1, x_2, x_3 are real. Then the equation $f(X) = 0$ is not solvable by real radicals, that is, the splitting field $\mathbb{Q}_f = \mathbb{Q}(x_1, x_2, x_3)$ of f is not a subfield of a radical extension $\mathbb{Q} \subseteq L$ such that $L \subset \mathbb{R}$.*

Proof. Assume to the contrary that there exists a radical extension:

$$K_0 = \mathbb{Q} \subset K_1 \subset \ldots \subset K_n = L \subset \mathbb{R}$$

such that $K_i = K_{i-1}(\alpha_i)$, $\alpha_i^{r_i} \in K_i$, r_i are prime numbers for $i = 1, \ldots, n$ and $\mathbb{Q}_f = \mathbb{Q}(x_1, x_2, x_3) \subset L$. Choose $i \geq 1$ such that K_{i-1} does not contain x_1, x_2, x_3 while some of

these numbers, say x_1, belongs to K_i. Since $K_{i-1} \subset K_{i-1}(x_1) \subseteq K_i$ and $[K_{i-1}(x_1) : K_{i-1}] = 3$ divides $[K_i : K_{i-1}] = r_i$, we have $r_i \geq 3$. The polynomial $X^{r_i} - a_i$, where $a_i = \alpha_i^{r_i}$, is irreducible over K_{i-1} (since it has only one real zero α_i, which does not belong to the real field K_{i-1}), but it must be reducible in $K_{i-1}(x_1)$, since the degree of the field $K_i = K_{i-1}(\alpha_i)$ over $K_{i-1}(x_1)$ is less than r_i. Thus $X^{r_i} - a_i$ has a zero in $K_{i-1}(x_1)$ and, as a consequence, it splits in the splitting field $K_{i-1}(x_1, x_2, x_3)$ of f over K_{i-1}. But it gives a contradiction, since the field $K_{i-1}(x_1, x_2, x_3)$ is real, but all the zeros of $X^{r_i} - a_i$ with the exception of α_i are non-real. □

Theorems of Chapter 14

T. 14.1 *Let K be the least subfield to $\mathbb{R}$ which contains the coordinates of all points belonging to a given set of points X in the plane. A point $P = (a, b)$ can be constructed from X by a straightedge-and-compass construction if and only if there is a chain of fields:*

$$K = K_0 \subset K_1 \subset \ldots \subset K_n = L \subset \mathbb{R} \qquad (*)$$

such that $a, b \in L$ and $[K_{i+1} : K_i] = 2$ for $i = 0, 1, \ldots, n-1$. In particular, the set of numbers which are constructible from X (like $\mathbb{K}$ when $X = \{(0,0),(1,0)\}$) is a field.

We start with an auxiliary result:

Lemma 14.1.1 *Let K be the least number field containing the coordinates of all points belonging to a point set X.*

(a) Every number in K can be constructed from X by a straightedge-and-compass construction.

(b) The coordinates of any point which can be directly constructed from X are in a real field L such that $[L : K] \leq 2$.

(c) If a point has its coordinates in a real field L such that $[L : K] \leq 2$, then it can be constructed from X by a straightedge-and-compass construction.

Proof (a) A line which goes through two points with coordinates in the field K has an equation $ax + by + c = 0$ with coefficients a, b, c in K. The coordinates of the intersection point of two such lines (if they intersect) is defined by the solution of a linear equation system consisting of two such equations. Thus the intersection point of the lines has its coordinates in the same field K.

A circle whose center (p, q) has coordinates in K and whose radius equals to the distance d between two points with coordinates in K has the equation $(x-p)^2 + (y-q)^2 = d^2$. It is clear that $d^2 \in K$. The intersections points of such a circle with a line as above are given by the solutions of the system:

$$ax + by + c = 0,$$
$$(x-p)^2 + (y-q)^2 = d^2.$$

In order to solve such a system, we express y by x from the first equation (or conversely) and put in the second equation. We get a quadratic equation with respect to x (or y) of the form $x^2+Ax+B=0$, where the coefficients $A, B \in K$ while the solutions $x = -A/2 \pm \sqrt{A^2/4 - B}$ belong to the field $L = K(\sqrt{A^2/4 - B})$ whose degree over K is at most 2.

If we have two circles as above and we want to find their intersection points, then we have to solve a system:

$$(x-p)^2 + (y-q)^2 = d^2,$$
$$(x-p')^2 + (y-q')^2 = d'^2$$

for some $p, q, p', q', d^2, d'^2 \in K$. We can do it, subtracting the two equations. Then we get an equivalent system consisting of an equation of a line and an equation of a circle just as in the previous case.

(b) First we show that the field K is the least set of numbers containing all the coordinates of the points in X, which is closed with respect to addition, subtracting, multiplying and division. Therefore the elements of K are the numbers obtained successively from the coordinates of the points in X by these four arithmetical operations. Thus we have to show that if $a, b \in K$ are constructible, then also $a \pm b$, ab and a/b (provided $b \neq 0$) are constructible. We may assume that $a, b > 0$. It is clear how to construct $a \pm b$ when a, b are given. In order to construct ab and b/a ($a \neq 0$), we can draw angles according to the figures below:

Now we have to show that any element of a quadratic real field L over K can be obtained by a straightedge-and-compass construction. As we know $L = K(\sqrt{d})$, where $d \in K, d > 0$, so each element of L is of the form $a + b\sqrt{d}$, where $a, b \in K$. Thus we only need to construct $\sqrt{d}$ when d is given, since we already know how to construct the product $b\sqrt{d}$ having b and $\sqrt{d}$, and the sum $a + b\sqrt{d}$ having its terms $a, b\sqrt{d}$. The construction of $\sqrt{d}$ follows from Fig. 14.2: first we draw a line with intervalls 1 and d, then we find the middle point of $1 + d$ and draw a half circle with radius $(1 + d)/2$. The line perpendicular to the line AC through the point C gives the intervall CD whose length is $\sqrt{d}$. In fact, by a known result on the altitude of a right triangle, we have $CD^2 = AC \cdot BC = 1 \cdot d$, that is, $CD = \sqrt{d}$.

□

Proof of T.14.1. If a point $P = (a, b)$ can be constructed from X by a straightedge-and-compass construction, then this can be done by constructing a sequence of points $P_0, P_1, P_2, \ldots, P_n = P$ such that each point can be directly constructed from X and the points preceding it. As we know from Lemma **14.1.1**(b), the coordinates of every new point are in a real extension of degree at most 2 over the preceding field (starting with K) which contains the coordinates of the points of X and all the points constructed earlier. This shows

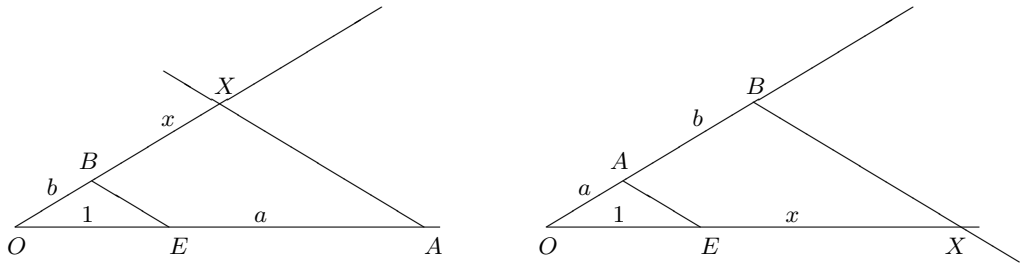


Fig. 14.1.

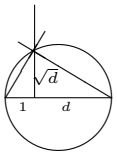


Fig. 14.2.

that the coordinates a, b of P belong to a field L, which can be obtained from K by a sequence of extensions each of which has degree at most 2. Thus we get a sequence $(*)$ if we only take those fields whose degrees are 2.

Conversely, if a point $P = (a, b)$ has its coordinates in an extension L of K, which can be obtained by a chain of quadratic extensions like in $(*)$, then an evident inductive argument using Lemma **14.1.1**(c) gives that the elements of each field K_i $(i = 1, \ldots, n)$ can be constructed from X. In particular, the point $P = (a, b)$ can be constructed from X.

Finally notice that the distance between two points $P = (a, b)$ and $P' = (a', b')$, where $a, b, a', b' \in L$ is $d = \sqrt{(a - a')^2 + (b - b')^2}$, so such a number d belongs to a quadratic extension of L. □

T. 14.2 *Let K be the least subfield of $\mathbb{R}$ which contains the coordinates of all points belonging to a point set X in the plane $\mathbb{R}^2$. A point $P = (a, b)$ can be constructed from X by a straightedge-and-compass construction if and only if one of the following equivalent conditions hold:*

(*a*) *There exists a Galois extension* $L \supseteq K$ *such that* $a, b \in L$ *and* $[L : K]$ *is a power of* 2.

(*b*) *There exists a Galois extension* $L \supseteq K$ *such that* $a + bi \in L$ *and* $[L : K]$ *is a power of* 2.

In order to prove this thoerem, we need some notations and an auxiliary result. Let K be a subfield of the real numbers and let $r_2(K)$ denote all complex numbers x for which there exists a chain of radical 2-extensions:

$$K = K_0 \subset K_1 \subset \cdots \subset K_n \subset \mathbb{C} \qquad (**)$$

such that $x \in K_n$ and $[K_i : K_{i-1}] = 2$ for $i = 1, \ldots, n$. Let $rr_2(K)$ denote all numbers for which there is such a chain of fields with $K_i \subset \mathbb{R}$. It follows easily from Lemma **13.1.2**(b) that $r_2(K)$ and $rr_2(K)$ are fields. Moreover, if $x \in r_2(K)$, then $\sqrt{x} \in r_2(K)$, while $x \in rr_2(K)$ and $x \geq 0$, imply $\sqrt{x} \in rr_2(K)$.

Lemma 14.2.1 *Let* a, b *be real numbers. Then the following conditions are equivalent:*

(*a*) $a, b \in rr_2(K)$,

(*b*) $a, b \in r_2(K)$,

(*c*) $a + bi \in r_2(K)$.

Proof. It is evident that (a) implies (b). If $a, b \in K_n$ in a tower $(**)$, then $a + bi \in K_{n+1} = K_n(i)$ and $[K_{n+1} : K_n] \leq 2$, which implies (c). We prove that (c) implies (a) by induction on the number n of fields in a tower $(**)$. Assume that $a + bi \in K_n$. If $n = 1$, then the claim is evident, since K is real and K_1 is a quadratic extension of K. Thus $a, b \in K \subset rr_2(K)$ as the real and imaginary parts of $a + bi$ (K_1 may be real when $b = 0$). Assume that the claim holds when the number of fields in the tower is less than n. Assume that $a + bi \in K_n$. Let $K_n = K_{n-1}(\sqrt{A + Bi})$, where $A + Bi \in K_{n-1}$, $A, B \in \mathbb{R}$ (it may happen that $B = 0$). We have:

$$a + bi = (x + yi) + (z + ti)\sqrt{A + Bi},$$

where $x + yi, z + ti \in K_{n-1}$, $x, y, z, t \in \mathbb{R}$. By the inductive assumption, $x, y, z, t, A, B \in rr_2(K)$. Moreover,

$$\sqrt{A + Bi} = \sqrt{\frac{\sqrt{A^2 + B^2} + A}{2}} + i\sqrt{\frac{\sqrt{A^2 + B^2} - A}{2}},$$

so denoting

$$\alpha = \sqrt{\frac{\sqrt{A^2 + B^2} + A}{2}}, \quad \beta = \sqrt{\frac{\sqrt{A^2 + B^2} - A}{2}},$$

we have $\alpha, \beta \in rr_2(K)$, $a = x + z\alpha - t\beta \in rr_2(K)$ and $b = y + t\alpha + z\beta \in rr_2(K)$. □

Proof of T.14.2. First note that (a) and (b) are equivalent. In fact, $L(i)$ is an extension of L such that $[L(i) : L] = 1$ or 2 and $L(i)$ is of course Galois over K (if L is a splitting field of a polynomial with coefficients in K, then $L(i)$ is a splitting field of the same polynomial multiplied by $X^2 + 1$). If L satisfies (a), then we take $L(i)$ as L in (b) – it contains $a + bi$ and its degree over K is a power of 2. If L satisfies (b), then $a - bi \in L$, since the minimal polynomial of $a + bi$ over the real field K has $a - bi$ as its zero, which must belong to the normal extension L of K. Hence $a, b \in L$.

Assume now that a point (a, b) is constructible from a point set X by a straightedge-and-compass construction, that is, $a, b \in rr_2(K)$ and let

$$K = K_0 \subset K_1 \subset \cdots \subset K_n \subset \mathbb{R}$$

be a tower of fields such that $[K_i : K_{i-1}] = 2$ for $i = 1, \ldots, n$ and $a, b \in K_n$. Let L be a normal closure of K_n. Then according to Lemma **13.1.2**, L is a Galois radical 2-extension of K. Of course, $a, b \in L$ and by **T.4.3**, the degree $[L : K]$ is a power of 2.

Conversely, assume that (a) holds. Then the order of the Galois group $G = G(L/K)$ is a power of 2, that is, $G(L/K)$ is a 2-group. This means that it has a filtration

$$G_0 = G(L/K) \supset G_1 \supset \cdots \supset G_{n-1} \supset G_n = \{id\}$$

such that G_i is a normal subgroup of G_{i-1} and the quotient group G_{i-1}/G_i has 2 elements. The corresponding tower of the fields $L^{G_i} = K_i$ is

$$K_0 = K \subset K_1 \subset \cdots \subset K_n = L$$

and $[K_i : K_{i-1}] = 2$, that is, $a, b \in r_2(K)$. According to Lemma **14.2.1**, $a, b \in rr_2(K)$, that is, the point (a, b) is constructible from X by a straightedge-and-compass construction. □

Theorems of Chapter 15

T. 15.1 (*a*) *Let G be a subgroup of S_n. Then for every subgroup H of G there exists a polynomial $F \in K[X_1, \ldots, X_n]$ such that $H = G_F$.*

(*b*) *Let $G = \sigma_1 G_F \cup \cdots \cup \sigma_m G_F$ be the presentation of G as a union of different left cosets with respect to G_F. Then $\sigma_i F(X_1, \ldots, X_n)$ for $i = 1, \ldots, m$ are all different images of F under the permutations belonging to G.*

Proof. (a) Consider the monomial $M = X_1 X_2^2 \cdots X_n^n$ and notice that for any two permutations $\sigma, \tau \in S_n$, we have $\sigma(M) = \tau(M)$ if and only if $\sigma = \tau$. In fact, since the exponents of all X_i in M are different, two different permutations map the monomial M onto

two different monomials (that is, $X_{\sigma(1)}X_{\sigma(2)}^2\cdots X_{\sigma(n)}^n = X_{\tau(1)}X_{\tau(2)}^2\cdots X_{\tau(n)}^n$ if and only if $\sigma(i) = \tau(i)$ for every $i = 1, 2, \ldots, n$). Define now $F = \mathrm{Tr}_H(M) = \sum_{\tau\in H}\tau(M)$. The polynomial $F(X_1, \ldots, X_n)$ is invariant with respect to every $\sigma \in H$ and $\sigma(F) = F$ for $\sigma \in G$ if and only if $\sigma \in H$. In fact, for any permutation $\sigma \in H$, the compositions $\sigma\tau$, where $\tau \in H$ give exactly all the elements of H, so $\sigma(F) = F$. On the other hand, if $\sigma \in G \setminus H$, then $\sigma(M)$ is different from all $|H|$ monomials whose sum gives F, that is, we have $\sigma(F) \neq F$. Thus $\sigma(F) = F$ for $\sigma \in G$, if and only if $\sigma \in H = G_F$. Notice that the definition of F only depends on H and not on the group G containing it.

(b) We have

$$\sigma(F) = \sigma'(F) \Leftrightarrow \sigma^{-1}\sigma'(F) = F \Leftrightarrow \sigma^{-1}\sigma' \in H = G_F \Leftrightarrow \sigma G_F = \sigma' G_F.$$

Thus different images $\sigma(F)$, when $\sigma \in G$, correspond to different left cosets of G_F in G. □

T. 15.2 *Let $f(X) \in K[X]$, $F(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$ and assume that* $\mathrm{Gal}(K_f/K) \subseteq G$*, where G is a subgroup of S_n. Then:*

(a) The resolvent polynomial $r_{G,F}(f)$ has its coefficients in K;

(b) If $K = \mathbb{Q}$, $F(X_1, \ldots, X_n) \in \mathbb{Z}[X_1, \ldots, X_n]$ and $f(X)$ has integer coefficients and the highest coefficient 1*, then the same is true on $r_{G,F}(f)$;*

(c) If all the zeros of $r_{G,F}(f)$ are different, then $\mathrm{Gal}(K_f/K)$ *is conjugated in G to a subgroup of G_F if and only if at least one of the zeros of $r_{G,F}(f)$ belongs to K.*

Proof. (a) Let $\sigma \in G$. Then

$$\sigma(r_{G,F}(f)(T)) = \prod_{i=1}^{m}(T - (\sigma\sigma_i F)(\alpha_1, \ldots, \alpha_n)) = (T - (\sigma_i F)(\alpha_1, \ldots, \alpha_n)) = r_G(F, f)(T),$$

since $\sigma\sigma_i$ for $i = 1, \ldots, m$ is also a set of representatives of left cosets of G_F in G. In fact, since $\sigma\sigma_i \in G$, so $\sigma\sigma_i = \sigma_j\tau$ for some $1 \leq j \leq m$ and $\tau \in G_F$. Thus $\sigma\sigma_i F = \sigma_j\tau F = \sigma_j F$, so $\sigma\sigma_i F(\alpha_1, \ldots, \alpha_n) = \sigma_j F(\alpha_1, \ldots, \alpha_n)$ is also a zero of $r_G(F, f)$. At the same time, it is clear that if $i \neq j$, then $\sigma\sigma_i$ and $\sigma\sigma_j$ represent different cosets of G_F in G. Hence $\sigma\sigma_i F(\alpha_1, \ldots, \alpha_n)$ for $1 \leq i \leq m$ is simply a permutation of the elements $\sigma_i F(\alpha_1, \ldots, \alpha_n)$, which means that $\sigma r_{G,F}(f)$ and $r_{G,F}(f)$ have the same coefficients for every $\sigma \in G$. In particular, this is true for every $\sigma \in \mathrm{Gal}(K_f/K)$, since $\mathrm{Gal}(K_f/K) \subseteq G$. Thus the coefficients of $r_{G,F}(f)$ are fixed by every element in the Galois group $\mathrm{Gal}(K_f/K)$, so they are in K.

(b)

(c) If $\sigma \in G$ and $\sigma = \sigma_i\tau$, where $\tau \in G_F$, then $\sigma F = \sigma_i F$ and $\sigma F(\alpha_1, \ldots, \alpha_n) = \sigma_i F(\alpha_1, \ldots, \alpha_n)$ is a zero of $r_G(F, f)$. If all the zeros of $r_G(F, f)$ are different, then $\sigma F(\alpha_1, \ldots, \alpha_n) = F(\alpha_1, \ldots, \alpha_n)$ is equivalent to $\sigma \in G_F$. In fact, $\sigma_i F(\alpha_1, \ldots, \alpha_n) = \sigma_1 F(\alpha_1, \ldots, \alpha_n)$ implies $\sigma_i = \sigma_1 = id$, so $\sigma = \tau \in G_F$.

If $\tau^{-1}\mathrm{Gal}(K_f/K)\tau \subseteq G_F$ for a $\tau \in G$, then $\tau^{-1}\sigma\tau F(\alpha_1,\ldots,\alpha_n) = F(\alpha_1,\ldots,\alpha_n)$ for each $\sigma \in \mathrm{Gal}(K_f/K)$. Hence $\sigma\tau F(\alpha_1,\ldots,\alpha_n) = \tau F(\alpha_1,\ldots,\alpha_n)$, that is, $\tau F(\alpha_1,\ldots,\alpha_n)$, which is a zero of $r_G(F,f)$, belongs to K.

Conversely, assume that $\sigma_i F(\alpha_1,\ldots,\alpha_n) \in K$ for some i. If $\sigma \in \mathrm{Gal}(K_f/K)$, we have $\sigma\sigma_i F(\alpha_1,\ldots,\alpha_n) = \sigma_i F(\alpha_1,\ldots,\alpha_n)$, that is, $\sigma_i^{-1}\sigma\sigma_i F(\alpha_1,\ldots,\alpha_n) = F(\alpha_1,\ldots,\alpha_n)$, so $\sigma_i^{-1}\sigma\sigma_i \in G_F$. Hence $\sigma_i^{-1}\mathrm{Gal}(K_f/K)\sigma_i \subseteq G_F$. □

T. 15.3 *The Galois group* $\mathrm{Gal}(k_f/k)$ *is isomorphic to any group* G_{r_i} *of those permutations of* $Y_1,\ldots,Y_n$ *which map* $r_i(X,Y_1,\ldots,Y_n)$ *onto itself for* $i = 1,\ldots,t$. *Moreover, all* $r_i(T,Y_1,\ldots,Y_n)$ *have the same degree* $[k_f : k]$ *with respect to* T *and they have a common splitting field* $K_f = k_f(Y_1,\ldots,Y_n)$ *over* $K = k(Y_1,\ldots,Y_n)$.

Proof. Define $\theta_\varrho = \alpha_1 Y_{\varrho(1)} + \cdots + \alpha_n Y_{\varrho(n)} \in k_f(Y_1,\ldots,Y_n) = K_f$ for $\varrho \in S_n$. The group S_n acts on the set of all θ_ϱ if $\sigma(\theta_\varrho) = \theta_{\sigma\varrho}$. Denoting $\theta = \theta_{id} = \alpha_1 Y_1 + \cdots + \alpha_n Y_n$, we have $\varrho(\theta) = \theta_\varrho$ so the action of S_n on the set of all θ_ϱ is transitive. Of course,

$$\alpha_1 Y_{\varrho(1)} + \cdots + \alpha_n Y_{\varrho(n)} = \alpha_{\varrho^{-1}(1)} Y_1 + \cdots + \alpha_{\varrho^{-1}(n)} Y_n.$$

Let $\theta_i = \sigma_i(\theta) = \theta_{\sigma_i}$ denote a zero of the polynomial $r_i(X,Y_1,\ldots,Y_n)$ and assume that $\sigma_1 = id$, that is, $\theta_1 = \theta$.

Notice now that each $\theta_i = \alpha_1 Y_{\sigma_i(1)} + \cdots + \alpha_n Y_{\sigma_i(n)} \in k_f(Y_1,\ldots,Y_n)$ is a primitive element of the extension $K = k(Y_1,\ldots,Y_n) \subseteq K_f = k_f(Y_1,\ldots,Y_n)$. In fact, according to the Ex. 15.10(a), the Galois group of this extension is isomorphic to $\mathrm{Gal}(k_f/k)$ when $\tau \in \mathrm{Gal}(k_f/k)$ corresponds to an automorphism of $K_f = k_f(Y_1,\ldots,Y_n)$ which acts on the coefficients of the rational functions in K_f as τ and as identity on Y_i. Thus for the element $\theta_i \in K_f$, we have

$$\tau(\theta_i) = \tau(\alpha_1) Y_{\sigma_i(1)} + \cdots + \tau(\alpha_n) Y_{\sigma_i(n)},$$

which shows that the number of different images of θ_i is equal to the order of the Galois group $\mathrm{Gal}(K_f/K)$ (diffrent automorphisms give different sets of coefficients of Y_i). Hence, according to Ex. 9.22, θ_i is a primitive element of the extension $K \subseteq K_f$ and every automorphism of K_f over K is uniquely defined by its action on θ_i. Since $r_i(X,Y_1,\ldots,Y_n)$ is the minimal polynomial of θ_i over K, the remaining zeros of this polynomial are the images $\tau(\theta_i)$ under the automorphisms τ of the Galois group $\mathrm{Gal}(K_f/K)$. Thus all polynomials $r_i(X,Y_1,\ldots,Y_n)$ have the same degree $|\mathrm{Gal}(K_f/K)| = [K_f : K] = [k_f : k]$ and they have a common splitting field K_f over K.

The Galois group $\mathrm{Gal}(k_f/k)$ acts on the set of θ_ϱ in two different ways. First of all each $\tau \in \mathrm{Gal}(k_f/k)$ acts as the permutation $\pi(\tau) \in S_n$ of $\{1,\ldots,n\}$ defined by the relation:

$$\pi(\tau)(i) = j \Leftrightarrow \tau(\alpha_i) = \alpha_j,$$

that is, $\tau(\alpha_i) = \alpha_{\pi(\tau)(i)}$. This gives the usual representation of the Galois group $\mathrm{Gal}(k_f/k)$ as a permutation group. Notice that π is an injective homomorphism of $\mathrm{Gal}(k_f/k)$ into S_n. In particular, $\pi(\tau^{-1}) = \pi(\tau)^{-1}$.

The second action is defined according to Ex. 15.10(a) – the Galois group of the extension $K = k(Y_1, \ldots, Y_n) \subseteq K_f = k_f(Y_1, \ldots, Y_n)$ is isomorphic to $\mathrm{Gal}(k_f/k)$ when $\tau \in \mathrm{Gal}(k_f/k)$ corresponds to an automorphism of $K_f = k_f(Y_1, \ldots, Y_n)$ which acts on the coefficients of the rational functions in K_f as τ and as identity on Y_i. Thus for the element $\theta_\varrho \in K_f$, we have

$$\tau(\theta_\varrho) = \tau(\alpha_1)Y_{\varrho(1)} + \cdots + \tau(\alpha_n)Y_{\varrho(n)}.$$

Let G_{r_i} denote the group of permutations $\varrho \in S_n$ such that

$$\varrho r_i(X, Y_1, \ldots, Y_n) = r_i(X, Y_{\varrho(1)}, \ldots, Y_{\varrho(n)}) = r_i(X, Y_1, \ldots, Y_n)$$

for $i = 1, \ldots, t$. We will show that π is a group isomorphism of $\mathrm{Gal}(k_f/k)$ onto G_{r_i}.

We have:

$$r_i(X, Y_1, \ldots, Y_n) = \prod_{\tau \in G(K_f/K)} (X - \tau(\theta_i)) = \prod_{\tau \in G(K_f/K)} (X - \tau(\alpha_1 Y_{\sigma_i(1)} + \cdots + \alpha_n Y_{\sigma_i(n)})).$$

If $\pi(\tau)$ is the permutation corresponding to $\tau \in \mathrm{Gal}(K_f/K)$, then

$$\pi(\tau) r_i(X, Y_1, \ldots, Y_n) = r_i(X, Y_{\pi(\tau)(1)}, \ldots, Y_{\pi(\tau)(n)}) =$$

$$\prod_{\tau' \in G(K_f/K)} (X - \tau'(\alpha_1 Y_{\pi(\tau)(\sigma_i(1))} + \cdots + \alpha_n Y_{\pi(\tau)(\sigma_i(n))})) =$$

$$\prod_{\tau' \in G(K_f/K)} (X - \tau'(\alpha_{\pi(\tau)^{-1}(1)} Y_{\sigma_i(1)} + \cdots + \alpha_{\pi(\tau)^{-1}(n)} Y_{\sigma_i(n)})) =$$

$$\prod_{\tau' \in G(K_f/K)} (X - \tau'\tau^{-1}(\alpha_1 Y_{\sigma_i(1)} + \cdots + \alpha_n Y_{\sigma_i(n)})) = r_i(X, Y_1, \ldots, Y_n)$$

taking into account that $\pi(\tau)^{-1} = \pi(\tau^{-1})$, $\alpha_{\pi(\tau^{-1})(i)} = \tau^{-1}(\alpha_i)$ and that $\tau'\tau^{-1}$ permutes all the elements of $\mathrm{Gal}(K_f/K)$ when $\tau \in \mathrm{Gal}(K_f/K)$ (τ arbitrary but fixed). Hence for every $\tau \in \mathrm{Gal}(k_f/k)$, we have $\pi(\tau) \in G_{r_i}$.

Conversely, let $\varrho \in G_{r_i}$, that is,

$$\varrho r_i(X, Y_1, \ldots, Y_n) = r_i(X, Y_{\varrho(1)}, \ldots, Y_{\varrho(n)}) = r_i(X, Y_1, \ldots, Y_n).$$

Then on the one hand,

$$r_i(X, Y_1, \ldots, Y_n) = \prod_{\tau \in G(K_f/K)} (X - \tau(\theta_i)) = \prod_{\tau \in G(K_f/K)} (X - \tau(\alpha_1 Y_{\sigma_i(1)} + \cdots + \alpha_n Y_{\sigma_i(n)})) =$$

$$\prod_{\tau \in G(K_f/K)} (X - \tau(\alpha_{\sigma_i^{-1}(1)} Y_1 + \cdots + \alpha_{\sigma_i^{-1}(n)} Y_n)).$$

ond on the other,

$$r_i(X, Y_{\varrho(1)}, \ldots, Y_{\varrho(n)}) = \prod_{\tau \in G(K_f/K)} (X - \tau(\alpha_{\sigma_i^{-1}(1)} Y_{\varrho(1)} + \cdots + \alpha_{\sigma_i^{-1}(n)} Y_{\varrho(n)})) =$$

$$\prod_{\tau \in G(K_f/K)} (X - \tau(\alpha_{\varrho^{-1}\sigma_i^{-1}(1)} Y_1 + \cdots + \alpha_{\varrho^{-1}\sigma_i^{-1}(n)} Y_n)) =$$

Hence $\alpha_{\sigma_i^{-1}(1)} Y_1 + \cdots + \alpha_{\sigma_i^{-1}(n)} Y_n$ is among the elements $\tau(\alpha_{\varrho^{-1}\sigma_i^{-1}(1)} Y_1 + \cdots + \alpha_{\varrho^{-1}\sigma_i^{-1}(n)} Y_n)$, that is, there is $\tau \in \mathrm{Gal}(k_f/k)$ such that $\tau(\alpha_{\varrho^{-1}\sigma_i^{-1}(k)}) = \alpha_{\sigma_i^{-1}(k)}$ for every $k = 1, \ldots, n$. Hence $\pi(\tau)\varrho^{-1}\sigma_i^{-1}(k) = \sigma_i^{-1}(k)$ for $k = 1, \ldots, n$. This means that $\varrho = \pi(\tau)$, so π is bijective, and consequently an isomorphism of $\mathrm{Gal}(k_f/k)$ and G_{r_i}. □

(One can find another proof of this theorem in [C].)

Before the proof of the next theorem, we recall the notations. Let $\varphi : R \to R^*$ be a ring homomorphism mapping an integral domain R into an integral domain R^*. Let K and K^* be fields of quotients of R and R^*, respectively. Let $f \in R[X]$ be separable (that is, without multiple zeros). Denote by f^* the image of f under the homomorphism extending φ to $R[X]$ by applying φ to the coefficients of the polynomials in $R[X]$. We write $\varphi(r) = r^*$, when $r \in R$ and call φ (on all levels) *the reduction homomorphism.*

T. 15.4 (**Dedekind**) (*a*) *Let $f \in R[X]$ be a separable monic polynomial and assume that its image $f^* \in R^*[X]$ is also separable and* $\deg(f) = \deg(f^*) = n$. *Then the Galois group of f^* over K^* has an embedding into the Galois group of f over K.*

(*b*) *Let in* (*a*), $R = \mathbb{Z}$, $R^* = \mathbb{F}_p$ *and let φ be the reduction modulo a prime number p. If $f \in \mathbb{Z}[X]$ and*

$$f^* = f_1^* \cdots f_k^*,$$

where f_i^* are irreducible over $\mathbb{F}_p$, then $\mathrm{Gal}(\mathbb{Q}_f/\mathbb{Q})$ *considered as a permutation subgroup of S_n contains a permutation which is a product of cycles of length* $\deg(f_i{}^*)$ *for $i = 1, \ldots, k$.*

Proof. (a) Let $L = K(\alpha_1, \ldots, \alpha_n)$ and $L^* = K^*(\alpha_1^*, \ldots, \alpha_n^*)$ be splitting fields of $f(X)$ over $K[X]$ and $f^*(X)$ over K^*. Consider the polynomials:

$$r(f)(T, Y_1, \ldots, Y_n) = \prod_{\sigma \in S_n} (T - (\alpha_{\sigma(1)} Y_1 + \cdots + \alpha_{\sigma(n)} Y_n)),$$

and

$$r(f^*)(T, Y_1, \ldots, Y_n) = \prod_{\sigma \in S_n} (T - (\alpha^*_{\sigma(1)} Y_1 + \cdots + \alpha^*_{\sigma(n)} Y_n)).$$

The coefficients of $r(f)(T, Y_1, \ldots, Y_n)$ (of the monomials in variables $T, Y_1, \ldots, Y_n$) are symmetric functions of $\alpha_1, \ldots, \alpha_n$ and as such can be expressed as integer polynomials of the coefficients of f. In exactly the same way, the coefficients of $r(f^*)(T, Y_1, \ldots, Y_n)$ are symmetric functions of $\alpha_1^*, \ldots, \alpha_n^*$ and can be expressed as integer polynomials of the coefficients of f^*. Since the formulae expressing the coefficients of $r(f)$ and $r(f^*)$ by the coefficients of f and f^* are the same, we see that the polynomial $r(f^*)(T, Y_1, \ldots, Y_n)$ is the polynomial $r(f)(T, Y_1, \ldots, Y_n)$ when the homomorphism φ is applied to its coefficients in R.

Notice also that all the $n!$ zeros $\alpha_{\sigma(1)} Y_1 + \cdots + \alpha_{\sigma(n)} Y_n$ of $r(f)$ and $\alpha^*_{\sigma(1)} Y_1 + \cdots + \alpha^*_{\sigma(n)} Y_n$ of $r(f^*)$ as polynomials of T are different when $\sigma \in S_n$. In fact, if $\alpha_{\sigma(1)} Y_1 + \cdots + \alpha_{\sigma(n)} Y_n = \alpha_{\tau(1)} Y_1 + \cdots + \alpha_{\tau(n)} Y_n$ for $\sigma, \tau \in S_n$, then $\alpha_{\sigma(i)} = \alpha_{\tau(i)}$ for $i = 1, \ldots, n$, so $\sigma(i) = \tau(i)$ for each i, since all α_i are different. Hence, we have $\sigma = \tau$. Similarly, we get that all $\alpha^*_{\sigma(1)} Y_1 + \cdots + \alpha^*_{\sigma(n)} Y_n$ are different.

Consider now the factorization of $r(f)(T, Y_1, \ldots, Y_n)$ into irreducible factors, the Galois resolvents, as in (15.3):

$$r(f)(T) = r_1(T, Y_1, \ldots, Y_n) \cdots r_t(T, Y_1, \ldots, Y_n).$$

The homomorphism φ applied to the coefficients in R of the polynomial $r(f)$ and its factors r_i gives the factorization:

$$r^*(f)(T) = r_1^*(T, Y_1, \ldots, Y_n) \cdots r_t^*(T, Y_1, \ldots, Y_n),$$

but the polynomials $r_i^*(T, Y_1, \ldots, Y_n)$ need no longer be irreducible. Consider the resolvent $r_1(T, Y_1, \ldots, Y_n)$ of $f(X)$ and let

$$r_1^* = r_{11}^* \cdots r_{1u}^*,$$

be the factorization of $r_1^*(T, Y_1, \ldots, Y_n)$ into irreducible factors r_{1j}^*. These factors are Galois resolvents of $f^*(X)$.

Consider all permutations of $Y_1, \ldots, Y_n$ which map the resolvent r_{11}^* into itself. By **T.15.3**, such permutations form the group $\mathrm{Gal}(K_f^*/K^*)$. Applying the same permutation to the

Galois resolvent r_1 of $f(X)$, we map it onto one of the resolvents r_i of $f(X)$ for some $i = 1, \dots, t$. We claim that this must be the same resolvent r_1. In fact, if the permutation gives r_i, with $i \neq 1$, then the same permutation transforms r_1^* to r_i^* and since the factor r_{11}^* of r_1^* maps onto itself, it must be also a factor of r_i^*. But if $i \neq 1$, then the polynomials r_1^* and r_i^* are relatively prime, since they are products of different linear factors $T - (\alpha^*_{\sigma(1)} Y_1 + \cdots + \alpha^*_{\sigma(n)} Y_n)$. Thus every permutations of $Y_1, \dots, Y_n$, which maps r_{11}^* into itself also maps r_1 into itself. By **T.15.3** every element of $\mathrm{Gal}(K_f^*/K^*)$ belongs to the group $\mathrm{Gal}(K_f/K)$.

(b) The Galois group of the polynomial f^* over $\mathbb{F}_p$ is cyclic (see **T.5.4**). Let σ be a generator of this group. By Ex. 9.4, the automorphism σ can be represented as a product of k cycles of length equal to the degrees of the irreducible factors of $f^*(X)$ over $\mathbb{F}_p$. Using (a), we get a permutation of this shape in the Galois group $\mathrm{Gal}(\mathbb{Q}_f/\mathbb{Q})$. □

18

Hints and answers

Problems of Chapter 1

1.1 (a) $-3,\ \frac{3}{2} \pm \frac{1}{2} i\sqrt{3}$;

(b) $-7, -1 - i\sqrt{3}, -1 + i\sqrt{3}$;

(c) $-\sqrt[3]{9} - \sqrt[3]{3} - 1,\ \frac{1}{2}(\sqrt[3]{9} + \sqrt[3]{3}) - 1 + \frac{1}{2}\, i\sqrt{3}\,(\sqrt[3]{3} - \sqrt[3]{9}),\ \frac{1}{2}(\sqrt[3]{9} + \sqrt[3]{3}) - 1 - \frac{1}{2}\, i\sqrt{3}\,(\sqrt[3]{3} - \sqrt[3]{9})$;

(d) $\sqrt[3]{2} - \sqrt[3]{4},\ \frac{1}{2}(\sqrt[3]{4} - \sqrt[3]{2}) - \frac{1}{2} i\sqrt{3}(\sqrt[3]{4} + \sqrt[3]{2}),\ \frac{1}{2}(\sqrt[3]{4} - \sqrt[3]{2}) + \frac{1}{2} i\sqrt{3}(\sqrt[3]{4} + \sqrt[3]{2})$;

(e) $1 - i\sqrt{3}, 1 + i\sqrt{3}, \sqrt{2}, -\sqrt{2}$;

(f) $1 - i, 1 + i, \frac{1}{2}(1 + \sqrt{13}), \frac{1}{2}(1 - \sqrt{13})$;

(g) $\frac{1 \pm \sqrt{2}}{2} \pm \frac{1}{2}\sqrt{-1 + 2\sqrt{2}}$;

(h) $1 \pm \sqrt{7} \pm \sqrt{6 + 2\sqrt{7}}$.

1.3 Notice that $(x_1 - x_2)^2 = x_3^2 + \frac{4q}{x_3}$ and similarly for $(x_2 - x_3)^2$ and $(x_3 - x_1)^2$. Express $x_1^3 + x_2^3 + x_3^3$ and $x_1^3 x_2^3 + x_2^3 x_3^3 + x_3^3 x_1^3$ by p, q using Vieta's formulae: $x_1 + x_2 + x_3 = 0$, $x_1 x_2 + x_2 x_3 + x_3 x_1 = p$, $x_1 x_2 x_3 = -q$.

1.4 The equation has solutions $2, -1 \pm \sqrt{3}$. Write down the trigonometric form of the numbers $-1 \pm i$. Thus with suitable choice of the values of the third roots, we have

$$\sqrt[3]{-2 + 2i} + \sqrt[3]{-2 - 2i} = 2.$$

1.5 Represent the complex numbers $-\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$ in the formulae (1.5) in trigonometric form.

1.6 (a) The equation satisfied by α is $x^3 - 3cx + 2a = 0$.

(b) Use the binomial formulae in the following form:

$$(X+Y)^5 = X^5 + Y^5 + 5XY[(X+Y)^3 - 3XY(X+Y)] + 10X^2Y^2(X+Y)$$

with $X = \sqrt[5]{a+\sqrt{b}}$, $Y = \sqrt[5]{a-\sqrt{b}}$. The equation satisfied by α is $x^5 - 5cx^3 - 5c^2x - 2a = 0$. If $a = 1, c = 0$ the polynomial is irreducible (see Chapter 3 concerning irreducibility). Of course, there are equations of degree 5, which can not be represented in this form (e.g. those with coefficient for x^2 different from 0). As we noted in the Remark following this exercise, it is not possible to find a general algebraic formula, which gives an expression of a solution to an arbitrary quintic equation (fifth degree polynomial equation) using the coefficients of the equation, the four arithmetic operations and roots (see Chapter 13).

1.7 If $a = 0$, then the equation $x^n - a = 0$ has only one solution $x = 0$ (with multiplicity n). In general, we have $a = |a|e^{i\varphi}$, so the equality $x^n = |a|e^{i\varphi}$ is equivalent to $x = \sqrt[n]{|a|}e^{\frac{\varphi+2\pi ik}{n}}$ for n different values of $k = 0, 1, \ldots, n-1$.

1.8 Notice that the discriminant of $f(X) = aX^2 + bX + c = a(X - x_1)(X - x_2)$ is $\Delta(f) = (x_1 - x_2)^2 = b^2 - 4ac$ (see the text on quadratic equations on p. 2).

Problems of Chapter 2

2.1 Only (d) is a field.

2.2 Let K be a subfield of $\mathbb{Q}$. Starting with $1 \in K$ motivate that all integers, and then, all rational numbers must belong to K.

2.3 For example, $\mathbb{Z}_p(X)$, where p is a prime number.

2.4 Use **T.2.1** and consider two cases depending whether the prime subfield of K is finite or infinite.

2.5 (a) Show that the sum, difference, product and the quotient of two elements of $K(\alpha)$ belong to $K(\alpha)$.

(b) If ab is a square in K, then it is easy to check the equality of the fields. In the opposite direction, consider two cases: $K(\sqrt{a}) = K(\sqrt{b}) = K$, $K(\sqrt{a}) = K(\sqrt{b}) \neq K$ and the second case use (a).

2.6 Use Ex. 2.5. (a) $a + b\sqrt{2}$, $a, b \in \mathbb{Q}$;
(b) $a + bi$, $a, b \in \mathbb{Q}$;
(c) $a + b\sqrt{2} + ci + di\sqrt{2}$, $a, b, c, d \in \mathbb{Q}$;
(d) $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$, $a, b, c, d \in \mathbb{Q}$.

2.7 If necessary see examples on p. 164.

2.8 (a) $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$;
(b) $\mathbb{Q}(i, \sqrt{2}) = \{a + bi + c\sqrt{2} + di\sqrt{2} : a, b, c, d \in \mathbb{Q}\}$;
(c) $\mathbb{Q}(i, \sqrt{5}) = \{a + bi + c\sqrt{5} + di\sqrt{5} : a, b, c, d \in \mathbb{Q}\}$;
(d) $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$.

2.9 (a) Check that all conditions in the definition of the field are satisfied if and only if every nonzero matrix in the given set has nonzero determinant. The condition that $X^2 + 1 = 0$ has no solutions in K is needed in order to exclude a possibility that a nonzero matrix has determinant equal to 0.

(b) The subfield of L isomorphic to K consist of the diagonal matrices $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$.

(c) Choose $K = \mathbb{F}_3$ in (a).

2.10 (a) Similarly as in Ex. 2.9 check that addition and multiplication of matrices in the given set satisfy all the conditions in the field definition. This time the suitable condition is that the polynomial $X^2 - X + 1$ has no zeros in K, which guarantees that nonzero matrices of given form have nonzero determinants.

(b) Choose $K = \mathbb{F}_2$ in (a). Then the field consists of the following matrices:

$$0 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \qquad 1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad \alpha = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \qquad \beta = 1 + \alpha = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}.$$

The addition and multiplication tables are as follows:

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\cdot$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

2.11 Show that $2a = 0$ for each $a \in K$. The answer is 2.

2.12 (a) For $m = 1$ use the binomial theorem and notice that the binomial coefficients $\binom{p}{i}$ are divisible by p if $0 < i < p$. Afterwards use induction.

(b) The same argument as in (a) for $m = 1$.

2.14 Let α be a zero of $f(X)$. Check that all $\alpha + i$ for $i = 1, \ldots, p - 1$ are also zeros of this polynomial. Motivate that the polynomial $X^p - X + a$ has no zeros in $\mathbb{F}_p$ when $a \in \mathbb{F}_p$ and $a \neq 0$.

Problems of Chapter 3

3.1 (b) In general, for any complex number a, we have $X^4+a^2 = X^4+2aX^2+a^2-2aX^2 = (X^2+a)^2-(\sqrt{2a}X)^2 = (X^2-\sqrt{2a}X+a)(X^2+\sqrt{2a}X+a)$.

3.2 All polynomials of degree 1 are x, $x+1$. Construct all reducible polynomials of degree 2 using these two. Which are not on the list? Answer: x^2+x+1. This is the only irreducible polynomial of degree 2. Construct all reducible polynomials of degree 3 using these three: $X, X+1, X^2+X+1$. Which are not on the list? Answer: X^3+X+1, X^3+X^2+1. Continue the process! Answer: X^4+X+1, $X^4+X^3+X^2+X+1$, X^4+X^3+1, X^5+X^2+1, X^5+X^3+1.

3.4 (a) $X^4+64 = (X^2+4X+8))(X^2-4X+8)$ (see above Ex. 3.1 (b));

(b) $X^4+1 = (X^2-\sqrt{2}X+1)(X^2+\sqrt{2}X+1)$ (see above Ex. 3.1 (b));

(c) $X^7+1 = (X+1)(X^3+X+1)(X^3+X^2+1)$;

(d) X^4+2 is irreducible in $\mathbb{F}_5[X]$;

(e) X^3-2 is irreducible in $\mathbb{Q}[X]$;

(f) $X^6+27 = \left(X^2+3\right)\left(X^2+3\,X+3\right)\left(X^2-3\,X+3\right)$;

(g) $X^3+2 = (X+2)^3$ in $\mathbb{F}_3[X]$;

(h) $X^4+2 = (X+1)(X+2)(X^2+1)$.

3.7 (a) Assume $f(X) = g(X)h(X)$, where $g(X), h(X)$ are monic polynomials in $\mathbb{Z}[X]$, $\deg g(X) = k \geq 1$ and $\deg h(X) = l \geq 1$ and look at the relation between the images of $f(X), g(X), h(X)$ when the reduction modulo p is applied.

(b) Choose $p = 2$ in Eisenstein's criterion.

(c) Consider the polynomial $f(X+1)$ and use Eisenstein's criterion.

3.8 (c) Use prime numbers $p = 2$ in (c_1) and (c_2), $p = 5$ in (c_3), $p = 2, 3$ in (c_4) and (c_6), $p = 2, 5$ in (c_5).

3.10 Let $f_1, f_2, \ldots, f_r$ be irreducible polynomials over K and consider the polynomial $f_1 f_2 \ldots f_n + 1$. Use the fact that $K[X]$ has unique factorization (see **T.3.2**). Observe that the exercise is trivial over infinite fields.

3.12 Use Gauss's Lemma **T.3.3**.

Problems of Chapter 4

4.1 (a), (b), (c) are algebraic. Use **T.4.6**. (d), (e), (f) are transcendental. Use **T.4.6** and the transcendence of e and π.

4.2 (a) Use **T.4.2** and **T.4.3** (one can also use Ex. 4.10 (b) and **T.4.2** (a)). You may need a result saying that the equation $f(X) = 0$ has a solution in a field containing L (see Chapter 5).

(b) Use (a).

4.3 The degree of each number is equal to the degree of its minimal polynomial. These polynomials are:

(a) $X^6 - 2X^3 - 2$;
(b) $X^6 - 6X^4 - 4X^3 + 12X^2 - 24X - 4$;
(c) $X^4 + X^3 + X^2 + X + 1$;
(d) $X^2 - 2$;
(e) $X^3 - 2$;
(f) $X^{p-1} + X^{p-2} + \ldots + X + 1$.

In each case, we have to motivate that the polynomial is irreducible. In order to prove this, one can use different methods discussed in Chapter 3. In case (b), it may be useful to apply **T.4.2**, and in case (e), Ex. 4.10 (b).

4.4 Use **T.4.2** and **T.4.3** in order to construct suitable bases.

(a) 4; a basis: $1, i, \sqrt{2}, i\sqrt{2}$;
(b) 4; a basis $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$;
(c) 6; a basis $1, i, \sqrt[3]{2}, \sqrt[3]{4}, i\sqrt[3]{2}, i\sqrt[3]{4}$;
(d) 3; a basis: $1, \sqrt[3]{2}, \sqrt[3]{4}$;
(e) 2; a basis: $1, X$;
(f) 8; a basis: $1, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{10}, \sqrt{15}, \sqrt{30}$;
(g) 3; a basis: $1, \alpha, \alpha^2$, where $\alpha = \sqrt[3]{1+\sqrt{3}}$;
(h) 4; a basis: $1, \alpha, \alpha^2, \alpha^3$;
(i) 3; a basis: $1, \alpha, \alpha^2$;
(j) 4; a basis: $1, X, X^2, X^3$.

4.5 Notice that if $z = a + bi$ is algebraic, so is also $\bar{z} = a - bi$ (give a suitable argument!). Use Ex. 3.5 and **T.4.6** in both directions.

4.6 Consider $z = \cos r\pi + i \sin r\pi$ and use Ex. 4.4.

4.7 (a) $x = \frac{1}{2}\sqrt[3]{4}$; (b) $x = \frac{1}{3}(1 - \sqrt[3]{2} + \sqrt[3]{4})$; (c) $x = -1 + \sqrt[3]{4}$.

4.8 (a) $x = -\sqrt{2} + \sqrt{3}$; (b) $x = \frac{1}{2} + \frac{1}{4}\sqrt{2} - \frac{1}{4}\sqrt{6}$; (c) $x = \frac{1}{2}(-5 + 4\sqrt{2} + 3\sqrt{3} - 2\sqrt{6})$.

4.9 (a) $x = 1 + \alpha^3$; (b) $x = \alpha + \alpha^2$; (c) $x = 1$; (d) $x = \alpha + \alpha^2$.

4.10 (a) Notice that $p(Y) - \frac{p(X)}{q(X)}q(Y)$ is a nonzero polynomial in Y of degree n over $K(\alpha)$, where $\alpha = \frac{p(X)}{q(X)}$ having X as its zero.

(b) Use (a) and **T.4.3**.

(c) Show that the polynomial $p(Y) - \alpha q(Y)$ is irreducible over the field $K(\alpha)$, for example, using a version of Gauss's Lemma **T.3.3** and the remark after it for $R = K[\alpha]$. Notice that the degree of this polynomial with respect to α is one.

4.11 In (b) and (c) use **T.4.3**.

(d) In general, we have $[M_1M_2 : K] \leq [M_1 : K][M_2 : K]$ and for trivial reasons, the inequality may be strict (e.g. $M_1 = M_2$ and bigger than K). If $[M_1M_2 : K] = [M_1 : K][M_2 : K]$, then $M_1 \cap M_2 = K$ and $[M_1M_2 : M_1] \leq [M_2 : K]$ (as a consequence of the inequality above).

4.12 Consider $[K(\alpha) : K(\alpha^2)]$ and use **T.4.3**. The answer to the second part of the exercise is no (give a counterexample!).

4.13 (a) Consider a minimal polynomial of an element $\alpha \in L \setminus \mathbb{C}$ (if such exists) and use the Fundamental Theorem of Algebra.

(b) Consider the minimal polynomial of an element $\alpha \in L \setminus \mathbb{R}$ (if such exists) and use Ex. 3.5 (b).

4.14 No. Consider $K = \mathbb{Q}$ and $L = \mathbb{Q}(\alpha) \supset \mathbb{Q}$, where $\alpha^4 + \alpha + 1 = 0$. Prove that there is no quadratic extension of $\mathbb{Q}$, which is contain in L.

4.15 Study the tower of extensions $\mathbb{Q}(e, \pi) \supset \mathbb{Q}(e + \pi, e\pi) \supset \mathbb{Q}$.

4.16 (a) Let $f(X) = \alpha_n X^n + \cdots + \alpha_1 X + \alpha_0$, where α_i for $i = 0, 1, \ldots, n$ are algebraic over K. Consider the tower of fields $K \subseteq K(\alpha_0, \alpha_1, \ldots, \alpha_n) \subseteq K(\alpha_0, \alpha_1, \ldots, \alpha_n, \alpha)$ and use **T.4.2**, **T.4.3** and **T.4.4**.

(b) Use **T.4.6** and (a).

4.17 Use **T.4.5**.

Problems of Chapter 5

5.1 (a) $4; 1, \sqrt{2}, \sqrt{5}, \sqrt{10}$;
(b) $6; 1, \sqrt[3]{2}, \sqrt[3]{4}, \varepsilon, \varepsilon\sqrt[3]{2}, \varepsilon\sqrt[3]{4}, \varepsilon^3 = 1, \varepsilon \neq 1$;
(c) $8; 1, i, \sqrt{2}, i\sqrt{2}, \sqrt[4]{2}, i\sqrt[4]{2}, \sqrt[4]{8}, i\sqrt[4]{8}$;
(d) $8; 1, \alpha, \alpha^2, \alpha^3, i, i\alpha, i\alpha^2, i\alpha^3$, where $\alpha = \sqrt{\frac{1}{2}(-1 + \sqrt{5})}$;
(e) $4, 1, \alpha, \alpha^2, \alpha^3$, where $\alpha = e^{\frac{\pi i}{4}}$;
(f) $4; 1, \alpha, \alpha^2, \alpha^3$, where $\alpha = \sqrt[4]{2}$;
(g) $4; 1, \sqrt{2}, \sqrt{3}, \sqrt{6}$;
(h) $p - 1; 1, \alpha, \ldots, \alpha^{p-2}$, where $\alpha = e^{\frac{2\pi i}{p}}$.

5.2 (a) yes; (b) yes; (c) no.

5.3 Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be zeros of $f(X)$ in $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Consider the chain of the fields

$$K \subseteq K(\alpha_1) \subseteq K(\alpha_1, \alpha_2) \subseteq \cdots \subseteq K(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

5.4 Use **T.5.4** and **T.4.3**.

5.5 (a) Compute the number of elements in the field $\mathbb{F}_p[X]/(f(X))$ and use **T.5.4**.

(b) Consider the field $\mathbb{F}_p[X]/(f(X))$ and use **T.5.4** and Ex. 5.4.

5.6 Prove the first formula using Ex. 5.5 (that is easy). The second formula is a special case of the following general theorem: If $f : \mathbb{N} \to \mathbb{C}$ and $g : \mathbb{N} \to \mathbb{C}$ are two arbitrary functions and

$$f(n) = \sum_{d|n} g(d), \text{ then } g(n) = \sum_{d|n} f(d)\mu\left(\frac{n}{d}\right).$$

The last implications is called Möbius' inversion formula and can be easily proved using the equality $\sum_{d|n} \mu(d) = 0$ when $n \neq 1$. Use the inversion formula when $f(n) = p^n$ and $g(n) = nv_p(n)$. For a detailed proof of the Möbius inversion formula see **A.10.2**.

5.7 (a) There are many proofs of this result. For one of them see **A.4.2**.

(b) According to (a), the group L^* is cyclic. Take one of its generators as γ. See also Ex. 8.15.

5.8 (a) Show that the zeros of the primitive polynomials are exactly the generators of the group of the nonzero elements of the field. In such a field with p^n elements, compute the number of elements, which generate the group of its nonzero elements. Afterwards, find the number of the irreducible polynomials, which have these elements as their zeros. Use Ex. 5.5.

(b) Using for example **T.5.4**, motivate that $\mathbb{F}$ has an extension of degree n. Use Ex. 5.7.

5.9 Use the evident formula for $(f + g)'$ and start the proof with $f = aX^m, g = bX^n$.

5.10 (a) Use Ex. 5.8 (a).

(b) In one direction, use **T.5.3**.

5.11 (b) Consider $X^4 + 4$, for example, over $\mathbb{Q}$.

5.12 Motivate that the polynomial $X^4 + 1$ has a zero in the field $\mathbb{F}_{p^2}$ by studying its multiplicative group of order $p^2 - 1$, which is divisible by 8 if only $p > 2$.

Problems of Chapter 6

6.1 (a) Let $f(X) = a_nX^n + \ldots + a_1X + a_0$ and $f(\alpha) = 0$. Look at $\sigma(f(\alpha))$.

(b) How to express the elements of the field $K(\alpha_1, \ldots, \alpha_n)$? See the definition in Chapter 2.

6.2 (a) $G = \{\sigma_0, \sigma_1\}$, $\sigma_0 = id.$, $\sigma_1(\sqrt{2}) = -\sqrt{2}$;
(b) $G = \{\sigma_0\}$, $\sigma_0 = id.$;
(c) $G = \{\sigma_0, \sigma_1\}$, $\sigma_0 = id.$, $\sigma_1(\sqrt[4]{2}) = -\sqrt[4]{2}$;
(d)

G	$\sqrt{2}$	$\sqrt{3}$
σ_0	$\sqrt{2}$	$\sqrt{3}$
σ_1	$-\sqrt{2}$	$\sqrt{3}$
σ_2	$\sqrt{2}$	$-\sqrt{3}$
σ_3	$-\sqrt{2}$	$-\sqrt{3}$

(e) $G = \{\sigma_0\}$, $\sigma_0 = id.$;
(f) $G = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}$. $\sigma_i(X) = iX$.

6.3 (a) Let σ be an automorphism of a field. Look at $\sigma(1), \sigma(2) = \sigma(1+1)$ and so on.

6.4 Show that $\sigma(x) > 0$ if $x > 0$ (use $x = (\sqrt{x})^2$). Assume that, e.g. $\sigma(x) > x$ and choose $r \in \mathbb{Q}$ such that $\sigma(x) > r > x$. Use afterwards Ex. 6.3 (a).

6.5 Consider $L^{G(L/K)}$ and use **T.6.2**.

6.6 (a) Use Ex. 4.9.

(c) Check that the mapping sending a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(K)$ onto a function $\varphi(X) = \frac{aX+b}{cX+d}$ is a group homomorphism. Find its kernel. For repetition see A.2.6.

6.7 $|G| = 6$, $L^G = \mathbb{Z}_2(\alpha)$, where $\alpha = \frac{(X^3+X+1)(X^3+X^2+1)}{(X^2+X)^2}$.

6.8 $|G| = 6$, $L^G = \mathbb{Z}_3(X^6 + X^4 + X^2)$.

6.9 (a) $L^G = \mathbb{R}(X^2, Y)$.

6.10 (a) $L^G = \mathbb{R}(X^2, XY)$.

6.11 $L^G = \mathbb{Q}(X^2, Y^2)$.

6.12 $L^G = \mathbb{Q}$. Use **T.6.2** and Ex. 4.9.

6.13 (a) $L^G = K(X + Y, XY)$.

6.14 No. Construct a counterexample using $L = K(X)$.

6.15 (a) 2; $\sigma_0(a) = a$, $\sigma_1(a) = 2a^2 - a^5$;

(b) 4; $\sigma_0(a) = a$, $\sigma_1(a) = -a$, $\sigma_2(a) = \frac{1}{2}a^5$, $\sigma_3(a) = -\frac{1}{2}a^5$;

(c) 4; $\sigma_0(a) = a$, $\sigma_1(a) = -a$, $\sigma_2(a) = 10a^5 - a^{11}$, $\sigma_3(a) = a^{11} - 10a^5$.

Problems of Chapter 7

7.1 (a), (b), (e) and (h) are not normal, all other are.

7.2 (a) $\mathbb{Q}(\sqrt[4]{2}, i)$;
(b) $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \varepsilon)$, $\varepsilon^3 = 1$, $\varepsilon \neq 1$;
(c) L;
(d) $\mathbb{Q}(X, \varepsilon)$, $\varepsilon^3 = 1$, $\varepsilon \neq 1$;
(e) $\mathbb{Q}(X, i)$, $i^2 = -1$;
(f) $L(\alpha), \alpha^2 + 1 = 0$.

7.3 (a) and (c) Not necessarily! Give an example! (b) Yes.

7.4 Use **T.5.1** (b) and **T.5.2**.

7.5 Use **T.7.1**, Ex. 6.1 and in (b), Ex. 7.4.

7.6 In (a) and (b) use **T.7.1**.

7.7 Show that a minimal polynomial of β over K is irreducible over $K(\alpha)$.

7.8 Let α_i and α_j be zeros of two irreducible factors of $f(X)$ over L. Consider the field extensions $K(\alpha_i) \subseteq L(\alpha_i)$ and $K(\alpha_j) \subseteq L(\alpha_j)$. Use **T.5.1** and **T.5.2**.

7.9 (a) Use **T.4.2**.

(b) Consider one concrete example of a splitting field of $X^n - 2$ with $n > 2$ (e.g. $n = 4$) – the general argument will be similar.

7.10 (a) 12,2; Two quadratic factors of $f(X)$ over K have the same splitting field: Find the discriminats of these polynomials and show that their product is a square (in fact, 9). The command `>galois(f(X)` also gives a solution.

(b) 6,1; (the polynomial is normal).

(c) 36,3; The polynomial $f(X)$ has a quadratic and a cubic irreducible factor over K. The splitting field of $f(X)$ over K has degree 6 as the quadratic factor remains irreducible over the cubic extension of K (see Ex. 4.2). You can use the command `>galois(f(X))`.

(d) 48,3; The polynomial $f(X)$ has an irreducible factor of degree 4 over K but it is not normal over K. Use the command `>galois(f(X))`, which gives the degree of the normal

closure. You can see that it is not sufficient to adjoin one zero of the quadric polynomial to K in order to get the normal closure.

(e) 5040,6; Use `>galois(f(X)` and Ex. 5.3 (possibly also Ex. 16.50)).

(f) 14,2; There are 3 irreducible quadratic factors of $f(X)$ over K and all have the same splitting field over K. Either use `>galois(f(X))` or check that for each two of these factors, the product of their discriminants is a square (so they have the same splitting field).

7.11 Only (b) is not normal.

Problems of Chapter 8

8.1 (a) Find the minimal polynomial of X over the field $\mathbb{F}_p(X^2)$. Use the definition of separability or **T.8.1**.

(b) For example, $L \supset K$, where $L = \mathbb{F}_p(X)$, $K = \mathbb{F}_p(X^p)$.

(c) $\mathbb{F}_2(X)$ is a splitting field of the polynomial $T^2 - X^2$ over the field $\mathbb{F}_2(X^2)$.

8.3 (a) Consider $K \subseteq K(\alpha^p) \subseteq K(\alpha)$. Use **T.8.1** (b).

(c) If K is perfect show that every irreducible factor of $X^p - a$, where $a \in K$ must be of degree 1. Use **T.8.1**(b). Conversely, when $K = K^p$ use the same argument as in the proof of **T.8.1**(a) on p. 105 in the case of a finite field K.

(d) Show that L is separable over K using (b) and (c).

8.4 (a) Use Ex. 8.3.

(b) Use (a) and **T.7.2**.

8.5 Use Ex. 8.4.

8.6 Use **T.8.1** (b).

8.7 As a first step, assume $L = K(\gamma)$.

8.8 Use Ex. 8.4.

8.9 Use Ex. 8.7.

8.10 (a) For example $\sqrt{2} + \sqrt{3}$; (d) For example $X + Y$;
(b) For example $\sqrt{2} + \sqrt{3} + i$; (e) For example X;
(c) For example $\sqrt{2} + \sqrt{3} + i$; (f) For example $\sqrt{2} + \sqrt[3]{2}$ or $\sqrt[6]{2}$.

8.11 Show that if γ exists, then $\gamma^2 \in K$. Find $[L : K]$.

8.12 (a) Compare the degrees of L over M and L over the subfield of M generated over K by the coefficients of the minimal polynomial of γ over M.

(b) If $L = K(\gamma)$, then use the fact that the minimal polynomial of γ over M divides the minimal polynomial of γ over K. In the opposite direction, show that L is finitely generated and algebraic over K. Use Ex. 4.10. Thereafter, consider separately K finite and K infinite. If K is finite use Ex. 5.7. If K is infinite, use the fact that L as a vector space over K is not a union of a finite number of proper subspaces (choose any γ, which is not in the union of all proper subfields of L containing K).

8.13 Consider $K \subset L$ from Ex. 8.11. (e.g. $\mathbb{F}_p(X^2, Y^2, X + cY)$, where $c \in K$).

8.14 Use **T.8.2**.

8.15 (b) No. (c) 4, 6 for $n = 2$, 13, 24 for $n = 3$, 32, 54 for $n = 4$.

8.16 Use Ex. 2.13 and Ex. 8.4.

8.17 For example: (a) $c = \sqrt[6]{2}$; (b) $c = \sqrt[15]{3^5 5^3}$; (c) $c = \sqrt[3]{3} + \sqrt[3]{5}$; (d) $c = \sqrt[15]{2}$.

Problems of Chapter 9

9.1 (c), (d), (e), (f) if $p \neq 2$ and (g) are Galois extensions, the remaining, are not Galois.

9.2 (a) $L = \mathbb{Q}(\sqrt{2}, \sqrt{5})$; $[L : \mathbb{Q}] = |G(L : \mathbb{Q})| = 4$, $G = G(L : \mathbb{Q}) = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}$, where

G	$\sqrt{2}$	$\sqrt{5}$	o
σ_0	$\sqrt{2}$	$\sqrt{5}$	1
σ_1	$-\sqrt{2}$	$\sqrt{5}$	2
σ_2	$\sqrt{2}$	$-\sqrt{5}$	2
σ_3	$-\sqrt{2}$	$-\sqrt{5}$	2

The subgroups of G: $I = \{\sigma_0\}$,
$H_1 = \{\sigma_0, \sigma_1\}$, $H_2 = \{\sigma_0, \sigma_2\}$, $H_3 = \{\sigma_0, \sigma_3\}$.

The fields between $\mathbb{Q}$ and L: $L^G = \mathbb{Q}$, $L^I = L$,
$L^{H_1} = \mathbb{Q}(\sqrt{5})$, $L^{H_2} = \mathbb{Q}(\sqrt{2})$, $L^{H_3} = \mathbb{Q}(\sqrt{10})$.

(b) $L = \mathbb{Q}(i, \sqrt{5})$. Compare (a).

(c) $L = \mathbb{Q}(\varepsilon)$, $\varepsilon = e^{\frac{2\pi i}{5}}$, $[L : \mathbb{Q}] = |G(L : \mathbb{Q})| = 4$, $G = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}$, where

G	ε	o
σ_0	ε	1
σ_1	ε^2	4
σ_2	ε^3	4
σ_3	ε^4	2

The subgroups of G: $G, I = \{\sigma_0\}$, $H = \{\sigma_0, \sigma_3\}$.
The fields between $\mathbb{Q}$ and L: $L^G = \mathbb{Q}$, $L^I = L$,
$L^H = \mathbb{Q}(\varepsilon + \varepsilon^4) = \mathbb{Q}(\cos\frac{2\pi}{5}) = \mathbb{Q}(\sqrt{5})$.

(d) $L = \mathbb{Q}(i, \sqrt{2})$. Compare (a).

(e) $L = K(\sqrt[4]{2}); [L:K] = |G(L/K)| = 4$, $G = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}$, where

G	$\sqrt[4]{2}$	o
σ_0	$\sqrt[4]{2}$	1
σ_1	$-\sqrt[4]{2}$	2
σ_2	$i\sqrt[4]{2}$	4
σ_3	$-i\sqrt[4]{2}$	4

The subgroups of G; $G, I = \{\sigma_0\}$, $H = \{\sigma_0, \sigma_1\}$.
The fields between K and L: $L^G = K : L^I = L$,
$L^H = K(\sqrt{2}) = \mathbb{Q}(i, \sqrt{2})$.

(f) $L = \mathbb{Q}(\sqrt[3]{5}, \varepsilon), \varepsilon^3 = 1, \varepsilon \neq 1; [L:\mathbb{Q}] = |G(L:\mathbb{Q})| = 6$, $G = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5\}$, where

G	$\sqrt[3]{5}$	ε	o
σ_0	$\sqrt[3]{5}$	ε	1
σ_1	$\sqrt[3]{5}$	ε^2	2
σ_2	$\varepsilon\sqrt[3]{5}$	ε	3
σ_3	$\varepsilon\sqrt[3]{5}$	ε^2	2
σ_4	$\varepsilon^2\sqrt[3]{5}$	ε	3
σ_5	$\varepsilon^2\sqrt[3]{5}$	ε^2	2

Subgroups till G: $G, I = \{\sigma_0\}$, $H_1 = \{\sigma_0, \sigma_1\}$, $H_2 = \{\sigma_0, \sigma_3\}$,
$H_3 = \{\sigma_0, \sigma_5\}$, $H = \{\sigma_0, \sigma_2, \sigma_4\}$.
The fields between $\mathbb{Q}$ and L: $L^G = \mathbb{Q}$, $L^I = L, L^{H_1} = \mathbb{Q}(\sqrt[3]{5})$,
$L^{H_2} = \mathbb{Q}(\varepsilon^2\sqrt[3]{5})$, $L^{H_3} = \mathbb{Q}(\varepsilon\sqrt[3]{5})$, $L^H = \mathbb{Q}(\varepsilon)$.

(g) $L = \mathbb{Q}(\alpha, i)$, $\alpha = \sqrt{\frac{1}{2}(\sqrt{5}-1)}; [L:\mathbb{Q}] = |G(L:\mathbb{Q})| = 8$. Let $\beta = \sqrt{\frac{1}{2}(\sqrt{5}+1)}$ $(\alpha\beta = 1)$.
$G = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6, \sigma_7\}$, where

G	α	i	o
σ_0	α	i	1
σ_1	$-\alpha$	i	2
σ_2	$i\beta$	i	2
σ_3	$-i\beta$	i	2
σ_4	α	$-i$	2
σ_5	$-\alpha$	$-i$	2
σ_6	$i\beta$	$-i$	4
σ_7	$-i\beta$	$-i$	4

Subgroups till G: $G, I = \{\sigma_0\}$, $H_1 = \{\sigma_0, \sigma_1\}$, $H_2 = \{\sigma_0, \sigma_2\}$,
$H_3 = \{\sigma_0, \sigma_3\}, H_4 = \{\sigma_0, \sigma_4\}, H_5 = \{\sigma_0, \sigma_5\}$,
$H_{23} = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}$, $H_{45} = \{\sigma_0, \sigma_1, \sigma_4, \sigma_5\}$, $H_{67} = \{\sigma_0, \sigma_1, \sigma_6, \sigma_7\}$.
The fields between $\mathbb{Q}$ and L: $L^G = \mathbb{Q}$, $L^I = L, L^{H_1} = \mathbb{Q}(\sqrt{5}, i)$,
$L^{H_2} = \mathbb{Q}(\alpha + i\beta)$, $L^{H_3} = \mathbb{Q}(\alpha - i\beta)$, $L^{H_4} = \mathbb{Q}(\alpha)$, $L^{H_5} = \mathbb{Q}(i\alpha)$,
$L^{H_{23}} = \mathbb{Q}(i)$, $L^{H_{45}} = \mathbb{Q}(\sqrt{5})$, $L^{H_{67}} = \mathbb{Q}(i\sqrt{5})$, .

(h) $L = K(\varepsilon)$, $\varepsilon^3 = 1$, $\varepsilon \neq 1; [L:K] = |G(L/K)| = 2$, $G = \{\sigma_0, \sigma_1\}$, where
$\sigma_0 = id.$, $\sigma_1(\varepsilon) = \varepsilon^2$. Only the trivial subgroups and subfields.

9.3 (b) We take in Ex. 9.2 (a)–(h) only the zeros of $f(X)$, which are not in the ground field K.

(a) The zeros: $\sqrt{2}, -\sqrt{2}, \sqrt{5}, -\sqrt{5}$ numbered $1, 2, 3, 4$, respectively. Then $\sigma_0, \sigma_1, \sigma_2, \sigma_3$ are $(1), (1,2), (3,4), (1,2)(3,4)$, respectively.

(b) The zeros: $i, -i, \sqrt{5}, -\sqrt{5}$ numbered $1, 2, 3, 4$, respectively. As in (a).

(c) The zeros: $\varepsilon, \varepsilon^2, \varepsilon^3, \varepsilon^4$ $(\varepsilon = e^{\frac{2\pi i}{5}})$ numbered $1, 2, 3, 4$, respectively. Then $\sigma_0, \sigma_1, \sigma_2, \sigma_3$ are $(1), (1,2,4,3), (1,3,4,2), (1,4)(2,3)$, respectively.

(d) The zeros: $\alpha = 1/2\sqrt{2} + 1/2\, i\sqrt{2}, -\alpha, \bar{\alpha}, -\bar{\alpha}$ numbered $1, 2, 3, 4$, respectively. The four automorphisms defined by $\sigma(\sqrt{2}) = \pm\sqrt{2}, \sigma(i) = \pm i$ are $\{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$.

(e) The zeros: $\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}$ numbered $1,2,3,4$, respectively. Then $\sigma_0, \sigma_1, \sigma_2, \sigma_3$ are $(1), (1,2)(3,4), (1,3,2,4), (1,4,2,3)$, respectively.

(f) The zeros: $\sqrt[3]{5}, \varepsilon\sqrt[3]{5}, \varepsilon^2\sqrt[3]{5}$, numbered $1,2,3$, respectively. Then $\sigma_0, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5$ are $(1), (2,3), (1,2,3), (1,2), (1,3,2), (1,3)$, respectively.

(g) In the notations of Ex. 9.2 (g), the zeros are $\alpha, -\alpha, i\beta, -i\beta$ numbered $1,2,3,4$ in this order. Then the automorphisms $\sigma_0, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6, \sigma_7$ are $(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3), (3,4), (1,2), (1,3,2,4), (1,4,2,3)$, respectively.

(h) The zeros are $\varepsilon, \varepsilon^2$, where $\varepsilon = e^{\frac{2\pi i}{3}}$, numbered $1,2$ in the given order. The automorphisms σ_0, σ_1 are $(1), (1,2)$.

9.4 (a) Use Ex. 6.1.

(b) Use **T.5.1**(b), **T.5.2**(b) and Ex. 6.1.

(c) Use Theorem **T.9.1**(b).

9.5 (a) Modify Ex. 9.2 (a).

(b) Modify Ex. 9.2 (f).

(c) $[L:\mathbb{Q}] = |G(L:\mathbb{Q})| = 8$, since L is a splitting field of $X^4 - 2$ over $\mathbb{Q}$. $G = G(L:\mathbb{Q}) = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6, \sigma_7\}$, where

G	$\sqrt[4]{2}$	i	o
σ_0	$\sqrt[4]{2}$	i	1
σ_1	$-\sqrt[4]{2}$	i	2
σ_2	$i\sqrt[4]{2}$	i	4
σ_3	$-i\sqrt[4]{2}$	i	4
σ_4	$\sqrt[4]{2}$	$-i$	2
σ_5	$-\sqrt[4]{2}$	$-i$	2
σ_6	$i\sqrt[4]{2}$	$-i$	2
σ_7	$-i\sqrt[4]{2}$	$-i$	2

The subgroups of G: $G, I = \{\sigma_0\}, H_1 = \{\sigma_0, \sigma_1\}$, $H_2 = \{\sigma_0, \sigma_4\}, H_3 = \{\sigma_0, \sigma_5\}, H_4 = \{\sigma_0, \sigma_6\}$, $H_5 = \{\sigma_0, \sigma_7\}, G_1 = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}$, $G_2 = \{\sigma_0, \sigma_1, \sigma_4, \sigma_5\}, G_3 = \{\sigma_0, \sigma_1, \sigma_6, \sigma_7\}$.
The fields between $\mathbb{Q}$ and L: $L^G = \mathbb{Q}, L^I = L$;
$L^{H_1} = \mathbb{Q}(\sqrt{2}, i), L^{H_2} = \mathbb{Q}(\sqrt[4]{2}), L^{H_3} = \mathbb{Q}(i\sqrt[4]{2})$,
$L^{H_4} = \mathbb{Q}((1+i)\sqrt[4]{2}), L^{H_5} = \mathbb{Q}((1-i)\sqrt[4]{2})$,
$L^{G_1} = \mathbb{Q}(i), L^{G_2} = \mathbb{Q}(\sqrt{2}), L^{G_3} = \mathbb{Q}(i\sqrt{2})$.

(d) $[L:K)| = 4$, since K is the fixed field of the group $G = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}$, which is the group of K-automorphisms of L, where:

G	X	o
σ_0	X	1
σ_1	$-X$	2
σ_2	$1/X$	2
σ_3	$-1/X$	2

The subgroups of G: $G, I = \{\sigma_1\}, H_1 = \{\sigma_0, \sigma_1\}$
$H_2 = \{\sigma_0, \sigma_2\}$, $H_3 = \{\sigma_0, \sigma_3\}$.
The fields between K and L: $L^G = K, L^I = L$,
$L^{H_1} = \mathbb{R}(X^2)$,
$L^{H_2} = \mathbb{R}(X + \frac{1}{X}), L^{H_3} = \mathbb{R}(X - \frac{1}{X})$.

(e) $[L:K] = |G(L/K)| = 4$, since K is the fixed field of the group $G = G(L/K) = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}$ of K-automorphisms of L, where

G	X	Y	o
σ_0	X	Y	1
σ_1	$-X$	Y	2
σ_2	X	$-Y$	2
σ_3	$-X$	$-Y$	2

The subgroups of G: $G, I = \{\sigma_0\}$, $H_1 = \{\sigma_0, \sigma_1\}$, $H_2 = \{\sigma_0, \sigma_2\}$, $H_3 = \{\sigma_0, \sigma_3\}$.
The fields between K and L: $L^G = K, L^I = L$, $L^{H_1} = \mathbb{R}(X^2, Y)$, $L^{H_2} = \mathbb{R}(X, Y^2)$, $L^{H_3} = \mathbb{R}(X^2, XY)$.

(f) $[L : K] = |G(L/K)| = 4$, since K is the fix field of the group $G = G(L/K) = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}$ of K-automorphisms of L, where

G	X	Y	o
σ_0	X	Y	1
σ_1	$-X$	$-Y$	2
σ_2	Y	X	2
σ_3	$-Y$	$-X$	2

The subgroups of G: $G, I = \{\sigma_0\}$, $H_1 = \{\sigma_0, \sigma_1\}$, $H_2 = \{\sigma_0, \sigma_2\}$, $H_3 = \{\sigma_0, \sigma_3\}$.
The fields between K and L: $L^G = K$, $L^I = L$, $L^{H_1} = \mathbb{R}(X^2, XY)$, $L^{H_2} = \mathbb{R}(X + Y, XY)$, $L^{H_3} = \mathbb{R}(X - Y, XY)$.

9.6 No.

9.7 $L = \mathbb{Z}_3(X)$, $L^G = \mathbb{Z}_3(X^6 + X^4 + X^2)$, $[L : L^G] = 6$.

G	X	o
σ_0	X	1
σ_1	$X + 1$	3
σ_2	$X + 2$	3
σ_3	$2X$	2
σ_4	$2X + 1$	2
σ_5	$2X + 2$	2

The subgroups of G: $G, I = \{\sigma_0\}, H_1 = \{\sigma_0, \sigma_3\}$, $H_2 = \{\sigma_0, \sigma_4\}, H_3 = \{\sigma_0, \sigma_5\}, H = \{\sigma_0, \sigma_1, \sigma_2\}$.
The fields between L^G and L: $L^G, L^I = L, L^{H_1} = \mathbb{Z}_3(X^2)$, $L^{H_2} = \mathbb{Z}_3(X^2 - X), L^{H_3} = \mathbb{Z}_3(X^2 + X), L^H = \mathbb{Z}_3(X^3 - X)$.

9.8 $L \supseteq M$ and $L \supseteq K$ are Galois extensions. Use **T.9.1**(a).

9.9 (b) Consider the index of $H(L/M)$ in $G(L/K)$ and use the homomorphism $\varphi : H(L/M) \to G(M/K)$, where $\varphi(\sigma) = \sigma|_M$. Use **T.9.1**.

(c) Use (b) and **T.9.1**(a).

(d) Check directly that $\mathcal{N}(G(L/M)) \subseteq H(L/M)$. Use (b) and the characterization of the normaliser as the biggest subgroup of $G(L/K)$ in which $G(L/M)$ is normal.

9.10 (a) Use the definition of the normal extension together with **T.9.1**(a) and **T.4.3**.

(b) How to describe all the zeros of $f_\alpha(X)$ in terms of α and $\sigma \in G(L/K)$? Use (a).

(c) Count how many times a given zero $\beta = \sigma(\alpha)$ of $f_\alpha(X)$ (for a fixed $\sigma \in G(L/K)$) appears among the images $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$.

9.11 (a) Consider L as vector space over L^H and use **T.6.3** in order to show that the image of Tr_H has dimension 1.

(b) Use (a) and the properties of Tr_H as a linear transformation.

9.12 (a) Use **T.5.4, T.??** and **T.9.1**(d).

(b) Use Ex. 2.12.

(c) $\mathrm{Nr}_{L/K}(x) = x^{\frac{q^n-1}{q-1}}$, where $n = [L : K]$. The mapping $\mathrm{Nr}_{L/K} : L^* \to K^*$ is a group homomorphism. How many elements belongs its kernel?

9.13 Use Ex. 9.12(b) and **T. 9.2**. For example, $\beta = \alpha^2 + \alpha$ (or $\alpha^2 + \alpha + 1$).

9.14 (a) Use Ex. 7.6, Ex. 8.16 and **T.9.1**(d).

(b) Consider a natural homomorphism mapping an automorphism $\sigma \in G(M_1M_2/M_2)$ onto its restriction to M_1. What is the image and the kernel of this homomorphism?

(c) Consider the homomorphism $\varphi : G(M_1M_2/K) \to G(M_1/K) \times G(M_2/K)$, where $\varphi(\sigma) = (\sigma|_{M_1}, \sigma|_{M_2})$. Show that $\mathrm{Ker}\ \varphi = \{e\}$. Then compute the orders of $G(M_1M_2/K)$ and $G(M_1/K) \times G(M_2/K)$ using **T.9.1**(a) and Ex. 7.7.

(d) Use Ex. 7.4(b).

9.15 In each case below, we give an example of a field (chosen among plenty of other possibilities).

(a) $\mathbb{Q}(i)$; (b) $\mathbb{Q}(\alpha)$, $\alpha = \varepsilon + \frac{1}{\varepsilon}$, $\varepsilon = e^{\frac{2\pi i}{7}}$; (c) Ex. 9.2(c);
(d) $\mathbb{Q}(\alpha)$, $\alpha = \varepsilon + \frac{1}{\varepsilon}$, $\varepsilon = e^{\frac{2\pi i}{11}}$; (e) Ex. 9.2(a); (f) $\mathbb{Q}(i, \varepsilon)$, $\varepsilon = e^{\frac{2\pi i}{5}}$;
(g) $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$; (h) $\mathbb{Q}(\alpha, \beta)$, $\alpha^3 = 3\alpha + 1$, $\beta^3 = 7\beta + 7$;
(i) Ex. 9.5(c); (j) Ex. 9.2(f);
(k) $L = K_f$, $f(X) = X^4 - 2X - 2$; (l) $L = K_f$, $f(X) = X^3 + 20X + 16$.

9.16 Use Dirichlet's theorem: For every natural number n, there exists a natural number k such that $nk + 1$ is a prime number. See also Ex. 10.12.

9.17 No. Try to find your own counterexample – it may be interesting.

9.18 $G(L/M_1M_2) = H_1 \cap H_2$ (motivate that each $\sigma \in G(L/M_1M_2)$ must be in both $H_1 = G(L/M_1)$ and $H_2 = G(L/M_2)$, as well as, conversely); $G(L/M_1 \cap M_2) =$ the least subgroup of $G(L/K)$ containing both H_1 and H_2 (that is, the group of all finite products in which every factor belongs either to H_1 or to H_2).

This answer can be also expressed in the following way: $M_1 = L^{H_1}, M_2 = L^{H_2}$ gives $L^{H_1 \cap H_2} = L^{H_1}L^{H_2}$ and $L^{\langle H_1, H_2\rangle} = L^{H_1} \cap L^{H_2}$, where $\langle H_1, H_2\rangle$ denotes the least subgroup of $G = G(L/K)$ containing both H_1 and H_2.

9.19 Show that $K(\alpha) \supseteq K$ is a Galois extension.

9.20 Follow similar argument as in the solution of Ex. 9.14(b).

9.21 What happens when you take the complex conjugation of a number in L?

9.22 Use **T.9.1**(a) and Ex. 9.10(a).

9.23 (a) Every permutations of the zeros is a composition of inversions (of only two zeros). What happens with the sign of $\alpha_i - \alpha_j$ when they are shifted? Even permutation is a composition of an even number of inversions, and an odd needs an odd number of inversions.

(b) Show that the index of $\mathrm{Gal}_0(L/K)$ in $\mathrm{Gal}(L/K)$ is 1 or 2 and the second possibility occurs if and only if $\sqrt{\delta(f)} \notin K$.

9.24 Let $\alpha_i = \alpha + i$ for $i = 0, 1, \ldots, i-1$. Let $f_i(X)$ be the minimal polynomial of α_i over K. Notice that $K(\alpha_i) = K(\alpha)$ for each $i = 0, 1, \ldots, p-1$.

9.25 Ex. 7.11(a): If $a_1 = a$ is a zero of $f(X)$, then the remaining are $a_2 = 2-a^2$, $a_3 = a^3-3a$, $a_4 = a^4 - a^3 - 3a^2 + 2a$, $a_5 = -(a^4 - 4a^2 + 2)$. The Galois group is cyclic of order 5 and is generated by $\sigma(a) = 2 - a^2$.

Ex.7.11(c): If a is a zero of $f(X)$, then the remaining zeros can be obtained from the factorization of $f(X)$ over the field $\mathbb{Q}(a)$ (using `>factor(f(X),a)`). Since the Galois group has order 7, it is cyclic and generated by any σ mapping a onto another zero (different from a) of $f(X)$.

Ex.7.11(d): If $a_1 = a$ is a zero of $f(X)$, then the remaining zeros are $a_2 = -a$, $a_{3,4} = \pm\frac{1}{6}(-252a + 468a^3 - 215a^5 + 3a^7)$, $a_{5,6} = \pm\frac{1}{24}(-552a + 1566a^3 - 1064a^5 + 15a^7)$, $a_{7,8} = \pm\frac{1}{24}(-1212a+3294a^3-1922a^5+27a^7)$. The automorphisms are functions fi defined by mapping a onto one of the 8 zeros (for example, `>f3:= a -> a_3` where a_3 is given as a function of a). Then we can check the orders of fi in the Galois group computing `>simplify(fi(fi(a))`. We get that $fi(fi(a) = -a$ for all $i \neq 1, 2$, so all elements in the Galois group with the exception of the identity and the automorphism mapping a onto $-a$ have order 4 (the involution mapping a onto $-a$ has order 2). This shows that the Galois group is the quaternion group (see Ex. 12.1(e)).

9.26 (a) The zeros of the polynomial are $a, a^2 - 2, 2 - a - a^2$, so $K = \mathbb{Q}(a)$. The Galois group is cyclic of order 3 and $G(K/\mathbb{Q}) = \langle\sigma\rangle$, where $\sigma(a) = a^2 - 2$.

(b) The zeros of the polynomial are $a, -a^2, -a^4, a^5, a-a^4, a^2-a^5$, so $K = \mathbb{Q}(a)$. The Galois group is cyclic of order 6 and $G(K/\mathbb{Q}) = \langle\sigma\rangle$, where $\sigma(a) = a^5$ (define `>σ:=a->a^5` and check the order of σ in the group using `>simplify(σ(σ(a)))` and `>simplify(σ(σ(σ(a))))`. You see that the order is not 2 or 3, so it must be 6).

(c) The zeros of the polynomial are $a, -\frac{1}{9}(9 - 12a^2 + a^5)$, $\frac{1}{3}(6 + 4a^3 + 2a^4 + a^5)$, $\frac{1}{9}(27 + 9a - 12a^2+12a^3+6a^4+4a^5$, $-\frac{1}{9}(45+9a-6a^2+18a^3+9a^4+5a^5)$, $-\frac{1}{9}(18+9a+6a^2+6a^3+3a^4+a^5)$. The Galois group of order 6 is S_3 and $G(K/\mathbb{Q}) = \langle\sigma, \tau\rangle$, where $\sigma(a) = \frac{1}{3}(6 + 4a^3 + 2a^4 + a^5)$ is of order 2, $\tau(a) = -\frac{1}{9}(9 - 12a^2 + a^5)$ is of order 3 and $\sigma\tau = \tau^2\sigma$ (check it defining the corresponding functions σ, τ in Maple like in (b)).

9.27 Use the command `>galois(f(X))`.

(a) The Galois group D_5 (dihedral of order 10 - see Ex. 12.1) and the minimal number of zeros generating the splitting field is 2.

(b) The Galois group A_5 (alternating of order 60) and the minimal number of zeros generating the splitting field is 3.

(c) The Galois group S_5 (symmetric of order 60) and the minimal number of zeros generating the splitting field is 4.

You may use Maple in order to adjoint zeros and check how the given polynomials split in the subsequent extensions but it is much more elegant to deduce the minimal number of zeros generating the splitting fields using the knowledge of the order of the Galois groups.

Problems of Chapter 10

10.1 $\Phi_1(X) = X-1$; $\Phi_2(X) = X+1$; $\Phi_3(X) = X^2+X+1$; $\Phi_4(X) = X^2+1$; $\Phi_5(X) = X^4+X^3+X^2+X+1$; $\Phi_6(X) = X^2-X+1$; $\Phi_7(X) = X^6+X^5+X^4+X^3+X^2+X+1$; $\Phi_8(X) = X^4+1$; $\Phi_9(X) = X^6+X^3+1$; $\Phi_{10}(X) = X^4-X^3+X^2-X+1$.

10.2 (a) $\Phi_p = (X^p-1)/(X-1)$.

(b) It is a special case of Ex. 10.3(a) for $k = r(n)$.

(c) It is a special case of Ex. 10.3(b) for $r = p, s = n$.

$\Phi_{20}(X) = 1 - X^2 + X^4 - X^6 + X^8$,

$\Phi_{105}(X) = 1+X+X^2-X^6-X^5-X^8-2\,X^{41}-X^{42}-X^{43}+X^{46}+X^{47}+X^{48}-2\,X^7-X^9+X^{12}+X^{13}+X^{14}+X^{15}+X^{16}+X^{17}-X^{20}-X^{22}-X^{24}-X^{26}-X^{28}+X^{31}+X^{32}+X^{33}+X^{34}+X^{35}+X^{36}-X^{39}-X^{40}$.

10.3 (a) Let ε_r for $r = 1, \ldots, \varphi(k)$ be all primitive k-th roots of 1 and let $d = n/k$. Show that all d-th roots of ε_r give all primitive n-th roots of 1 (notice that $\varphi(n) = d\varphi(k)$ depending on the assumption on primes dividing n and k).

(b) Use the formula expressing the cyclotomic polynomials by binomials X^d-1 in **T.10.2(a)**.

10.4 Notice that if $m > 1$ is odd and ε is a primitive m-th root of 1, then $-\varepsilon$ is a primitive $2m$-th root of 1.

10.5 (a) Use Ex. 9.14(b).

(b) Look at the degree of $\mathbb{Q}(\varepsilon_m)\mathbb{Q}(\varepsilon_n)$ over $\mathbb{Q}(\varepsilon_m)$ using (a), Ex. 9.14(b), **T.9.1** and **T.4.1**.

(c) $\mathbb{Q}(\varepsilon_m)\mathbb{Q}(\varepsilon_n) = \mathbb{Q}(\varepsilon_{[m,n]})$ and $\mathbb{Q}(\varepsilon_m) \cap \mathbb{Q}(\varepsilon_n) = \mathbb{Q}(\varepsilon_{(m,n)})$, where $[m,n]$ is the least common multiple and (m,n) the greatest common divisor of m and n.

10.6 Use Ex. 9.21. One can choose $\eta = \varepsilon_n + \overline{\varepsilon_n}$ (notice that $\overline{\varepsilon_n} = 1/\varepsilon_n$).

10.7 (a) Use Ex. 5.8(a).

(b) Use T.9.2 taking into account that the Galois group is cyclic (see **A.4.2**).

(c) Find the number of different images of θ_d by all automorphisms of $G(K/\mathbb{Q})$. Use Ex. 9.22.

10.8 (a) $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{-2})$; (b) $\mathbb{Q}(\sqrt{5})$; (c) $\mathbb{Q}(\sqrt{-7})$.

10.9 (a) $\sigma(\varepsilon)=\varepsilon^2$ has order 4, $G_2=\langle\sigma^2\rangle$, $K^{G_2}=\mathbb{Q}(\theta_2)=\mathbb{Q}(\sqrt{5})$, $\theta_2=\varepsilon_5+\sigma^2(\varepsilon_5)=\varepsilon_5+\varepsilon_5^4$ has minimal polynomial X^2+X-2;

(b) $\sigma(\varepsilon_7)=\varepsilon_7^3$ has order 6,

$G_2=\langle\sigma^3\rangle$, $K^{G_2}=\mathbb{Q}(\theta_3)$, $\theta_3=\varepsilon_7+\sigma^3(\varepsilon_7)=\varepsilon_7+\varepsilon_7^6$ has the minimal polynomial $X^3+X^2-2\,X-1$;

$G_3=\langle\sigma^2\rangle$, $K^{G_3}=\mathbb{Q}(\theta_2)=\mathbb{Q}(\sqrt{-7})$, $\theta_2=\varepsilon_7+\sigma^2(\varepsilon_7)+\sigma^4(\varepsilon_7)=\varepsilon_7+\varepsilon_7^2+\varepsilon_7^4$ has the minimal polynomial X^2+X+2.

(c) $\sigma(\varepsilon_{17})=\varepsilon_{17}^3$ has order 16,

$G_2=\langle\sigma^8\rangle$, $K^{G_2}=\mathbb{Q}(\theta_8)$, $\theta_8=\varepsilon_{17}+\sigma^8(\varepsilon_{17})=\varepsilon_{17}+\varepsilon_{17}^{16}$ has the minimal polynomial $X^8+X^7-7X^6-6X^5+15X^4+10X^3-10X^2-4X+1$.

$G_4=\langle\sigma^4\rangle$, $K^{G_6}=\mathbb{Q}(\theta_4)$, $\theta_4=\sum_0^3\sigma^{4i}(\varepsilon_{17})=\varepsilon_{17}+\varepsilon_{17}^{3^4}+\varepsilon_{17}^{3^8}+\varepsilon_{17}^{3^{12}}$ has the minimal polynomial $X^4+X^3-6\,X^2-X+1$,

$G_8=\langle\sigma^2\rangle$, $K^{G_8}=\mathbb{Q}(\theta_2)$, $\theta_2=\sum_0^7\sigma^{2i}(\varepsilon_{17})=\varepsilon_{17}+\varepsilon_{17}^{3^2}+\varepsilon_{17}^{3^4}+\varepsilon_{17}^{3^6}+\varepsilon_{17}^{3^8}+\varepsilon_{17}^{3^{10}}+\varepsilon_{17}^{3^{12}}+\varepsilon_{17}^{3^{14}}$ has the minimal polynomial X^2+X-4,

10.10 Use Ex. 10.7(c) for $\theta_2=\sum_{i=1}^{\frac{p-1}{2}}\sigma^{2i}(\varepsilon)=\sum_{i=1}^{\frac{p-1}{2}}\varepsilon^{g^{2i}}$, where σ is a generator of the Galois group $G(\mathbb{Q}(\varepsilon)/\mathbb{Q})$ and ε a p-th root of 1 ($\varepsilon\neq 1$). Define $\theta_2'=\sum_{j=0}^{\frac{p-3}{2}}\sigma^{2j+1}(\varepsilon)=\sum_{j=0}^{\frac{p-3}{2}}\varepsilon^{g^{2j+1}}$. Compute $\theta_2\theta_2'$ and consider in the product all the terms such that $g^{2i}+g^{2j-1}$ (mod p) has a fixed value. These values are given by the values of the quadratic form X^2+gY^2 over the field $\mathbb{F}_p$. Motivate that for $p=1$ (mod 4) this quadratic form does not represent 0 (that is, the only solution of the equation $X^2+gY^2=0$ is $X=Y=0$ (mod)) and each nonzero value in $\mathbb{F}_p$ is represented in $p+1$ different ways. Count the number of possibilities for X^2 and $Y\neq 0$ ($X=g^i, Y=g^j$). Show that for $p=3$ (mod 4), the quadratic form represents 0 in $(p-1)/2$ different ways with $XY\neq 0$, and every nonzero element in $\mathbb{F}_p$ in $(p-3)/2$ different ways. Show that θ_2 has the minimal polynomial $X^2+X-\frac{p-1}{4}$, when $p=1$ (mod 4) and $X^2+X+\frac{p+1}{4}$, when $p=3$ (mod 4).

10.11 (a1) $X^6+X^5+X^4+X^3+X^2+X+1=(X^3+X+1)(X^3+X^2+1)$;

(a2) $X^6+6X^3+8=(X^3+2)(X^3+4)$;

(a3) $X^{12}+2\,X^{11}+X^{10}+2\,X^9+X^8+2\,X^7+X^6+2\,X^5+X^4+2\,X^3+X^2+2\,X+1=(X^3+2X+1)(X^3+2X^2+1)(X^3+X^2+2X+1)(X^3+2X^2+X+1)$.

(b) Let ε be a primitive n-th root of 1 over $\mathbb{F}_p$ and let k be the degree of the field $\mathbb{F}_p(\varepsilon)$ over $\mathbb{F}_p$. What is a relation between n and k?

10.12 (a) Use **T.10.2**(a) and show that $X^n - 1$ has a double zero x.

(b) What can be said about the order k of x in the group $\mathbb{Z}_p^*$? What is its relation to n? Consider the cases $k = n$ and $k < n$ and use (a).

(c) Use induction starting from Ex. 10.2(a), and to the inductive step Ex. 10.3(a).

(d) Assume that the number of primes congruent to 1 modulo n is finite and consider their product with n. Take a prime p which divides $\Phi_n(N^k)$ for a sufficiently big k and show that it must be congruent 1 modulo n using (b).

10.13 (a) G is a product of cyclic groups of some orders $n_1, \ldots, n_r$. For every order n_i, we can find a prime number $p_i = n_i k_i + 1$, where k_i is an integer (this is a special case of Dirichlet's theorem on primes in arithmetical progressions – see Ex. 10.12) and we can choose k_i, so that all p_i are different. We have a surjection of $\mathbb{Z}_{p_i}^*$ onto $\mathbb{Z}_{n_i}$ and hence, a surjection of $\mathbb{Z}_{p_1}^* \times \cdots \times \mathbb{Z}_{p_r}^* = \mathbb{Z}_{p_1 \ldots p_r}^*$ onto $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$.

(b) Use (a) and **T.9.3**(b).

10.14 (a) Consider a tower $K \subseteq K(\varepsilon) \subseteq K(\varepsilon, \alpha)$, where $\varepsilon^n = 1$, $K(\varepsilon)$ is a splitting field of $X^n - 1$ and $\alpha^n = a$. The maximal order of $G(L/K)$ is $n\varphi(n)$, where φ is the Euler function (see p. 256).

(b) Let $\sigma \in G(L/K)$ and let $\sigma(\varepsilon) = \varepsilon^a$, $a \in \mathbb{Z}_n^*$ and $\sigma(\alpha) = \varepsilon^b \alpha$, $b \in \mathbb{Z}_n$. Map σ onto the matrix $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$.

(c) If $X^p - a$, where $a \in \mathbb{Q}$, is irreducible over $\mathbb{Q}$ then the Galois group is isomorphic to the group of all matrices as in (b), where $a \in \mathbb{Z}_p^*$ and $b \in \mathbb{Z}_p$, so its order is $p(p-1)$. For $p = 2$, we have a cyclic group of order 2, for $p = 3$, the group of order 6 isomorphic to S_3 and for $p = 5$, the group of order 20 (usually denoted by $GA(1, 5)$ as a special case of the **general affine groups** $GA(1, p)$ given by the matrices in (b)).

(d) The Galois group is a cyclic group of order n.

10.15 (a) What is the m-th power of a primitive $2m$-th root of 1?

(b) Take a primitive m-th root of 1 and find a zero of the second polynomial.

10.16 (a) 4; (b) 8; (c) 6; (d) 12;
(e) 12; (f) 8; (g) 16; (h) 16;

10.17 The first coefficient with absolute value bigger than 1 appears for $n = 105 = 3 \cdot 5 \cdot 7$. The number 105 is the least one having 3 different odd prime factors. The formulae for $\Phi_{n,\mathbb{Q}}(X)$ say that the size of the coefficients depends on the number of different primes dividing n (see Ex. 10.2(b)). But it is not true that 3 different factors of n imply that there

are coefficients with absolute value bigger than 1. For example, the coefficients of $\Phi_{n,\mathbb{Q}}(X)$ for $n = 231 = 3 \cdot 7 \cdot 11$ are all of absolute value at most 1. However, it is a not bad guess, since it is possible to prove that n with only two odd prime factors give polynomials with coefficients of absolute value at most 1 (see Ex. 10.2(b) and Ex. 10.4). It is known that for sufficiently big n, the coefficients can be arbitrarily large (check in the Wikipedia).

10.18 (a) Motivate that the splitting field of $X^6 - a$ has at most degree 12 over $\mathbb{Q}$. When it is less than 12? Answer: $a = -3b^2$ for an integer $b \neq 0$. Motivate that this happens if and only if $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{-3})$, which is (the quadratic subfield of) the cyclotomic field $\mathbb{Q}(\varepsilon_6)$.

(b) The Galois group of an irreducible binomial $X^7 - a$ has always order 42. For an irreducible binomial $X^8 - a$, the order of the Galois group is at most 32. It is always divisible by 8 (why?) and, in fact, may be 8 or 16, but usually is 32. The exceptional cases appear when $a = -b^2$ (8) or $a = \pm 2b^2$ (16) for an integer $b \neq 0$. This may be obtained experimentally using Maple (and supplemented by a proof) or deduced from the properties of cyclotomic extensions (see Ex. 10.14). For irreducible binomials $X^9 - a$, the order of the Galois group is always 54. In fact, if the polynomial $X^9 - a$ is reducible over the field $M = \mathbb{Q}(\varepsilon_9)$, where ε_9 is a primitive 9-th root of 1, then $a = b^3$, where $b \in M$ by Capelli's theorem (see Ex. 5.11). Then $X^3 - a$ which is irreducible over $\mathbb{Q}$ (since $X^9 - a$ is irreducible) has a zero b in M. So the splitting field of $X^3 - a$ is contained in M, which is a contradiction, since $G(M/\mathbb{Q})$ is an abelian group, while the Galois group of $X^3 - a$ is S_3. Thus $\mathbb{Q}(\varepsilon_6, \sqrt[9]{a})$ has degree 54 over $\mathbb{Q}$.

Problems of Chapter 11

11.1 (a) $G(\mathbb{Q}(i)/\mathbb{Q}) = \{\sigma_0, \sigma_1\}$, where $\sigma_0(i) = i$,$\sigma_1(i) = -i$. A normal basis: $\sigma_0(\alpha) = 1 + i, \sigma_1(\alpha) = 1 - i$, where $\alpha = 1 + i$.

(b) $G(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}$, where

G	$\sqrt{2}$	$\sqrt{3}$
σ_0	$\sqrt{2}$	$\sqrt{3}$
σ_1	$-\sqrt{2}$	$\sqrt{3}$
σ_2	$\sqrt{2}$	$-\sqrt{3}$
σ_3	$-\sqrt{2}$	$-\sqrt{3}$

A normal basis: $\sigma_0(\alpha) = 1 + \sqrt{2} + \sqrt{3} + \sqrt{6}, \sigma_1(\alpha) = 1 - \sqrt{2} + \sqrt{3} - \sqrt{6}, \sigma_2(\alpha) = 1 + \sqrt{2} - \sqrt{3} - \sqrt{6}, \sigma_3(\alpha) = 1 - \sqrt{2} - \sqrt{3} + \sqrt{6}$, where $\alpha = 1 + \sqrt{2} + \sqrt{3} + \sqrt{6}$.

(c) $G(\mathbb{Q}(\varepsilon)/\mathbb{Q}) = \langle\sigma\rangle$, where $\sigma(\varepsilon) = \varepsilon^2$. A normal basis: $\sigma^0(\alpha) = \varepsilon, \sigma(\alpha) = \varepsilon^2, \sigma^2(\alpha) = \varepsilon^4, \sigma^3(\alpha) = \varepsilon^3$, where $\alpha = \varepsilon$.

(d) $G(\mathbb{F}_2(\gamma)/\mathbb{F}_2) = \langle\sigma\rangle$, where $\sigma(\gamma) = \gamma^2$. A normal basis: $\sigma^0(\alpha) = \gamma, \sigma(\alpha) = \gamma^2, \sigma^2(\alpha) = \gamma^4 = \gamma^2 + \gamma + 1$, where $\alpha = \gamma$

11.2 (a) Let σ be the nontrivial automorphism of L over K. If $\alpha \notin K$, then $L = K(\alpha)$. Let $\beta = \sigma(\alpha) = p - \alpha$, where $\alpha^2 = p\alpha + q$. When α, β form a basis of L over K?

(b) Let $L = K(\alpha)$ and let σ be a generator of the Galois group $G(L/K)$. Denote $\beta = \sigma(\alpha)$ and $\gamma = \sigma(\beta)$. Notice that $\sigma^3 = 1$ so $\sigma(\gamma) = \alpha$. When α, β, γ form a basis of L over K? You may use **L.11.1** on p. 112.

11.3 (a) Use Ex. 9.22. The converse is not true – find a suitable example.

(b) In both cases the answer is "no". Try to construct suitable examples using finite fields.

11.6 (a) Use **T.11.3** for $K = E = \mathbb{Q}(\varepsilon)$ and $n = 3$. Notice that $E = \mathbb{Q}(\sqrt{-3})$ is the quotient field of $\mathbb{Z}[\varepsilon]$ and any α can be replaced by $r^2\alpha$, where $r \in \mathbb{Z}[\varepsilon]$.

(b) Use Ex. 9.14, **T.9.2** and the fact that the cyclic group $\mathbb{Z}_2 \times \mathbb{Z}_3 = \mathbb{Z}_6$ has exactly one subgroup of order 3.

(c) Use **T.11.4** for $n = 3$.

(d) Use (19.1). Examples: the splitting fields of $X^3 - 3X + 1$ ($f = 1 + \varepsilon$), $X^3 - 7X + 7$ ($\varepsilon = 2 + 2\varepsilon$), $X^3 - 13X + 13$ ($f = 4 + 3\varepsilon$).

11.7 (a) Use **T.11.3** for $K = E = \mathbb{Q}(i)$ and $n = 4$. Notice that $E = \mathbb{Q}(i)$ is the quotient field of $\mathbb{Z}[i]$ and any α can be replaced by $r^2\alpha$, where $r \in \mathbb{Z}[i]$.

(b) Use Ex. 9.14, **T.9.2** and the fact that the group $G = \mathbb{Z}_2 \times \mathbb{Z}_4$ has exactly two subgroups H of order 2 such that G/H is cyclic (of course, of order 4). Consider the fixed subfields corresponding to these two subgroups.

(c) Use **T.11.4** for $n = 4$.

(d) Use (c) and check that the automorphism, which maps $\sqrt[4]{\alpha}$ onto $\sqrt[4]{\overline{\alpha}}$ has order 2. Take its fixed field. It is possible to show directly that the Galois group of this field is cyclic of order 4. The minimal polynomial of γ is $X^4 - 4\mathrm{Nr}(f)gX^2 + \mathrm{Nr}(f)g^2[4\mathrm{Nr}(f) - \mathrm{Tr}(f)^2]$. Examples: the splitting fields of $X^4 + 8X^2 + 8$ ($f = -(1 + i), g = -1$), $X^4 - 10X^2 + 20$ ($f = 1 + 2i, g = 2$), $X^4 - 52X^2 + 468$ ($f = 2 + 3i, g = 1$).

11.8 Use **T.11.2**(b) and Ex. 9.22.

11.9 By Ex. 8.3(d), we know that L is a Galois extension of K. Let q be a prime dividing the order of the Galois group $G(L/K)$. Assume that $[L : K] = q$ and consider two cases: $\mathrm{char}(K) \neq q$ and $\mathrm{char}(K) = q$ (in the first case the characteristic of K may be 0). In the first case show that all q-th roots of 1 are in K. Thereafter use **T.11.3** and show that $L = K(\alpha)$, where $\alpha^q = a \in K$. Take $\beta \in K$ such that $\beta^q = \alpha$ and take the norms to K of the two sides (see (6.1)). This gives a contradictions unless $q = 2$.

In the second case, use Ex. 11.8 to show that $L = K(\alpha)$, where $\alpha^q - \alpha = a \in K$. Take $\beta \in K$ such that $\beta^q - \beta = a\alpha^{q-1}$ in order to find a contradiction to the fact that $\alpha \notin K$.

Finally consider the case when the order of $G(L/K)$ is a power of 2 and consider what happens if i (a solution of $X^2+1=0$ in L) belongs to K.

Problems of Chapter 12

12.1 (b) Consider the chain $G = G_0 = S_3 \supset G_1 = \langle\sigma\rangle \supset G_2 = \langle I\rangle$, where σ is an element of order 3 (any nontrivial rotation) and I the identity.

(c) Consider the chain $G = G_0 = S_4 \supset G_1 = A_4 \supset G_2 = V_4 \supset G_4 = \langle I\rangle$, where A_4 is the group of even permutations of $1,2,3,4$ (the group of the rotations of a regular tetrahedron), V_4 is the subgroup of permutations of order at most 2 in A_4 (it consists of $(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)$ and is Klein's four group) and I is identity.

(d) Consider the chain $G_0 = D_n \supset G_1 = C_n \supset \langle I\rangle$, where C_n is the group of all rotations of the regular polygon with n sides and I is the identity.

(e) Consider the chain $G_0 = \mathbb{H}^*(\mathbb{Z}) \supset G_1 = \langle -1\rangle \supset G_2 = \langle 1\rangle$.

12.2 (c) The group A_n is normal in S_n as a subgroup of index 2. Use (b) and **T.12.1**.

12.3 (a) Among all possible chains $G = G_0 \supset G_1 \supset \ldots \supset G_n = \{e\}$ consider a chain with maximal possible value of n. Motivate that then all the quotients G_i/G_{i+1} are cyclic of prime order. Use **A.2.10** and **A.2.8**.

(b) Use (a).

12.4 (a) Motivate that the functions $\varphi_{a,b}(x)$ are bijections on the set $\{0,1,\ldots,n-1\}$ and as such can be considered as permutations belonging to the group S_n of all permutations of this set (with n elements).

Notice that different $x \in \{0,1,\ldots,n-1\}$ have different images $\varphi_{a,b}(x)$, so $\varphi_{a,b}(x)$ is bijective on the set $\{0,1,\ldots,n-1\}$.

(b) The number of functions $\varphi_{a,b}(x)$ is $n\varphi(n)$. Show that $\varphi_{a,b} \circ \varphi_{c,d} = \varphi_{ac,ad+b}(x)$ and $\gcd(ac,n) = 1$. Use **A.2.1**.

(c) Check that Φ is a group homomorphism (use (b)) and find its kernel $\mathcal{T}_n$. Notice that $\mathcal{T}_n$ is abelian. Use **T.12.1**(c) for $G = \mathcal{G}_n$ and $N = \mathcal{T}_n$.

(d) Notice that already the subgroup $\mathcal{T}_n$ of all translations $\varphi_{1,b}(x) = x + b$ acts transitively on $\{0,1,\ldots,p-1\}$. How many solutions has equation $\varphi_{a,b}(x) = x$ when a, b are fixed?

(e) Let $\varphi_{a,b}(x)$ be a function of order p. Show that $a = 1$, so $\varphi_{a,b}(x) \in \mathcal{T}_p$. Use (b) above.

(f) Denote by $\mathcal{M}$ the group of the matrices in (d) and show that $\Psi : \mathcal{G}_n \to \mathcal{M}$ such that $\Psi(\varphi_{a,b}) = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$, is a group isomorphism.

12.5 (d) Look at the fix group G_x of any element $x \in X$ and use the formula $|X||G_x| = |G|$ (see **A.8.2**(a)).

(e) If H is a subgroup of a transitive group G on a set X with p elements, then H is also transitive on X or every element of H acts as the identity on X.

(e) Show that if $x, x' \in X$ and $gx = x'$ for some $g \in G$, then $H_{x'} = gH_xg^{-1}$. Conclude that two arbitrary orbits Hx and Hx' for $x, x' \in X$ have the same number of elements. Use **A.8.2** (on $|Hx| = |H|/|H_x|$).

12.6 Show that the center of a $p-$group, is always nontrivial. Consider the action of G on the set $X = G$ by conjugation, that is, for $g \in G$ and $x \in X$ the action of g takes x on gxg^{-1}. Notice that the fix elements for this action of G are x such that $gxg^{-1} = x$ for each $g \in G$, so $gx = xg$, that is, such x form the center $C(G)$ of G. Use formula in **A.8.2**(a) in this case.

Use the fact that G has nontrivial center together with **T.12.1** and induction with respect to the order of the group taking into account that $C(G)$ is a normal subgroup of G.

Problems of Chapter 13

13.3 Consider a longest possible chain of fields

$$K = K_0 \subset K_1 \subset \ldots \subset K_n = L$$

such that $K_i = K_{i-1}(\alpha_i)$, where $\alpha_i^{r_i} \in K_{i-1}$ and r_i are positive integers for $i = 1, \ldots, n-1$. Show that for such a chain all r_i are prime numbers (observe that the next field is really bigger than the preceding one).

13.4 (a) Denote by L a splitting field of $f(X)$ over K and consider the the Galois group $G(L/K)$ as a subgroup of S_p. Notice that the order of $G(L/K)$ is divisible by p and use Cauchy's theorem (see **A.8.3**) to prove the existence of a cycle of length p in $G(L/K)$. Show that the complex conjugation is a transposition of two zeros and use **A.9.4** to show that $G(L/K) = S_p$.

(b) Study the derivative of the polynomial $f(X)$ and plot its graph in order to show that exactly 3 zeros are real. Use (a).

13.5 For example, $X^{n-5}f(X)$, where $n \geq 5$ and $f(X) = X^5 - 4X - 2$ according to Ex. 13.4(b) for $p = 2$.

13.6 (b) Assume that the polynomial $f(X)$ is reducible over K_i. We show that it can not happen considering two possibilities: $f(X) = g(X)h(X)$ over K_i, where $\deg(g) = 2$, $\deg(h) = 3$ or $\deg(g) = 1$, $\deg(h) = 4$. Compare the degree of a splitting field M of $f(X)$

over K_{i-1} (this is 120 by Ex. 13.4(a)) with its degree resulting from the two possibilities of reducibility.

13.7 Discuss all possible Galois groups and use **T.13.1**. Alternatively, show how to solve such equations.

13.8 Compare the splitting fields of $f(X)$ and $f(X^n)$ over K. Alternatively: How to express the solutions of $f(X^n) = 0$ when the solutions of $f(X) = 0$ are known and conversely?

13.9 (a) If two of the zeros of a polynomial do not generate its splitting field, then there is an automorphism of this field having these two zeros as fix points but moving another zero by **T.9.1** and **T.9.3**.

(b) Notice that the Galois group $\mathrm{Gal}(K_f/K)$ is a transitive permutation group on the set of zeros of $f(X)$ by Ex. 7.4 and use the description of solvable groups with this property given in Ex. 12.5. Use (a).

13.10 Let K_f be a splitting field of $f(X)$ over K. What can be said about the field K_f if $f(X)$ has at least two real zeros?

13.11 (a) The discriminant of $f(X)$ is $\Delta(f) = \prod_{1\le i<j\le 5}(\alpha_i-\alpha_j)^2$, where α_i, $i = 1, 2, 3, 4, 5$ denote its zeros. Study the sign of $\Delta(f)$ depending on the cases: All α_i real, exactly three real, only one real.

(b) An example of a solvable equation with $\Delta(f) > 0$ is $f(X) = X^5 - 2 = 0$ (only one real zero). If $f(X) = X^5 + X^2 + 1$, then $f(X)$ also has only one real zero (thus $\Delta(f) > 0$), but $G(\mathbb{Q}_f/\mathbb{Q}) = S_5$ (for a proof, see Ex. 15.11(a)), so the equation $f(X) = 0$ is not solvable by radicals.

13.14 (a) Let $K = \mathbb{R}(\alpha)$, where α is a zero of an irreducible polynomial $f(X) \in \mathbb{R}[X]$ of odd degree. Use the fact that $f(X)$ has a zero in $\mathbb{R}$.

(b) Use the formula for solving of quadratic equations.

(c) Consider a Sylow 2-subgroup H of $G = G(K/\mathbb{R})$ and its fixed field K^H over $\mathbb{R}$. Use (a), and then use Ex. 12.3 in combination with (b).

Problems of Chapter 14

14.1 (a) The side of the new cube has length $\sqrt[3]{2}$. Use **T.14.1** and $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

(b) We have to construct the point $(\cos 20°, \sin 20°)$. From $\cos 3\alpha = 4\cos^3\alpha - 3\cos\alpha$, we get that $\cos 20°$ satisfies the equation $4x^3 - 3x = \frac{1}{2}$. Show that $[\mathbb{Q}(\cos 20°) : \mathbb{Q}] = 3$ and use **T.14.1**.

(c) If the construction is possible, the point $(0, \sqrt{\pi})$ can be constructed from $(0,0),(1,0)$. Motivate that $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}] = \infty$ using the fact that π is a transcendental number (see Chapter 4, p. 17 and Ex 4.16). Use **T.14.1**.

14.3 (a) Yes. The radius of the new circle is $\sqrt{r_1^2 + r_2^2}$, where r_1 and r_2 are the radii of the two given circles.

(b) Sometimes. The radius of the new sphere satisfies the equation $X^3 - r_1^3 - r_2^3 = 0$, where r_1 and r_2 are the radii of the two given spheres. For example, if $r_1 = r_2 = 1$, then a construction is impossible, but if $r_1 = 1, r_2 = \sqrt[3]{7}$, then it is possible (use **T.14.1**).

14.4 Yes. The side of the square is $x = \sqrt{\frac{1}{2}ah}$, where a is the length of a side of the triangle and h the corresponding hight – both a and h are given.

14.5 No. The volume of a regular tetrahedron with side a is equal $\frac{a^3\sqrt{2}}{12}$. Thus the side of the cube is $x = \frac{1}{\sqrt[6]{72}}$. Use **T.14.1**.

14.6 A regular polygon with n sides is constructible if and only if the angle $\frac{2\pi}{n}$ is constructible, which means that the point $(\cos\frac{2\pi}{n}, \sin\frac{2\pi}{n})$ is constructible. Study the fields $L = \mathbb{Q}(\cos\frac{2\pi}{n}, \sin\frac{2\pi}{n})$ and $L(i) \supseteq \mathbb{Q}(\varepsilon)$, where ε is a primitive n-th root of 1. Use **T.14.1** and **T.14.2** as well as the fact that $[\mathbb{Q}(\varepsilon) : \mathbb{Q}] = \varphi(n)$ where φ is the Euler function (see **T.10.1**).

14.7 (a) $\cos 72° = \frac{\sqrt{5}-1}{4}$; (b) and (c): Use (a) and Ex. 14.6 (b).

14.8 (a) $1° = \frac{2\pi}{360}$ is not constructible by Ex. 14.6, since $360 = 2^3 \cdot 3^2 \cdot 5$;
(b) $3° = \frac{2\pi}{120}$ is constructible by Ex. 14.6, since $120 = 2^3 \cdot 3 \cdot 5$;
(c) $5° = \frac{2\pi}{72}$ is not constructible by Ex. 14.6, since $72 = 2^3 \cdot 3^2$.

14.9 For example, $\alpha = \frac{2\pi}{7}$. Use Ex. 14.6 and the equality $\frac{\alpha}{3} = 2(\frac{\pi}{3} - \alpha)$.

Problems of Chapter 15

15.1 (a) Consider two cases: $f(X)$ reducible or irreducible over K. Notice that $\Delta(f) = g(\alpha_1)^2(\alpha_2 - \alpha_3)^2$, when $\alpha_1, \alpha_2, \alpha_3$ are zeros of $f(X)$ and $g(X) = f(X)/(X - \alpha_1) = (X - \alpha_2)(X - \alpha_3)$ has its coefficients in $K(\alpha_1)$. Notice also that the Galois group of an irreducible cubic equation has at least 3 and at most 6 elements (as a subgroup of S_3 – see Ex. 6.1).

(b) Motivate that $F(X_1, X_2, X_3)$ has two different images $\pm F(X_1, X_2, X_3)$ under the permutations in $G = S_3$, notice that $G_F = A_3$ and use the definition of $r_{G,F}(f)$. Apply **T.15.2**.

15.2 Motivate that $F(X_1,\dots,X_n)$ has two different images $\pm F(X_1,\dots,X_n)$ under the permutations in $G=S_n$, notice that $G_F=A_n$ and use the definition of $r_{G,F}(f)$. Apply **T.15.2**.

15.3 Consider a factorization $X^4+pX^2+qX+r=(X^2+aX+b)(X^2+a'X+b')$. Compare the coefficients on the left and on the right. How to express a,a',b,b' by p,q,r? Find a polynomial with coefficients depending on p,q,r whose zero is a^2.

15.4 (a) What are the possibilities for a in the factorization $X^4+pX^2+qX+r=(X^2+aX+b)(X^2+a'X+b')$?

15.5 (a) Check directly that the permutations in G_F do not change $F(X_1,X_2,X_3,X_4)$ and that this polynomial has exactly 3 different images under the action of the permutations in A_4 (and S_4).

(b) Use the definition $r_{G,F}(f)$ and the three different images of $F(X_1,X_2,X_3,X_4)$ in order to compute the resolvent $r_{G,F}(f)$. Use either the Vieta's formulae for the zeros $\alpha_1,\alpha_2,\alpha_3,\alpha_4$ of $f(X)$ or (a) in Ex 15.3.

15.6 Use Ex. 15.1 and Ex. 15.4 in order to study K_f through $K_{r(f)}$ (but this needs some effort, so if needed check a solution in the next chapter).

15.7 Consider a factorization $f(X)=X^4+pX^2+qX+r=(X^2-aX+b)(X^2+aX+b')$, where $a,b,b'\in K$, $\delta=a^2-4b$ and $\delta'=a^2-4b'$ are not squares in K (since otherwise, the polynomial $f(X)$ has zeros in K). Compute $r(f)$ and its zeros. Discuss two possibilities depending on $K(\sqrt{\delta})=K(\sqrt{\delta'})$ and $K(\sqrt{\delta})\neq K(\sqrt{\delta'})$.

15.8 (a) This is true for both types of resolvents discussed in Ex. 15.5. If $r(f)(T)=T^3+2pT^2+(p^2-4r)T-q^2=T^3+2pT^2+(p^2-4r)T=T(T^2+2pT+p^2-4r)$, then one zero is $T=0$ and the remaining two are $-p\pm 2\sqrt{r}$. If $r(f)(T)=T^3-pT^2-4rT+4pr-q^2=T^3-pT^2-4rT+4pr=(T-p)(T^2-4r)$, then the zeros are p and $\pm 2\sqrt{r}$. Use Ex. 15.6(a) in order to express the discriminant by the coefficients.

(b) Use directly Ex. 15.6(b).

15.9 Use Ex. 15.6 in order to construct suitable examples. For example, the Galois group of X^4+X+1 is S_4, X^4+3X+3 is D_4, X^4+5X+5 is C_4, $X^4+8X+12$ is A_4 and X^4+1 is V_4.

15.10 (a) Use **T.8.2** to represent $k'=k(\theta)$ for some θ and notice that $K'=K(\theta)$. If $[k':k]=m$, show that $1,\theta,\dots,\theta^{m-1}$ form a basis of K' over K. Map any automorphism of k' over k on the automorphism of K' over K having the same effect on θ – use Ex. 6.1.

(b) The resolvent is $r_{G,F}(f)(X)=X^2+p(Y_1+Y_2)X+(p^2-2q)Y_1Y_2+q(Y_1^2+Y_2^2)$. The resolvet is reducible if and only if its discriminant $\Delta(r_{G,F}(f))=(p^2-4q)(Y_1-Y_2)^2=0$, that is, $p^2-4q=0$ (which could be, of course, expected).

15.11 Consider reductions modulo prime numbers: (a) $2, 3, 5$; (b)$2, 3, 23$ (14 is a zero modulo 23); (c) $3, 7, 23$; (d) $3, 13, 17$ (or Eisenstein's Criterium instead of reduction modulo 3). The discriminant is $2^8 \cdot 5^6 \cdot 11^4$.

15.12 (a) Choose a prime number $p > n-2$ ($n > 2$) and three polynomials of degree n such that the first is irreducible over $\mathbb{F}_2$, the second is a product of an irreducible polynomial of degree $n-1$ by a first degree polynomial over $\mathbb{F}_3$, and the third is a product of an irreducible quadratic polynomial by $n-2$ different first degree polynomials. Use the Chinese Remainder Theorem **A.5.1** in order to show that there is a polynomial $f(X) \in \mathbb{Z}[X]$, which has the chosen polynomials as reductions modulo 2,3 and p. Use **T.15.4** and **A.9.4** in order to show that the Galois group of $f(X)$ is S_n.

(b) Follow the prescription in (a) for $n = 6, 8$.

APPENDIX: Groups, rings and fields

A.1 Equivalence relations

A relation on a set X is any subset $\mathcal{R}$ of the product $X \times X = \{(x, y)|x, y \in X\}$. For example, the relation "less or equal" on the set of real numbers is the subset $\mathcal{R} \subset \mathbb{R} \times \mathbb{R}$ consisting of all pairs (x, y) such that $x \leq y$. If we don't have any special reason to use a specific notation for a relation, we shall write $x \sim y$ when $x, y \in X$ are in a relation $\mathcal{R}$ on X, that is, $(x, y) \in \mathcal{R}$.

A.1.1 Definition. We say that a relation $\mathcal{R}$ on X is an equivalence relation if it is reflexive, symmetric and transitive, that is, if for $x, y, z \in X$, we have

(a) $x \sim x$ (reflexivity);

(b) if $x \sim y$, then $y \sim x$ (symmetry);

(c) if $x \sim y$ and $y \sim z$, then $x \sim z$ (transitivity).

An equivalence class $[x]$ of $x \in X$ with respect to an (equivalence) relation $\mathcal{R}$ is the set of all $x' \in X$, which are related to x with respect to this relation, that is, $[x] = \{x' \in X|x' \sim x\}$ (in terms of pairs, $[x] = \{x' \in X|(x', x) \in \mathcal{R}\}$). Every element belonging to an equivalence class is called its representant.

The equivalence relations play a very important role, since they split all the elements of X into equivalence classes so that every class contains elements with some special property ("relatives" to a fixed $x \in X$):

A.1.2 Proposition. *The equivalence classes of an equivalence relation on X form a partition of X, that is, every element of X belongs to an equivalence class and different equivalence classes are disjoint.*

Proof. Every element of $x \in X$ belongs to an equivalence class – its own class $[x]$. If $[x_1]$ and $[x_2]$ are two equivalence classes with a common element x, then $x_1 \sim x, x_2 \sim x$, which

implies that $x_1 \sim x_2$ by symmetry and transitivity. If now $y \in [x_1]$, then $y \sim x_1$, so $x_1 \sim x_2$ implies that $y \sim x_2$, that is, $y \in [x_2]$. In the same way, if $y \in [x_2]$, then $y \in [x_1]$. Thus $[x_1] = [x_2]$, which means that two equivalence classes with at least one common element already coincide. Hence different equivalence classes can not have any element in common, that is, they are disjoint. ♦

In general, if X is any set, then its partition is a family X_i of subsets of X (for i in an index set) which cover X (that is, $X = \bigcup X_i$) and are disjoint (that is, $X_i \cap X_j =$ if $i \neq j$). It is clear that any partition defines an equivalence relation on X, when we declare that two elements are equivalent when they are in the same subset X_i. Of course, the equivalence classes are just the sets X_i. Thus essentially, the notion of equivalence relation is exactly the same as the notion of partition.

In this book, we meet several examples of equivalence relations, so we mention here only one, which is very important.

A.1.3 Exmple. Let $X = \mathbb{Z}$ be the set of integers and let $n \neq 0$ be a fixed integer. Define $\mathcal{R}$ as the set of all pairs of integers (x, y) such that x, y give the same residue when divided by n. We check immediately that it is an equivalence relation on $\mathbb{Z}$. An equivalence class $[x]$ consists of all integers, which give the same residue when divided by n. Since there are exactly n possible residues $0, 1, \ldots, n-1$, we get that there are exactly n different equivalence classes represented by these residues. This set of equivalence classes $[0], [1], \ldots, [n-1]$ is often denoted by $\mathbb{Z}_n$ and is called the set of residues modulo n. Very often the notation $[a]$ is simplified to a with no risk of confusion, and we write $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. The set $\mathbb{Z}_n$ inherits also addition and multiplication (modulo n) from $\mathbb{Z}$, which makes it to a ring (see below in connection with the notions of the quotient group and quotient ring.

A.2 Groups

A **group** is a set G with a binary operation, which maps every pair $g_1, g_2 \in G$ onto $g_1 g_2 \in G$ in such a way that

(a) $(g_1 g_2) g_2 = g_1 (g_2 g_3)$ (associativity),

(b) there is $e \in G$ such that $eg = ge = g$ for each $g \in G$ (existence of a **unit**),

(c) for each $g \in G$ there exists $g' \in G$ such that $gg' = g'g = e$ (existence of an **inverse**).

One checks easily that in any group, there is only one unit e and for each g there is only one inverse g'. The inverse of an element $g \in G$ is denoted by g^{-1}. A group is called **abelian** if it is commutative, that is, $g_1 g_2 = g_2 g_1$ for every pair $g_1, g_2 \in G$.

The multiplicative notation of the group operation is more convenient (more compact) and it is usually used when general theory of groups is presented, but sometimes the group operation is denoted as addition and then the binary operation maps a pair $g_1, g_2 \in G$ onto $g_1 + g_2 \in G$. The associativity means then that $(g_1 + g_2) + g_3 = g_1 + (g_2 + g_3)$, the unit

(rather called zero) is usually denoted by 0, and the inverse of $g \in G$ is then called the opposite element and is denoted by $-g$.

Most of the groups considered in this text are finite, that is, G has finitely many elements. If G is finite, then its number of elements is denoted by $|G|$ and called the order of the group. If G has infinitely many elements, we often write $|G| = \infty$.

A subgroup H of G is a nonempty subset of G which also is a group when the binary operation is restricted to it. A nonempty subset H of G is a subgroup if and only if $h_1 h_2 \in H$ for each pair $h_1, h_2 \in H$ and $h^{-1} \in H$ whenever $h \in H$. In fact, the associativity holds as it holds in G and the unit element is in H as $e = hh^{-1}$ for any $h \in H$. For a finite subset of a group, the situation is a little better:

A.2.1 Proposition. *If H is a finite subset of a group G, then it is a subgroup if and only if $h_1 h_2 \in H$ whenever $h_1, h_2 \in H$.*

Proof. We have to show that $h^{-1} \in H$ when $h \in H$. All powers h^n when $n = 1, 2, \ldots$ are in H and since H is finite, they can not be all different. Thus there exists $m < n$ such that $h^m = h^n$, which gives $h^{n-m} = e$ in G. But this equality says that $h^{-1} = h^{n-m-1} \in H$. ■

If $g \in G$, then the powers of g are defined in the usual manner, that is, g^n as a product of n factors g, when $n > 0$ and of $-n$ factors g^{-1} when $n < 0$. We define $g^0 = e$. If $g_1, \ldots, g_k \in G$, then the least subgroup of G containing these elements (the intersection of all subgroups containing them) is denoted by $\langle g_1, \ldots, g_k \rangle$ and is called the subgroup of G generated by $g_1, \ldots, g_k$. It is not difficult to see that this subgroup consists of all possible products of powers $g_{i_1}^{n_1} \ldots g_{i_r}^{n_r}$, where $1 \leq i_1, \ldots, i_r \leq k$ and the exponents $n_1, \ldots, n_r$ are arbitrary integers. In particular, the group generated by one element $g \in G$ is $\langle g \rangle$ and consists of the powers g^n where n is an integer. This group is called **cyclic** (generated by g). Its order is called the **order** of g, which is denoted by $o(g)$. If $g^0 = e, g, \ldots, g^{n-1}$ are all different and g^n is equal to one of these powers, then it is easy to check that it must be e and $\langle g \rangle = \{e, g, \ldots, g^{n-1}\}$. Thus the order of g is the least positive integer n such that $g^n = e$. Notice that if $g^N = e$ and $o(g) = n$, then $n \mid N$. In fact, if $N = qn + r$, where $0 \leq r < n$, then $e = g^N = g^{qn+r} = g^r$, which implies that $r = 0$, since $r < n$.

A.2.2 *Let $G = \langle g \rangle = \{e, g, \ldots, g^{n-1}\}$, $g^n = e$, be a cyclic group of order n.*

(a) The element g^k for $0 < k < n$ is a generator of G if and only if $\gcd(k, n) = 1$, so G has $\varphi(n)$ generators, where φ is Euler's totient function *(see p. 256)**.*

(b) For every divisor d of n, the element $g^{\frac{n}{d}}$ generates a subgroup of order d and such a subgroup is unique.

Proof. (a) If g^k generates G, then there is an integer l such $(g^k)^l = g$, that is, $g^{kl-1} = e$. Since the order of g is n, we have $n \mid kl - 1$, which shows that n and k are relatively prime, that is, $\gcd(k, n) = 1$ (if d is a common divisor of n and k, then d must divide 1).

Conversely, if k and n are relatively prime, then $\gcd(k,n) = 1 = kl + nq$ for some integers l, q. Hence $(g^k)^l = g^{1-nq} = g$ as $g^n = e$. This shows that a power of g^k equals g, so the powers of g^k generate G.

(b) Let as before $G = \langle g \rangle$ and let H be a subgroup of G. Let m be the least positive power of g such that $h = g^m \in H$. If $g^M \in H$ for some integer M, then $m \mid M$, since otherwise $M = mq + r$, where $0 < r < m$ and $g^M = g^{mq+r} = g^r \in H$, which contradicts the choice of m. Thus $g^n \in H$ implies that $n = md$ and we have $H = \langle h \rangle = \{e, h, \ldots, h^{d-1}\}$, since H consists of some powers of g and all these powers have exponents divisible by m. Thus the order d of $H \subseteq G$ uniquely defines $m = n/d$ and consequently the subgroup H of G is uniquely defined by its order d. ■

Notice that the group $\mathbb{Z}_n$ with addition modulo n (see **A.1.3**) is cyclic of order n, since 1 is its generator. According to A.2.2 this group has $\varphi(n)$ generators and k is one of them if and only if $\gcd(k,n) = 1$.

Cyclic subgroups are generated by one element of the group. If A is any subset of G, then there is the least subgroup of G containing A – the intersection of all subgroups of G containing A. Such a subgroup consists of all finite products $a_1 \cdots a_k$, where each a_i or its inverse is in A. In fact, a product of two such products and the inverse of one such product keep the required type. If $A = \{a_1, \ldots, a_k\}, a_i \in G$ is a finite set, then the least subgroup of G containing A is denoted by $\langle a_1, \ldots, a_k \rangle$. If $G = \langle a_1, \ldots, a_k \rangle$, then we say that the group G is generated by $a_1, \ldots, a_k$ and these elements are called generators of G. Notice that cyclic groups are the groups with one generator. Every equality such that a product of the generators or they inverses is equal to the unity is called a relation between the generators. For example, if $G = \langle g \rangle$ is a cyclic group of order n, then $g^n = e$ is a relation for the generator g. If group is not cyclic, for example $G = S_3$, then the number of generators must be at least 2. In the case of $G = S_3$, we have $G = \langle a, b \rangle$, where $a^3 = 1$, $b^2 = 1$ and $ba = a^2b$ (that is, $a^2ba^{-1}b^{-1} = 1$), where $a = (1,2,3)$ and $b = (1,2)$ (as a, b one can choose any element of order 3 and an element of order 2). Using generators and relations between them gives a very convenient way to describe groups, which is often used in different computer packages. A group G is defined by a set of its generators $a_1, \ldots, a_k$ and relations between them if every group with some generators $b_1, \ldots, b_k$ satisfying the same relations (with a_i replaced by b_i) is isomorphic to G.

As an example consider the symmetry group of a regular polygon with n sides denoted usually by D_n ($n \geq 3$), whose order is $2n$. It consists of n rotations of the polygon and n symmetries. As for S_3 (which is D_3), we can choose two elements a, b, where the first is the rotation by the angle $\frac{2\pi}{n}$ and b is any symmetry of the polygon. Since the rotation a has order n, it generates a cyclic subgroup C_n of D_n of order n. A symmetry b has order 2 and is not in C_n, so the products a^kb for $k = 1, \ldots, n$ give n different elements (symmetries) in the group D_n. Notice that the relations defining D_n generated by a, b are $a^n = 1, b^2 = 1$ and $bab = a^k$ for some k (depending on the choice of the symmetry b – the simplest choice is $k = -1$, when the relation is $abab = 1$).

If A, B are two subsets of a group G, then AB denotes the set of all products ab, where $a \in A$ and $b \in B$. Such a product is of course associative, that is, $A(BC) = (AB)C$ for any

subsets A, B, C of G. Notice that if H is a subgroup of G, then $HH = H$. If in particular, we take $A = \{g\}$ and $B = H$ is a subgroup of G, then the product gH is called a **left coset** of H in G. Similarly, the product Hg is a **right coset** of H in G. Here follow some simple, but important properties of cosets:

Notice that if H is a subgroup of G and $g \in G$, then a coset gH may be represented in different ways, that is, we may have $gH = g'H$ for $g' \in G$ different from g. We say that g represents gH and it may happen that also g' is a representant of the same coset. This happens precisely when g' belongs to the coset of g, that is, if and only if $g' \in gH$. In fact, if $g'H = gH$, then evidently $g' = gh$ for some $h \in H$, so $g' \in gH$ and, conversely, if $g' = gh$ for some $h \in H$, then $g'H = ghH = H$, since $hH = H$ when $h \in H$. The equality $g' = gh$ for some $h \in H$ is equivalent to $g^{-1}g' \in H$. In additive notation, the equality $g + H = g' + H$ is equivalent to $g' = g + h$ for some $h \in H$ or $g' - g \in H$. Notice that (left) cosets are equivalence classes of the equivalence relation on G such that $g \sim g'$ if and only if $g^{-1}g' \in H$.

A.2.3 *Let H be a subgroup of a group G.*

(*a*) *$gH = H$ if and only if $g \in H$;*

(*b*) *If $g' \in gH$, then $g'H = gH$ (every element in a coset represents it);*

(*c*) *$g'H = gH$ if and only if $g^{-1}g' \in H$ (additively: $g + H = g' + H$ if and only if $g' - g \in H$);*

(*d*) *$g \in gH$ (every element in G belongs to a coset);*

(*e*) *If $g \in g_1H \cap g_2H$, then $g_1H = g_2H$ (two different cosets are disjoint);*

(*f*) *If H is finite, then $|gH| = |H|$ for any $g \in G$.*

(*g*) *The left (or right) cosets of H in G form a partition of the set G.*

Proof. (a) If $gH = H$, then $ge = g$ belongs to H. If $g \in H$, then $gH \subseteq H$ and, conversely, $H \subseteq gH$, since the equation $h = gx$, $h \in H$ implies $x = g^{-1}h \in H$.

(b) If $g' = gh$, $h \in H$, then $g'H = ghH = gH$ by (a).

(c) We have $g'H = gH$ if and only if $g^{-1}g'H = H$ if and only if $g^{-1}g' \in H$ by (a).

(d) We have $g = ge$, $e \in H$.

(e) If $g \in g_1H \cap g_2H$, then $g_1H = g_2H = gH$ by (b).

(f) If H is finite and $H = \{h_1, \ldots, h_m\}$, then $gH = \{gh_1, \ldots, gh_m\}$ and all products gh_i are different, since $gh_i = gh_j$ implies $h_i = h_j$ (multiply from left by g^{-1}).

(g) This is clear from (d) and (e) and means that any subgroup defines an equivalence relation on the set G by declaring two elements equivalent if and only if they belong to the same coset. ■

A.2.4 Lagrange's Theorem. *The order of a subgroup in a finite group divides its order. In particular, the order of an element in a finite group divides its order.*

Proof. Let $|G| = n$ and $|H| = m$. The group G is a union of the left cosets of H in G by **A.2.3**(d). These cosets are disjoint **A.2.3**(e) and each of them consists of m elements **A.2.3**(e). Hence $n = mi$, so m divides n. ■

The number of cosets of a subgroup H in a group G is called the index of H in G and is denoted by $[G : H]$. This number is finite when G is finite, but it may be also finite when G is infinite. For a finite group G, we have $[G : H] = |G|/|H|$ according to the argument given in the proof of Lagrange's theorem. Notice that in a finite group, the number of left cosets of a subgroup is equal to the number of its right cosets, which easily follows from Lagrange's theorem by noting that the argument in the proof works equally well for right as for left cosets. In general it is easy to construct a bijection between the sets of right and left cosets. Sometimes, we write $[G : H] = \infty$ when there are infinitely many cosets of H in G. Since usually what can be said about right cosets can be also said about the left, we shall use the term coset alone meaning either type of them, but of course fixed in any statement about them (like in the preceding statement). We prefer to use left cosets in different arguments concerning one type of them.

Sometimes the cosets of a subgroup H in a group G form a group with respect to the multiplication of subsets of G. The first condition to assure this is a property of H that the product of any two cosets $gHg'H$ is again a coset. When it happens, then this coset must be $gg'H$ (of course, $gg' \in gHg'H$, so if the product $gHg'H$ is a coset, it must be $gg'H$ by **A.2.3**). When a product of any cosets is a coset, then these cosets form a group, since multiplication of cosets is associative, the unit is the coset H and the inverse of gH is $g^{-1}H$. This group is then called the **quotient group** of G modulo H and is denoted by G/H. If G is finite, then its order is the number of cosets of H in G, that is, the index of H in G. Thus for the orders, we have $|G/H| = |G|/|H|$, which in some way motivates the terminology. The subgroups for which the above construction of the quotient group is possible are called **normal subgroups**. More exactly, we have the following characterization of normal subgroups:

A.2.5 *Each of the following equivalent conditions defines a normal subgroup H of G:*

(*a*) *The product of any two cosets of H in G is a coset*;

(*b*) *For each $g \in G$ the left and the right cosets of g coincide, that is, $gH = Hg$*;

(*c*) *For each $g \in G$, we have $g^{-1}Hg \subseteq H$.*

Proof. First, we prove that (a) implies both (b) and (c), which are equivalent. Since the product of cosets is a coset, we have $gHgH = g^2H$ (as we know, the product is the coset containing g^2, so it must be g^2H). Thus for every $h \in H$, there exists $h' \in H$ such that $ghg = g^2h'$, that is, $hg = gh'$. Hence for every $g \in H$, we have $Hg \subseteq gH$, that is, $g^{-1}Hg \subseteq H$, which is (c). Since (c) holds for any $g \in G$, we can replace g by g^{-1} and we get $gHg^{-1} \subseteq H$. Now notice that this inclusion is the same as $gH \subseteq Hg$ and $g^{-1}Hg \subseteq H$ as $Hg \subseteq gH$, so $gH = Hg$, which is (b). Thus (c) implies (b), and of course (b) implies (c).

Now (b) implies that $gHg'H = gg'HH = gg'H$, so we get (a). ■

Notice that if $g \in G$, then the mapping $x \mapsto gxg^{-1}$ for $x \in G$ is called **conjugation** by g. Using this terminology, **A.2.5**(c) says that H is a normal subgroup of G if and only if it is invariant with respect to conjugation by any element of G. The fact that H is a normal subgroup of G is often denoted by $H \lhd G$.

If H is any subgroup of a group G, then it is easy to check that $\mathcal{N}(G) = \{g \in G | gHg^{-1} \subseteq H\}$ is a group containing H in which H is of course normal by **A.2.5**(c). The group $\mathcal{N}(G)$ is called the **normaliser** of H in G and is the biggest subgroup of G in which H is normal. Of course, it may happen that $\mathcal{N}(H) = H$ or $\mathcal{N}(H) = G$ and in the last case, the subgroup H is normal in G.

In $G = \mathbb{Z}$ is the group of integers with respect to the addition, then any subgroup is the set of all multiples $\langle n \rangle$ of a fixed integer n. The quotient group $\mathbb{Z}/\langle n \rangle$ consists of the cosets $a + \langle n \rangle$ and each such coset consists of all $b = a + qn$ for integers q, that is, $b - a = qn$. Hence a coset consists of all integers giving the same residue as a when divided by n. It is possible to choose the least residue $0 \leq r < n$, that is, each coset has a representative r satisfying this restriction. Hence all cosets are $r + \langle n \rangle (= r + \mathbb{Z}n)$, where $r = 0, 1, \ldots, n-1$. In fact, the group $\mathbb{Z}/\langle n \rangle$ is simply the set of equivalence classes of the equivalence relation defined in **A.1.3** (the same as above defining the cosets modulo $\langle n \rangle$) and denoted by $\mathbb{Z}_n$.

If H is a normal subgroup of G, then we have a natural function $\iota : G \to G/H$ such that $\iota(g) = gH$ mapping any element $g \in G$ onto its coset. This function has a multiplicative property: $\iota(gg') = \iota(g)\iota(g')$, since $gg'H = gHg'H$. In general, a function $\varphi : G \to G'$ is called homomorphism if this property holds, that is, $\varphi(gg') = \varphi(g)\varphi(g')$ for any $g, g' \in G$. The homomorphism $\iota : G \to G/H$, where H is normal in G is called the natural surjection (defined by a normal subgroup H). Notice that the elements mapping on the unit of G/H, that is, on H, are those $g \in G$ for which $\iota(g) = gH = H$. The equality, $gH = H$ is equivalent to $g \in H$ (see **A.2.3**(a)), so the kernel of the natural homomorphism of G onto G/H is H.

In general, the kernel of a group homomorphism $\varphi : G \to G'$ is the set of elements in G whose image in G' is the unit element e'. The kernel is denoted by $\mathrm{Ker}(\varphi)$, that is, $\mathrm{Ker}(\varphi) = \{g \in G | \varphi(g) = e'\}$. Notice that the kernel of a homomorphism is a normal subgroup of G. In fact, if $g, g' \in \mathrm{Ker}(\varphi)$, then $\varphi(gg') = e'$, so $gg' \in \mathrm{Ker}(\varphi)$. We have also $g^{-1} \in \mathrm{Ker}(\varphi)$ if $g \in \mathrm{Ker}(\varphi)$, since $\varphi(g^{-1}) = \varphi(g)^{-1}$. The last equality follows from the fact that $\varphi(e) = e'$ (since $\varphi(e) = \varphi(ee) = \varphi(e)\varphi(e)$) and $\varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(e) = e'$, that is, $\varphi(g^{-1})$ is the inverse of $\varphi(g)$. Thus the kernel $H = \mathrm{Ker}\varphi$ of a homomorphism $\varphi : G \to G'$ is a subgroup of G. In order to check that H is normal, we have to check that $ghg^{-1} \in H$ whenever $h \in H$. This follows immediately, since $\varphi(g^{-1}hg) = \varphi(g^{-1})\varphi(h)\varphi(g) = \varphi(g^{-1})\varphi(g) = \varphi(g^{-1}g) = \varphi(e) = e'$.

A homomorphism $\varphi : G \to G'$ is injective, that is, the images of different elements are different, if and only if $\mathrm{Ker}\varphi = \langle e \rangle$. In fact, we have $\varphi(g) = \varphi(g')$ if and only if $\varphi(g'g^{-1}) = e'$, that is, $g'g^{-1} \in \mathrm{Ker}\varphi$. Hence, if $\mathrm{Ker}\varphi = \langle e \rangle$, then $g'g \in \mathrm{Ker}\varphi$ gives $g'g = e$, that is, $g' = g$ and, conversely, if the mapping φ is injective and $g \in \mathrm{Ker}\varphi$, then $\varphi(g) = e' = \varphi(e)$ gives $g = e$, that is, $\mathrm{Ker}\varphi = \langle e \rangle$. The image of the homomorphism φ, that is, $\varphi(G)$ is often denoted by $\mathrm{Im}\,\varphi$. A homomorphism $\varphi : G \to G'$ is called **isomorphism** if it is bijective, that is, it is injective ($\mathrm{Ker}\,\varphi = (e)$) and surjective ($\mathrm{Im}\,\varphi = \varphi(G) = G$). An isomorphism $\varphi : G \to G$

is called an **automorphism** of G. We have met several times the **inner automorphisms** $\varphi_g : G \to G$ defined by the elements $g \in G$ as conjugation $\varphi_g(x) = gxg^{-1}$ for $x \in G$.

The quotient group $G/\mathrm{Ker}\varphi$ is closely related to the image of G in G'. In fact, all elements in the coset gH, where $H = \mathrm{Ker}\varphi$ have the same image in G' since $\varphi(gh) = \varphi(g)\varphi(h) = \varphi(g)$. Hence we can define a function $\Phi : G/H \to G'$ mapping the whole coset gH onto $\varphi(g)$, that is, $\Phi(gH) = \varphi(g)$. It is easy to check that this function is an isomorphism from G/H to G' and its image is, of course, $\varphi(G)$. In fact, using the fact that H is normal, we have

$$\varphi(gHg'H) = \varphi(gg'H) = \varphi(gg') = \varphi(g)\varphi(g') = \varphi(gH)\varphi(g'H),$$

so Φ is a homomorphism of G/H into G'. But $\mathrm{Ker}\Phi = \{gH \in G/H | \Phi(gH) = \varphi(g) = e'\} = H$, so the kernel of Φ is the unit element of G/H. Thus Φ is injective, so it is an isomorphism of $G/\mathrm{Ker}\,\varphi$ with $\varphi(G)$. This is an important fact which is very often called the main theorem on group homomorphisms:

A.2.6 *If $\varphi : G \to G'$ is a group homomorphism, then the kernel $H = Ker\varphi$ is a normal subgroup of G and the function $\Phi(gH) = \varphi(g)$ is an injection $\varphi^* : G/Ker\varphi \to G'$. Thus φ^* is an isomorphism of the groups $G/Ker\varphi$ and $Im\varphi$. In particular, if G is finite, we have $|G| = |Ker\varphi||Im\varphi|$.*

The homomorphism φ^* in **A.2.6** is a special case of a more general context when a group homomorphism induces a homomorphism of quotient groups. Let H be a normal subgroup of G, and H' a normal subgroup of G'. We say that a group homomorphism $\varphi : G \to G'$ is a **homomorphism of pairs** if $\varphi(H) \subseteq H'$ – the pair $G \supseteq H$ is mapped into the pair $G' \supseteq H'$. The situation like this is very common and we meet it several times in Chapter 12 where we use the following very important consequence of it:

A.2.7 Group homomorphism of pairs. *Let $\varphi : G \to G'$ be a group homomorphism of the pair $G \rhd H$ into the pair $G' \rhd H'$. Then there exist an induced homomorphism*

$$\overline{\varphi} : G/H \to G'/H'$$

such that $\overline{\varphi}(gH) = \varphi(g)H'$. Moreover, we have $Ker\overline{\varphi} = \varphi^{-1}(H')/H$ and $\overline{\varphi}(G) = \varphi(G)H'/H'$.

Proof. We have only to check that the function $\overline{\varphi}$ is correctly defined, since we see immediately that if the definition is correct, then

$$\overline{\varphi}(g_1Hg_2H) = \overline{\varphi}(g_1g_2H) = \varphi(g_1g_2)H' = \varphi(g_1)\varphi(g_2)H' = \varphi(g_1)H'\varphi(g_2)H' = \overline{\varphi}(g_1H)\overline{\varphi}(g_2H).$$

In order to check the definition of $\overline{\varphi}$, we must show that if $g_1H = g_2H$, then $\overline{\varphi}(g_1)H' = \overline{\varphi}(g_2)H'$, that is, the definition is independent of the choice of a representant of a coset of H. But $g_1H = g_2H$ is equivalent to $g_1^{-1}g_2 \in H$, which implies $\varphi(g_1^{-1}g_2) \in H'$, so $\varphi(g_1)^{-1}\varphi(g_2) \in H'$, which gives $\varphi(g_1)H' = \varphi(g_2)H'$, that is, $\overline{\varphi}(g_1H) = \overline{\varphi}(g_2H)$. □

A.2.8 *Let $\varphi : G \to G'$ be a group homomorphism with kernel $N = Ker\varphi$.*

(a) The image $\varphi(H)$ of a subgroup H of G is a subgroup of G' and the inverse image $\varphi^{-1}(H')$ of any subgroup H' of G' is a subgroup of G containing N. We have $\varphi(\varphi^{-1}(H')) = H'$ and $\varphi^{-1}(\varphi(H)) = NH$. The inverse image $\varphi^{-1}(H')$ is normal in G if H' is normal in G'.

(b) If φ is surjective (so $G' \cong G/N$), then there is a one-to-one correspondence between the subgroups H' of G' and the subgroups H of G containing N in which H' corresponds to the inverse image $\varphi^{-1}(H')$ and H corresponds to its image $\varphi(H)$. In this correspondence, normal subgroups of G containing N correspond to normal subgroups of G'.

Proof. (a) If H' is a subgroup in G', then one checks easily that $\varphi^{-1}(H')$ is a subgroup of G. Of course, the group $H = \varphi^{-1}(H')$ contains N, which is the inverse image of the identity e' of G'. If H' is normal in G', then for any $g \in G$ and $h \in G$ such that $\varphi(h) \in H'$, we have $\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1} \in H'$, since H' is normal in G'. Hence $ghg^{-1} \in \varphi^{-1}(H')$, so this subgroup of G is normal.

The equality $\varphi(\varphi^{-1}(H')) = H'$ is evident (for any function between sets G, G' not just groups). In order to check the second equality $\varphi^{-1}(\varphi(H)) = HN$, take $g \in \varphi^{-1}(\varphi(H))$. Then $\varphi(g) = \varphi(h)$ for some $h \in H$, so $\varphi(gh^{-1}) = e'$. Hence, we have $gh^{-1} \in N$, which means that $g \in NH$. Conversely, if $g \in NH$, then $g = nh$ for some $n \in N, h \in H$. Thus $\varphi(g) = \varphi(nh) = \varphi(h) \in \varphi(H)$, so $g \in \varphi^{-1}(\varphi(H))$.

(b) Let $X_N(G)$ denote the set of all subgroups of G containing N, and let $X(G')$ denote the set of all subgroups of G'. We have two functions: $\Phi(H) = \varphi(H)$ mapping the subgroups of G on subgroups in G' (see (a)), and $\Psi(H') = \varphi^{-1}(H')$ mapping the subgroups in G' on subgroups in G containing N. Now $\Phi(\Psi(H')) = \varphi(\varphi^{-1}(H') = H'$ by (a), and $\Psi(\Phi(H)) = \varphi^{-1}(\varphi(H)) = NH = H$ by (a) and the assumption $N \subseteq H$, which implies that $NH = H$. Hence both compositions $\Phi \circ \Psi$ and $\Psi \circ \Phi$ give identities, so both are bijections between the corresponding sets $X_N(G)$ and $X(G')$. ■

A.2.9 *Let G be a finite abelian group. Then the exponent of G, that is, the least natural number m such that $g^m = e$ for each element $g \in G$ equals the maximal order n of the elements of G. Moreover, m divides the order of G.*

Proof. First we note that if $g, h \in G$ are elements whose orders $o(g)$ and $o(h)$ are relatively prime, then $o(gh) = o(g)o(h)$. In fact, if r is the order of gh, then $(gh)^r = e$ gives $(gh)^{ro(h)} = g^{ro(h)} = e$. Hence $o(g) \mid ro(h)$ and by the assumption, $o(g) \mid r$. Similarly, $o(h) \mid r$, so $o(g)o(h) \mid r$. Since, of course, $(gh)^{o(g)o(h)} = e$, we have $r = o(g)o(h)$.

Now let n be the maximal order of elements in G and let g be an element of that order. Assume that h is an element whose order does not divide n. Then $\mathrm{GCD}(o(h), n) = d$ and $n = da$, $o(h) = db$, where $\mathrm{GCD}(a, b) = 1$ and $b > 1$ (if $b = 1$ then the order of h divides n). The order of g^d equals a, and the order of h^d equals b, so the order of $g^d h^d$ equals ab. Thus the order of gh equals $dab = nb > n$. This is a contradiction, since n was the maximal order of the elements in G. Thus $b = 1$ and $o(h) \mid n$, so n is the exponent of G.

The last statement is clear, since the order of every element of G divides the order of this group, so in particular, the exponent divides this order. □

A.2.10 *A group G of order at least 2 has no nontrivial subgroups if and only if it is cyclic of prime order.*

Proof. If the order of G is a prime number p and H is its subgroup, then as the order of H divides p by Lagrange's theorem **A.2.4**, the order of H is 1 or p. Thus H is either the unit subgroup or the whole group G.

Now assume that G has at least one element different from the unit and no nontrivial subgroups. Take $g \in G$, $g \neq e$. The cyclic subgroup $\langle g \rangle$ of G is not nontrivial, so $G = \langle g \rangle$. If the order of g is infinite, then G contains nontrivial subgroups e.g. $\langle g^2 \rangle$. Thus the order of g is finite, say, n. If n is not a prime number, then $n = kl$, where $k > 1, l > 1$. Thus G contains a nontrivial subgroup e.g. $\langle g^k \rangle$. Hence n must be a prime number. □

A group G without nontrivial normal subgroups is called **simple**. Simple groups are in some sense building stones of all finite groups, since a group G having a nontrivial normal subgroup N can be described in terms of N and G/N (even if such a description is usually not "simple"). All simple groups were classified thanks to the efforts of many generations of mathematicians. The classification was ready about 1980 and so far the presentations of it take several thousands of pages. Those simple groups which we use are the alternate groups A_n for $n \geq 5$. Groups from **A.2.10** which do not contain any subgroups are of course simple. These are all simple abelian groups.

If G_1 and G_2 are two groups, then we can form a new group $G_1 \times G_2$, called their product, which consists of all pairs (g_1, g_2), where $g_1 \in G_1$, $g_2 \in G_2$ with coordinate-wise operation, that is, $(g_1, g_2)(g_1', g_2') = (g_1 g_1', g_2 g_2')$.

There are two groups related to a given group G, which in some sense gives a measure of non-commutativity of G. The first is the **center** $C(G)$ of G consisting of those elements of G, which commute with all elements in this group, that is, $C(G) = \{x \in G | \forall g \in G xg = gx\}$. Of course, the center is a normal subgroup of G and the group is abelian exactly when $C(G) = G$. The second group is the G' of G (denoted also by $[G, G]$. If $g_1, g_2 \in G$, then $g_1 g_2$ and $g_2 g_1$ differ by an element $c \in G$ such that $g_1 g_2 = c g_2 g_1$ (c "corrects" $g_2 g_1$ to be the same as $g_1 g_2$). Of course, we have $c = g_1 g_2 g_1^{-1} g_2^{-1}$. The element c is often denoted by $[g_1, g_2]$ and called the **commutator** of g_1, g_2. Notice that $[g_1, g_2] = e$ precisely when g_1, g_2 commute. The subgroup of G generated by all commutators of pairs $g_1, g_2 \in G$ is denoted by G' and called the **commutator group** of G. The group G' consists simply of all finite products of commutators, since inverse of a commutator is a commutator: $[g_1, g_2]^{-1} = [g_1^{-1}, g_2^{-1}]$. Notice that the group G' reduces to e if and only if all commutators are trivial, that is, the group G is abelian.

The commutator subgroup G' of G is normal. In fact, if $c = [g_1, g_2]$ is a commutator and $g \in G$, then $gcg^{-1} = [gg_1g^{-1}, gg_2g^{-1}]$ is also a commutator, so conjugation by g maps any product of commutators onto a product of commutators, so commutators are invariant with respect to conjugation.

The most important property of the commutator group G' of G is the fact that the quotient group G/G' is abelian and that every normal subgroup N of G such that G/N is abelian contains G'. This means that G/G' is the biggest abelian quotient group of G (since $N \supseteq G'$, we have an imbedding of the pair $G' \subseteq G$ into the pair $N \subseteq G$ and as a consequence an induced surjection of the quotient G/N onto the quotient G/G' (see **A.2.7**).

A.3 Rings

A ring is a set R with two operations usually called addition " $+$ " and multiplication " $\cdot$ " such that R with respect to the addition is an abelian group, multiplication is associative and addition is distributive with respect to multiplication, that is, $a(b+c) = ab + ac$ and $(b+c)a = ba + ca$ for all $a, b, c \in R$. In this text, we always assume that R is commutative, that is, $ab = ba$ for all $a, b \in R$. We say that R is a ring with identity if there exists an element $1 \in R$ such that $1a = a$ for all $a \in R$. It is easy to see that the identity 1 is unique if it exists. In the sequel, we only consider rings with identity. A **zero divisor** in a ring R is a nonzero element $a \in R$ such that $ab = 0$ for some nonzero $b \in R$. A ring without zero divisors is called **integral domain**. We will always assume that an integral domain has an identity element 1. Thus, the ring $\mathbb{Z}$ is an integral domain, whereas the rings $\mathbb{Z}_n$ of integers modulo n are integral domains only when n is a prime number (see A.1.3). For example, in $\mathbb{Z}_4 = \{0, 1, 2, 3\}$, we have $2 \cdot 2 = 0$.

A subring of a ring R is any nonempty subset R', which is also a ring with respect to the same addition and multiplication as in R. In practical terms, in order to check that a nonempty subset R' of R is a ring, it suffices to check that when $a, b \in R'$, then $a + b, ab, -a \in R'$. All other conditions in the definition of ring are automatically satisfied, since they are satisfied in R.

If a ring R is a subring of ring S and $\alpha \in S$, then $R[\alpha]$ denotes the least subring of S containing R and α. It is easy to see that it consists of all sums $r_0 + r_1\alpha + \cdots + r_n\alpha^n$, where $r_i \in R$ and n is a nonnegative integer. For example, the ring of integers $\mathbb{Z}$ is a subring of the complex numbers $\mathbb{C}$ and taking $\alpha = i$, we get the ring $\mathbb{Z}[i]$. This ring consists of all $a + bi$, where $a, b \in \mathbb{Z}$, since the equality $i^2 = -1$ makes all powers of i with exponents bigger than 1 needless.

If R is a commutative ring with identity, then an element $a \in R$ is called a **unit** (or an **invertible element**) if there exists $a' \in R$ such that $aa' = 1$. The element a' is called an inverse of a. All invertible elements form a group with respect to the multiplication in R, which is often denoted by R^*. For example, we have $\mathbb{Z}^* = \{\pm 1\}$, $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$. In the ring $\mathbb{Z}_n$ the invertible elements form the group $\mathbb{Z}_n^*$ consisting of all k such that $\gcd(k, n) = 1$. Its order is the value of Euler's function $\varphi(n)$ (see p.256). In fact, if $\gcd(k, n) = 1$, then $kx + ny = 1$ for some integers x, y, so $kx = 1$ in $\mathbb{Z}_n$, that is, k is invertible. Conversely, if k is invertible in $\mathbb{Z}_n$, then $kx = 1$ for some $x \in \mathbb{Z}_n$, so $n|kx - 1$, that is, $kx - 1 = ny$ for some $y \in \mathbb{Z}$. Hence, $\gcd(k, n) = 1$.

If R_1 and R_2 are rings, then it is possible to form a new ring $R_1 \times R_2$ consisting of pairs (r_1, r_2), where $r_1 \in R_1$ and $r_2 \in R_2$, which are added and multiplied coordinate-wise. This ring is called the product of the two rings. Of course, it is possible to extend this definition to any finite number of rings. If both rings has identity, then $(1, 1)$ is the identity of the product. For future use, observe that (r_1, r_2) is invertible if and only if r_1 and r_2 are invertible and $(R_1 \times R_2)^* = R_1^* \times R_2^*$, where on the right hand side, we have the direct product of groups.

If R, R' are rings, then a ring homomorphism is a function $\varphi : R \to R'$, which respects both addition and multiplication, that is, $\varphi(a + b) = \varphi(a) + \varphi(b)$ and $\varphi(ab) = \varphi(a)\varphi(b)$. If R, R' are rings with identity, we shall also assume that a ring homomorphism maps the identity in R onto the identity in R'. The kernel of φ is its kernel as a homomorphism of the additive group R into the additive group R', so $\mathrm{Ker}\varphi = \{a \in R | \varphi(a) = 0\}$. This set is not only a subgroup of the additive group R, but it is a subring with a stronger property: if $a \in \mathrm{Ker}\,\varphi$ and $b \in R$, then $ab \in \mathrm{Ker}\,\varphi$. In fact, if $\varphi(a) = 0$, then $\varphi(ab) = \varphi(a)\varphi(b) = 0$ for any $b \in R$. A subring I of R having this strong property for multiplication, that is, $ab \in I$ whenever at least one of the factors $a, b \in R$ is in I is called **ideal**. Thus kernels of the homomorphisms of R are ideals. In fact, every ideal is also a kernel of a homomorphism, which will be clear in a moment. Notice that $\mathrm{Ker}\,\varphi = \{0\}$ if and only if $\varphi : R \to R'$ is an injective function. In fact, if φ is injective, than $\varphi(a) = 0 = \varphi(0)$ implies that $a = 0$, that is, $\mathrm{Ker}\,\varphi = \{0\}$. Conversely, assuming the last equality, we get from $\varphi(a) = \varphi(b)$, which is the same as $\varphi(a - b) = 0$, that $a - b = 0$, that is, $a = b$. This means that φ is injective.

In the ring of integers $\mathbb{Z}$ every ideal is the set of all multiples of any fixed integer n (see **A.3.2**). Such an ideal is denoted by (n). If $n = 1$, we get the whole ring $\mathbb{Z}$ and for $n = 0$ the zero ideal (0) having only one element 0. Both these ideals are called trivial. In any ring one can fix a finite number of elements $a_1, \ldots, a_k$ and consider all sums $r_1a_1 + \cdots + r_ka_k$, where $r_1, \ldots, r_k \in R$. It is easy to check that all such sums of products form an ideal I in R. It is called the ideal generated by $a_1, \ldots, a_k$ and is denoted by $(a_1, \ldots, a_n)$. The elements $a_1, \ldots, a_k$ are called generators of I. An ideal may have many sets of generators. If there is only one generator of an ideal I, that is, $I = (a)$ for some $a \in R$, then I is called principal. We have $(a) = (b)$ if and only if $a = b\varepsilon$ and $b = a\eta$ for some $\varepsilon, \eta \in R$. If R is an integral domain and $ab \neq 0$, then these equalities imply $\varepsilon\eta = 1$. Hence ε and η are units in R. In general, two elements of a ring, which differ by a unit are called **associated**. We summarize:

A.3.1 *Two elements $a, b \in R$ in an integral domain R generate the same ideal, that is, $(a) = (b)$, if and only if they are associated. In particular, we have $(a) = R$ if and only if a is a unit.*

A ring R is called a **principal ideal ring** if every ideal in R is principal. If moreover, there are no zero divisors in R and an identity element 1, then it is called principal ideal domain (PID). The following examples of such rings are very important:

A.3.2 *The ring of integers $\mathbb{Z}$ and the polynomial rings $K[X]$, where K is a field, are principal ideal domains.*

Proof. Let I be an ideal in $\mathbb{Z}$. The zero ideal is always principal and generated by 0, so assume that I is nonzero. Let d be a nonzero integer in I with the least absolute value. If $a \in I$, we use the division algorithm and get $a = dq+r$, where $0 \leq r < |d|$. But $r = a-dq \in I$, so by the definition of d, we have $r = 0$. Hence each element of I is a multiple of d, that is, $I = (d)$ is principal.

Let now I be an ideal in $K[X]$. The zero ideal is always principal and generated by 0, so assume that I is nonzero. Let d be a nonzero polynomial in I of the least possible degree. If $f \in I$, we use the division algorithm and get $f = dq + r$, where $-1 \leq \deg r < \deg r$. But $r = a-dq \in I$, so by the definition of d, we have $r = 0$. Hence each element of I is a multiple of d, that is, $I = (d)$ is principal. ■

In any ring R it is possible to consider the notion of divisibility saying that $a \in R$ is **divisible** by $b \in R$ (notation: $b \mid a$) if there is $c \in R$ such that $a = bc$. However, such a notion has meaningful properties when R is an integral domain (there are no zero divisors in R), which we will assume when discussing divisibility. A nonzero element $a \in R$ is called **irreducible** if it is not a unit and it is not a product of two non-units. We say that a ring is a unique factorization domain (UFD) if it is an integral domain in which every nonzero element, which is not a unit can be represented uniquely as a product of irreducible elements. Uniqueness here means that if $r \in R$ and

$$(UFD) \qquad r = a_1 \cdots a_k = b_1 \cdots b_l,$$

where a_i, b_j are irreducible and $k, l \geq 1$, then $k = l$ and it is possible to order the factors in such a way that a_i and b_i are associated.

If $a, b \in R$, then we say that $d \in R$ is a **greatest common divisor** (gcd) of a, b if d divides both these elements and every common divisor of a and b divides d. If d exists, it is often denoted by (a, b) or $\gcd(a, b)$. If $ab \neq 0$ and d exists then it is defined only up to a unit in R. In fact, if d' is also a greatest common divisor of $a, b \in R$, $ab \neq 0$, then by the definition, we have $d \mid d'$ and $d' \mid d$, that is, $d' = d\varepsilon$ and $d = d'\eta$ for some $\varepsilon, \eta \in R$. Hence, we have $\varepsilon\eta = 1$, so both these factors are units in R and $(d') = (d)$.

A dual to the notion of greatest common divisor is the notion of **least common multiple** (denoted by $\mathrm{lcm}(a, b)$ or $[a, b]$ for two integers a, b). If R is an integral domain, then a least common multiple of two elements $a, b \in R$ is an element $m \in R$, which is divisible by both these elements and divides every element with this property. As for a greatest common divisor, if m exists, it is unique up to a unit.

A.3.3 *Let R be a principal ideal domain.*

(a) Any two elements $a, b \in R$ have a greatest common divisor and it is equal to any generator d of the ideal $(a, b) = (d)$.

(b) If $a, b \in R$ and $d = \gcd(a, b)$, then there exist $x, y \in R$ such that $d = ax + by$.

(c) Any two elements $a, b \in R$ have a least common multiple and it is equal to any generator m of the ideal $(a) \cap (b) = (m)$ and $(a, b)((a) \cap (b)) = (ab)$, so that

$$\operatorname{lcm}(a,b) = \frac{ab}{\gcd(a,b)}.$$

Proof. We prove simultaneously (a) and (b). Consider the ideal (a,b) in R. Since it is principal, there exists d such that $(a,b) = (d)$. Of course, we have $d = ax + by$ for some $x, y \in R$, which proves (b) when we show that $d = \gcd(a,b)$. But $a, b \in (a,b) = (d)$, so $d \mid a$ and $d \mid b$. On the other hand, if $d' \mid a$ and $d' \mid b$, then the equality $d = ax + by$ shows that $d' \mid d$. Hence d really is a greatest common divisor of a, b.

(c) The ideal $(a) \cap (b)$ is principal and if m is its generator, then $(m) \subseteq (a)$ and $(m) \subseteq (b)$, so $a \mid m$ and $b \mid m$. On the other hand, if $a \mid m'$ and $b \mid m'$ for some $m' \in R$, then $(m') \subseteq (a)$ and $(m') \subseteq (b)$, so $(m') \subseteq (a) \cap (b) = (m)$. This implies that $m \mid m'$. Hence , m is a least common multiple of a and (b).

Now we prove of formula relating $\operatorname{lcm}(a,b)$ to $\gcd(a,b)$. Denote

$$d' = \frac{ab}{\operatorname{lcm}(a,b)}.$$

We want to show that $d' = d$ (up to an invertible element). The equality above implies that:

$$\frac{a}{d'} = \frac{\operatorname{lcm}(a,b)}{b} \quad \text{and} \quad \frac{b}{d'} = \frac{\operatorname{lcm}(a,b)}{a}$$

so d' divides both a and b (since the right hand sides are elements of R). Thus d' as a common divisor to a and b divides the greatest common divisor d. Conversely, both a and b divide $\frac{ab}{d}$, since it is both a multiple of a as $a\frac{b}{d}$ and b as $\frac{a}{d}b$. Thus $\operatorname{lcm}(a,b)$ divides $\frac{ab}{d}$, which means that the quotient $\frac{ab}{d} : \operatorname{lcm}(a,b) = \frac{d'}{d}$ is an element of R. Hence, we get that d divides d'. Since both $d' \mid d$ and $d \mid d'$, these two elements are associated. ■

Sometimes, the elements x, y in **A.3.3**(b) may be found effectively. In particular, it is possible when R is the ring of integers or a polynomial ring $K[X]$ over a field K using the Euclidean algorithm. Since the last nonzero remainder in the Euclidean algorithm for $a, b \in R$ is a greatest common divisor of these two elements, it is possible to express it as a linear combination of a, b tracing back all the steps of this procedure. In these two most common cases, that is, $R = \mathbb{Z}$ or $R = K[X]$, both $\gcd(a,b)$ and $\operatorname{lcm}(a,b)$ are chosen in a unique way. In $\mathbb{Z}$, the units are ± 1, and the standard choice is $\gcd(a,b)$ and $\operatorname{lcm}(a,b)$ as positive integers. In $R = K[X]$ the units are all nonzero constants and in any class of associated elements it is possible to choose monic polynomial (that is, with highest coefficient 1). Thus $\gcd(a,b)$ and $\operatorname{lcm}(a,b)$ are chosen uniquely as monic polynomials.

Any ideal I in a ring R forms a subgroup of the additive group R, which by definition is abelian. Therefore, we can form the quotient group R/I with respect to addition, since I is a normal subgroup of the additive group R. But R/I inherits a ring structure from R when multiplication of the cosets $a+I, b+I$, $a, b \in R$ is defined by the equality $(a+I)(b+I) = ab+I$. Here it is necessary to know that the result of multiplication of $a+I$ and $b+I$ does not depend

on the representation of cosets by the representants a, b. In fact, we may have $a+I = a'+I$ and $b+I = b'+I$ for some $a', b' \in R$. Then our multiplication is correctly defined if $ab+I = a'b'+I$. But $a+I = a'+I$ if and only if $a'-a \in I$ and similarly, $b+I = b'+I$ if and only if $b'-b \in I$ according to the properties of cosets in groups. Thus $a' = a+i$ and $b' = b+j$, where $i, j \in I$ and $a'b'-ab = ib+ja+ij \in I$, so $a'b'+I = ab+I$. The ring R/I is called the quotient ring of R modulo I. As for groups, we have a natural surjection $\iota : R \to R/I$ mapping an element $a \in R$ onto the coset $a+I \in R/I$. This mapping is not only a group homomorphism, but also a ring homomorphism, since $\iota(ab) = ab+I = (a+I)(b+I) = \iota(a)\iota(b)$. Its kernel is the set of $a \in R$ such that $\iota(a) = a+I = I$, that is, $a \in I$. Thus $\operatorname{Ker}\iota = I$, which shows that every ideal I really is a kernel of a ring homomorphism – namely, the kernel of the natural surjection $\iota : R \to R/I$.

If $\varphi : R \to R'$ is any ring homomorphism and $I = \operatorname{Ker}\varphi$ its kernel, then there is a similar relation between the quotient R/I and the image $\varphi(R)$ as for the group homomorphisms, since φ is a group homomorphism of R into R' considered as additive groups and I is its kernel. The only new ingredient is the presence of multiplication and the mapping $\Phi : R/I \to R'$, where $\Phi(a+I) = \varphi(a)$ is not only a group isomorphism of the quotient R/I onto the image $\varphi(R)$ but also a ring isomorphism. In order to check this, we only need to note that

$$\Phi((a+I)(b+I)) = \phi(ab+I) = \varphi(ab) = \varphi(a)\varphi(b) = \Phi(a+I)\Phi(b+I).$$

Thus we can summarize these facts in what is called the main theorem on ring homomorphisms:

A.3.4 *If $\varphi : R \to R'$ is a ring homomorphism, then the kernel $I = Ker\varphi$ is an ideal of R and the function $\Phi(a+I) = \varphi(a)$ is a ring isomorphism of $R/Ker\varphi$ and $Im\varphi$.*

A.3.5 *Let $\varphi : R \to R'$ be a ring homomorphism with kernel $I = Ker\varphi$.*

(a) The image $\varphi(S)$ of a subring S of R is a subring of R' and the inverse image $\varphi^{-1}(S')$ of any subring S' of R' is a subring of R containing I. We have $\varphi(\varphi^{-1}(S')) = S'$ and $\varphi^{-1}(\varphi(S)) = S+I$. The inverse image $\varphi^{-1}(I')$ is an ideal in R if I' is an ideal in R'.

(b) If φ is surjective (so $R' \cong R/I$), then there is a one-to-one correspondence between the ideals I' of R' and the ideals I of R containing I in which I' corresponds to the inverse image $\varphi^{-1}(I')$ and I to its image $\varphi(I)$.

If R is a ring and I, J its ideals, then it is possible to form theirs sum $I+J$ and product IJ. The sum is simply the set of all sums $i+j$, where $i \in I$ and $j \in J$. It is easy to check that all such sums form an ideal. The product IJ is defined as the set of all finite sums of products ij, where $i \in I$ and $j \in J$. Here also it is evident that such finite sums of products form an ideal. This ideal IJ is in fact contained in the ideal $I \cap J$. If R is a principal ideal ring and $I = (a)$, $J = (b)$, then $I+J = (a, b) = (\gcd(a, b))$ and $IJ = (ab)$. As we know from **A.3.3**(c), we have $(I+J)(I \cap J) = IJ$, so if $I+J = R$, then $I \cap J = IJ$. Two ideals I, J in any ring are called **relatively prime** if $I+J = R$. This condition simply means that $1 = i+j$, where $i \in I$ and $j \in J$ (since every ideal which contains 1 is equal to R). Notice

that if I is relatively prime with J and J', then it is also relatively prime with JJ'. in fact, $I+J=R$ and $I+J'=R$ imply that $i+j=1$ and $i'+j'=1$ for $i,i'\in I$, $j\in J$, $j'\in J'$. Thus $ii'+ij'+i'j+jj'=1$, where $i"=ii'+ij'+i'j\in I$ and $jj'\in JJ'$, so $i"\in I$ and $i"+jj'=1$, that is, $I+JJ'=R$. In several places, we use the following isomorphism:

A.3.6 *If I,J are relatively prime ideals in a ring R, then the homomorphism $\varphi: R\to R/I\times R/J$ such that $\varphi(r)=(r+I,r+J)$ induces an isomorphism $\varphi^*: R/(I\cap J)\to R/I\times R/J$.*

Proof. It is easy to check that φ is a homomorphism and that $\ker\varphi = I\cap J$ ($\varphi(r)=(r+I,r+J)=(0,0)$ if and only if $r+I=R$ and $r+J=R$, that is, $r\in I$ and $r\in J$).

We show that φ is surjective. Since $I+J=R$, we have $1=i+j$ for some $i\in I$ and $j\in J$. Notice that $1+I=j+I$ and $1+J=i+J$. Hence, for $(x+I,y+J)$ in $R/I\times R/J$, we can take $r=xj+yi$ and then

$$\varphi(r)=(xj+yi+I,xj+yi+J)=(xj+I,yi+J)=((x+I)(j+I),(y+J)(i+J))=$$

$$((x+I)(1+I),(y+J)(1+J))=(x+I,y+J),$$

so φ is surjective and by **A.3.4**, we get the induced isomorphism φ^*. ■

A.3.7 Example. Take $R=\mathbb{Z}$, $I=(a)$ and $J=(b)$ where a,b are relatively prime, so that $I+J=\mathbb{Z}$ by **A.3.3**(a). As we know, the assumption $\gcd(a,b)=1$ implies that $I\cap J=IJ=(ab)$. Hence, by **A.3.6**, we have

$$\mathbb{Z}/(ab)\cong\mathbb{Z}/(a)\times\mathbb{Z}/(b),$$

where the isomorphism maps the residue of an integer n modulo ab on the pair of its residues (n_1,n_2) modulo a and b. In more compact notation, we write $\mathbb{Z}_{ab}\cong\mathbb{Z}_a\times\mathbb{Z}_b$,. If $n=p_1^{k_1}\cdots p_r^{k_r}$ is a factorization of an integer into a product of prime numbers, then applying the formula above several times, we get a very useful isomorphism of rings:

$$\mathbb{Z}_n\cong\mathbb{Z}_{p_1^{k_1}}\times\cdots\times\mathbb{Z}_{p_r^{k_r}}.$$

Taking units in these rings, we have also an isomorphism of groups, which we use several times:

$$\mathbb{Z}_n^*\cong\mathbb{Z}_{p_1^{k_1}}^*\times\cdots\times\mathbb{Z}_{p_r^{k_r}}^*.$$

Similarly, if $R=K[X]$ is a polynomial ring, $I=(f(X))$ and $J=(g(X))$, where $f(X),g(X)$ are relatively prime polynomials, then as above, we have $I+J=K[X]$ and **A.3.6** gives this time

$$K[X]/(fg) \cong K[X]/(f) \times K[X]/(g).$$

A.3.8 Characteristic of a ring. If R is a commutative ring with identity, then the additive subgroup $\langle 1 \rangle$ generated by the identity consists of multiples $k \cdot 1$ for $k \in \mathbb{Z}$. If the order of this group is infinite, then it is isomorphic with the group of integers $\mathbb{Z}$. In this case, we say that the characteristic of R is zero. If 1 generates a finite group of order n, then $\langle 1 \rangle = \{0 \cdot 1, 1 \cdot 1, \ldots, (n-1) \cdot 1\}$ and $n \cdot 1 = 0$. This group is isomorphic to $\mathbb{Z}_n$ the group of residues modulo n. In this case, we say that R has characteristic n. Observe that n is the order of 1 in the additive group of the ring R in this case. The characteristic of a commutative ring R with identity is sometimes denoted by $\mathrm{char}(R)$. Notice that the multiples $k \cdot 1$ for $k \in \mathbb{Z}$ form a subring of R, so a commutative ring R with identity contains a subring isomorphic to the integers $\mathbb{Z}$ if its characteristic is 0, and a subring isomorphic to $\mathbb{Z}_n$ if its characteristic is n. In particular, the ring of integers $\mathbb{Z}$ has characteristic 0, and the ring $\mathbb{Z}_n = \{0, 1, \ldots, n\}$ of residues modulo n has characteristic n. For convenience of references, we record these facts:

A.3.9 *The characteristic of a commutative ring with identity is either* 0 *or a positive integer* n*. The identity* $1 \in R$ *generates a subring isomorphic to the integers* $\mathbb{Z}$ *in the first case, and a subring isomorphic to* $\mathbb{Z}_n$ *in the second case.*

Notice that if the number n is composite, that is, $n = kl$, where $k, l > 1$, then the ring $\mathbb{Z}_n$ has zero divisors, that is, $k \neq 0$ and $l \neq 0$ but $kl = 0$. If the number $n = p$ is a prime, then $\mathbb{Z}_p$ is without zero divisors, since $kl = 0$ in this ring means that $p \mid kl$, which implies that $p \mid k$ or $p \mid l$, that is, $k = 0$ or $l = 0$ in $\mathbb{Z}_p$.

A.4 Fields

If in a commutative ring with identity every nonzero element is invertible, then this ring is called a field. In somewhat other words, a field is a commutative ring with identity in which nonzero elements form a group with respect to multiplication. Notice that invertible elements are not zero divisors, so any field is an integral domain (if a is invertible with the inverse a^{-1} and $ab = 0$, then $a^{-1}ab = b = 0$).

Fields are often denoted by letters $K, L, M, \ldots$ (with K having its explanation in the German term "Körper"). Thus any field contains at least two elements: 0 and 1. A subring of a field K, which also is a field is called subfield of K. In order to check that K' is a subfield of K it suffices to check that $a, b \in K'$ imply $a + b, ab, -a, a^{-1} \in K'$ (a^{-1} for $a \neq 0$).

Among all fields considered in this text, a special role is played by the field of rational numbers $\mathbb{Q}$ and the fields of residues modulo prime numbers $\mathbb{Z}_p$. The former fields are very often denoted by $\mathbb{F}_p$ and we follow this tradition. The fact that $\mathbb{F}_p$ is a field follows from a general property of finite integral domains (commutative rings with identity without zero divisors). In fact, if R is a finite integral domain and $a \in R$, $a \neq 0$, then the powers a^n for $n = 1, 2, \ldots$ are nonzero and can not be different, so there exist exponents k, l such that

$l > k$ and $a^l = a^k$. Hence, we have $a^k(a^{l-k} - 1) = 0$, which implies $a^{l-k} = 1$ as $a^k \neq 0$. Thus a has an inverse a^{l-k-1} in R. Notice that $\mathbb{Q}$ has characteristic 0 (the order of 1 in the additive group of $\mathbb{Q}$ is infinite) and $\mathbb{F}_p$ has characteristic p (the order of 1 is p).

A.4.1 (*a*) *The characteristic of a field is* 0 *or a prime number.*

(*b*) *Any field K of characteristic* 0 *contains a unique subfield isomorphic to the rational numbers $\mathbb{Q}$, and any field of characteristic p contains a unique subfield isomorphic to $\mathbb{F}_p$.*

Proof. (a) The characteristic of any commutative ring with identity is either 0 or a positive integer n by **A.3.8**. If characteristic of a field K is not 0, then it is n for some positive integer n and K contains a subring isomorphic to $\mathbb{Z}_n$ also by **A.3.8**. But if n is composite (that is, $n = kl, k < n, l < n$), then $\mathbb{Z}_n$ contains zero divisors ($kl = 0$, $k \neq 0, l \neq 0$), which are absent in fields. Thus n must be a prime.

(b) If a field K has characteristic 0, then the multiples $k \cdot 1$, $k \in \mathbb{Z}$ form a subring of K isomorphic to $\mathbb{Z}$. Since every quotient $(k \cdot 1)/(l \cdot 1)$, where $l \neq 0$ must belong to K, this field contains a subfield isomorphic to the rational numbers $\mathbb{Q}$. If K has characteristic p, then K contains a subfield isomorphic to $\mathbb{F}_p$. Such subfields of K are unique, since every subfield contains 1, so it must contain the subfield generated by this element. In fact, the subfield generated by 1 is the intersection of all subfields of K (it is contained in any subfield). □

The fields $\mathbb{Q}$ and $\mathbb{F}_p$ are called **prime**, since they are the smallest ones in the sense that every field contains (an isomorphic copy) of exactly one of them and they do not contain any proper subfields.

The fields, which we use to exemplify the Galois theory in this book are mainly number fields, that is, subfields of the field of complex numbers $\mathbb{C}$, finite fields (see Chapter 5) and fields of rational functions with coefficients in number fields or finite fields. The latter, we introduce in the next section of this Appendix, but already here, we note that fields of rational functions are fields of fractions of integral domains through a construction, which generalizes the construction of the field of rational numbers from the ring of the integers.

Take any integral domain R (for example, the ring of integers $\mathbb{Z}$). Consider the set $K = R_0$ of all pairs (a, b) such that $a, b \in R, b \neq 0$. We think of a as nominator and b as denominator of a fraction. We say that (a, b) and (c, d) are equivalent if $ad = bc$ (both these pairs define the same fraction). This equivalence can be denoted in some way, for example as $(a, b) \sim (c, d)$. Denote by a/b the set of all pairs equivalent to (a, b). Such a class will be called a fraction. Now we define addition and multiplication of fractions in such a way that we get a field:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \qquad \frac{a}{b}\frac{c}{d} = \frac{ac}{bd}.$$

It needs a little formal calculations that the addition and multiplication of fractions give the same result independently of the presentation of the involved fractions by the pairs of elements of R (for example, we have to show that if $(a, b) \sim (a', b')$ and $(c, d) \sim (c', d')$, then $(ad + bc, bd) \sim (a'd' + b'c', b'd')$). When this is done, we have to check that the fractions really form a field and this also needs a little of very simple (but also tedious) computations.

Anyway, we check that we get a field in which R can be naturally embedded by mapping $a \in R$ onto the fraction $a/1$. In fact, in this way, we usually consider R as a subring of its field of fractions $K = R_0$. Of course, if $R = \mathbb{Z}$, then $\mathbb{Z}_0 = \mathbb{Q}$ is the field of rational numbers. Notice that the field of fractions of R is very often called the quotient field of R (meaning the field of quotients a/b rather than fractions a/b). There is a little danger that using "quotient ring" in this sense may be confused with quotients of rings modulo ideals. We use the term "field of fractions" in order to avoid such misunderstandings.

A.4.2 *Any finite subgroup of the multiplicative group of a field K is cyclic.*

Proof. Let G be a subgroup of order n of the multiplicative group of a field K. Let the exponent of G be m, that is, $x^m = 1$ for every element $x \in G$. Since the equation $X^m - 1 = 0$ has at most m solution in the field K and every element of G satisfies this equation, we have $n \leq m$. But as we know (see Lemma A), the exponent m is the maximal order of the elements of G and $m \mid n$. Hence $m = n$ and the group G has an element of order n, that is, G is cyclic. □

Notice that as a special case, the last result says that the groups of nonzero residues $(\mathbb{Z}/p\mathbb{Z})^*$ modulo prime number p are cyclic as the groups of nonzero elements in the fields $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

A.4.3 Maximal ideals and fields. An ideal I in a ring R is called **maximal** if it is not equal R and if an ideal J is such that $I \subseteq J \subseteq R$, then $J = I$ or $J = R$. A very important property of maximal ideals, which we use on some occasions is the following result:

A.4.4 *An ideal I in a ring R with identity is maximal if and only if R/I is a field.*

Proof. If R/I is a field, then there are no nontrivial ideals in this ring, so the ideal I is maximal by **A.3.5**(b). Conversely, if I is a maximal ideal, then **A.3.5**(b) says that R/I is without proper ideals, so it is a field by **A.4.6**. □

We apply **A.4.4** mostly when R is the ring of integers or the ring of polynomials over a field. As we know, all ideals in $\mathbb{Z}$ and $K[X]$ (K a field) are principal (see **A.3.2**). For such rings, we have

A.4.5 *In a principal ideal ring, the maximal ideals are exactly those generated by irreducible elements.*

Proof. If R is a principal ideal ring and (a) an ideal generated by an irreducible element (a) (see the definition of irreducible elements on p.233), then the ideal is maximal. In fact, if $(a) \subseteq (b) \subset R$, then a (b) gives $a = bc$, where $c \in R$. Hence, we have that b or c must be a unit in R. But b is not a unit (otherwise $(b) = R$), so c is a unit, which means that $(a) = (b)$ (see **A.3.1**. Thus (a) is maximal.

Conversely, if (a) is maximal, then a must be irreducible, since otherwise $a = bc$, where both b and c are not units. Hence, we have $(a) \subset (b) \subset R$, since $(a) = (b)$ gives that $a = bc$ implies that c is a unit, whereas $(b) = R$ gives that b is a unit (see **A.3.1**). □

In the ring $\mathbb{Z}$ the irreducible elements are prime numbers, so all maximal ideals are the ideals (p), where p is a prime number. In the polynomial rings $K[X]$, K a field, the irreducible elements are exactly all irreducible polynomials $f(X)$, which generate the maximal ideals. Thus each quotient $\mathbb{Z}/(p)$ is a field (with p elements). Similarly, each quotient ring $K[X]/(f(X))$ is a field when $f(X)$ is an irreducible polynomial.

If $K[X]$ is a polynomial ing over a field K and $I = (f(X))$ an ideal generated by a nonconstant polynomial $f(X) \in K[X]$ then we write $[g(X)] = g(X) + I$ to denote the class of $g(X)$ in the quotient. Of course, the class $[g(X)]$ consists of all polynomials $g(X) + f(X)q(X)$, where $q(X)$ is an arbitrary polynomial. We have as usual, $[g(X)] = [h(X)]$ if and only if $g(X) - h(X) \in I = (f(X))$, that is, $g(X) - h(X)$ is a multiple of $f(X)$. Of course, we have $[f(X)] = [0]$.

In particular, if $a \in K$ is a constant polynomial, then its class $[a]$ may be simply identified with a, since for classes of the constant polynomials, we have $[a] = [b]$ if and only if $f(X)$ (a nonconstant polynomial) divides $a - b$ (a constant), so it must be $a = b$. In fact, every class $[g(X)]$, we have $[g(X)] = [r(X)]$, where $r(X)$ is the residue of $g(X)$ divided by $f(X)$, since $g(X) - r(X)$ is divisible by $f(X)$. As we know, the residue is unique, so every class has a unique representation as $[r(X)]$ with $\deg(r(X)) < \deg(f(X))$.

We will always identify $[a]$ with a for constants so that K will be considered as a subring of the quotient $K[X]/(f(X))$. If we denote $\alpha = [X]$ and $r(X) = b_k X^k + \cdots + b_1 X + b_0$, then $[r(X)] = b_k[X]^k + \cdots + b_1[X] + b_0 = b_k\alpha^k + \cdots + b_1\alpha + b_0$. In particular, if $f(X) = a_n X^n + \cdots + a_1 X + a_0$ is a polynomial of degree n, then $0 = [f(X)] = a_n\alpha^n + \cdots + a_1\alpha + a_0$, that is, we have $f(\alpha) = 0$, which means that $f(X)$ has a zero α in the quotient $K[X]/(f(X))$. Thus, the quotient $K[X]/(f(X))$ can be described as the ring $K[\alpha]$ of all polynomials expressions $b_k\alpha^k + \cdots + b_1\alpha + b_0$, where α is a zero of $f(X)$ and $0 \leq k < n$.

As an example, we have $\mathbb{R}[X]/(X^2 + 1) = \mathbb{R}[\alpha]$, where $\alpha^2 + 1 = 0$ and every element hasa unique representation as $a + b\alpha$. Thus the quotient is the field of complex number as $\alpha^2 = -1$.

In particular when $K = \mathbb{F}$ is a finite field with q elements and $f(X)$ is a polynomial of degree n, then $\mathbb{F}[X]/(f(X)) = \mathbb{F}[\alpha]$ is a ring with q^n elements $b_k\alpha^k + \cdots + b_1\alpha + b_0$, where $0 \leq k < n$ (so there are q possible choices for each b_i, $i = 0, 1, \ldots, n-1$). The ring $\mathbb{F}[X]/(f(X))$ is a field exactly when $f(X)$ is irreducible in $\mathbb{F}[X]$.

A.4.6 *A ring with unity has only the trivial ideals* (0) *and* R *if and only if it is a field.*

Proof. If R is a field and I is a nonzero ideal, then there is $a \in I$ such that $a \neq 0$. Thus a has an inverse, that is, there is $a' \in R$ such that $aa' = 1$. Hence $1 \in I$, so $I = R$.

If R is a ring whose only ideals are (0) and R, then for any $a \in R$, $a \neq 0$, we can take the principal ideal Ra. This ideal is nonzero, since $a = a \cdot 1 \in I$. Hence $I = R$. This means that $1 = a'a$ for some $a' \in R$, so a has an inverse in R. Hence R is a field. ■

A.5 Chinese Remainder Theorem

The Chinese Remainder Theorem (CRT) says that if $d_1, \ldots, d_k \in R$ are relatively prime positive integers and $r_1, \ldots, r_k$ are any integers, then there is an integer a such that the residue of a when divided by d_i is r_i for $i = 1, \ldots, k$. When we say that the remainder of a when divided by d is r, we mean that d divides $a - r$, which is denoted by $d \mid a - r$ or $a - r \in (d)$ or $a \equiv r \pmod{d}$ (a is congruent to r modulo d). This result is true in much greater generality. Since we use it both for integers and polynomials, we give a formulation, which covers this two cases:

A.5.1 *Let R be an integral domain and let $d_1, \ldots, d_k \in R$ be relatively prime elements, that is, $(d_i, d_j) = R$. If $r_1, \ldots, r_k \in R$, then there exists $a \in R$ such that $a - r_i \in (d_i)$ for all $i = 1, \ldots, k$.*

Proof. We use induction starting with $k = 1$ when the result is of course true. Notice know that it is true for $k = 2$, since by **A.3.6**, we have a surjection of R onto $R/(d_1) \times R/(d_2)$ mapping a onto $(a + (d_1), a + (d_2))$. But this means that if we take $(r_1 + (d_1), r_2 + (d_2))$, then we can find $a \in R$ such that $a + (d_1) = r_1 + (d_1)$ and $a + (d_2) = r_2 + (d_2)$, that is, $a - r_1 \in (d_1)$ and $a - r_2 \in (d_2)$.

Assume now that the theorem is true for $k-1$ elements of R and consider k relatively prime elements $d_1, \ldots, d_k \in R$. Denote $d = d_1 d_2 \cdots d_k$. First we note that every d_i, $(i = 1, \ldots, k)$, and d/d_i are relatively prime. In fact, we noted earlier (see the text preceding **A.3.6**) that an ideal relatively prime with two other is relatively prime with their product ((d/d_i) is the product of all (d_j) for $j \neq i$). Now we use k times the case of two factors d_i and find $x_1, \ldots, x_k \in R$ such that

$$x_i - 1 \in (d_i) \quad \text{and} \quad x_i \in (d/d_i) \subseteq (d_j) \quad \text{for } j \neq i.$$

Take now $a = r_1 x_1 + \cdots + r_k x_k$. We check that $a - r_i \in (d_i)$ for all $i = 1, \ldots, k$. In fact, we have $a - r_i = r_1 x_1 + \cdots + r_i(x_i - 1) + \cdots + r_k x_k \in (d_i)$. ■

A.6 Polynomial rings

If R is a commutative ring, then the ring of polynomials with coefficients in R is the set of all expressions $a_0 + a_1 X + a_2 X^2 + \cdots$ where $a_i \in R$, almost all a_i are 0 and X is a symbol (called a variable), which are added and multiplied as usual polynomials. This ring is denoted by $R[X]$. The construction may be used inductively – we can construct a polynomial ring over $R[X]$ and so on. Thus $R[X][Y] = R[X, Y]$ is the polynomial ring in two variables over R. Continuing in this way, we get polynomial rings $R[X_1, \ldots, X_n]$ over R in n variables $X_1, \ldots, X_n$.

The most common in this book are polynomial rings over fields and, in particular, the polynomial rings $K[X]$ in one variable over a field K. In this case, we have the well-known

division algorithm which for $f(X), g(X) \in K[X]$ with $g(X) \neq 0$, gives the unique quotient $q(X) \in K[X]$ and the remainder $r(X) \in K[X]$ such that $g(X) = g(X)q(X) + r(X)$ and $\deg r(X) < \deg g(X)$.

A.6.1 Factor Theorem. *Let $K \subseteq L$ be a field extension.*

(a) The remainder of $f \in K[X]$ divided by $X - a$, $a \in L$, is equal $f(a)$;

(b) An element $a \in L$ is a zero of $f \in K[X]$ if and only if $X - a | f(X)$ (in $L[X]$).

Proof. (a) The division algorithm for polynomials gives

$$f(X) = (X - a)q(X) + r,$$

where $\deg r < 1$, that is, the remainder r is a constant polynomial. Thus, taking $X = a$, we get $f(a) = r$.

(b) Using (a), we have $f(a) = 0$ if and only if $r = f(a) = 0$. □

The polynomial rings $K[X]$, like the ring of integers $\mathbb{Z}$ are unique factorization domains (see (UFD)). This property is shared by all principal ideal domains (see **A.3.2**) but we refrain from proving this in such a generality. The unique factorization property also holds in the polynomial rings over the ring of integers and over fields, since in general it is true that if a domain R is UFD, then also the polynomial ring $R[X]$ is UFD (see [L], Chap.IV, Thm. 2.3). Below, we give a proof that the polynomial rings over fields are unique factorization domains

A.6.2 *Let K be a field. Every polynomial of degree degree ≥ 1 in $K[X]$ is a product of irreducible polynomials. If*

$$f = p_1 \dots p_k = p'_1 \dots p'_l,$$

where p_i and p'_i are irreducible polynomials, then $k = l$ and with suitable numbering of the factors p_i, p'_j, we have $p'_i = c_i p_i$, where $c_i \in K$.

Proof. First we prove by induction that every polynomial $f(X)$ of degree at least one is a product of irreducible polynomials. It is clear for polynomials of degree one (they are irreducible). Assume that we have proved that every polynomial of degree less than $n > 1$ is a product of irreducible polynomials. Take an arbitrary polynomial $f(X)$ of degree n. If $f(X)$ is irreducible, we have what we want. If $f(X)$ is reducible, then $f(X) = g(X)h(X)$, where $1 \leq \deg g < n$ and $1 \leq \deg h < n$, so both g, h are products of irreducible polynomials. Thus also $f(X)$ is such a product.

Now consider two factorizations of $f(X)$ given in the theorem:

$$p_1 \dots p_k = p'_1 \dots p'_l,$$

where all p_i, p'_j are irreducible. We prove theorem by induction with respect to $m = k + l$. If $m = 2$, then we have one factor to the left and one to the right, so the claim that $k = l$ is true (and the factors are equal). Assume that the theorem is true when the number of factors p_i, p'_j is less than $m \geq 2$. Consider the case when the number of factors is m. The irreducible polynomial p_k divides the product on the right hand side. Hence p_k must divide at least one of the factors of this product. Say that $p_k | p'_l$ (we can change the numbering of the factors if necessary). But both these polynomials are irreducible, so $p'_l = c_k p_k$ for some constant c_k. We divide both sides by p_k and get

$$p_1 \dots p_{k-1} = c_k p'_1 \dots p'_{l-1},$$

so the number m is now $k+l-2$ and by our inductive assumption the theorem is true. Thus $k - 1 = l - 1$, that is, $k = l$ and by suitable numbering of the factors, we get $p'_i = c_i p_i$ for $i = 1, \dots, k - 1$. □

A.7 Modules over rings

If R is a ring and M is an abelian group, then we say that M is a left module over R if for every pair $(r, m) \in R \times M$, we have an element $rm \in M$ so that

(a) $r(m_1 + m_2) = rm_1 + rm_2$,

(b) $(r_1 + r_2)m = r_1 m + r_2 m$,

(c) $(r_1 r_2)m = r_1(r_2 m)$,

(d) $1m = m$,

where $r, r_1, r_2 \in R$ and $m, m_1, m_2 \in M$. A right module is defined in similar way. If $R = K$ is a field, then K-modules are called vector spaces or linear spaces (over the field K) and their elements are called vectors. A homomorphism of modules over R is a function $\varphi : M \to M'$ satisfying:

(a) $\varphi(m_1 + m_2) = \varphi(m_1) + \varphi(m_2)$;

(b) $\varphi(rm) = r\varphi(m)$,

when $m, m_1, m_2 \in M$ and $r \in R$. The kernel of φ is its kernel as a homomorphism of abelian groups, that is, $\operatorname{Ker} \varphi = \{m \in M_1 | \varphi(m) = 0\}$. The kernel is also a submodule of M_1, that is, if $r \in R$ and $m \in \operatorname{Ker} \varphi$, then $rm \in \operatorname{Ker} \varphi$.

If M_1, M_2 are R-modules, then the pairs (m_1, m_2), where $m_1 \in M_1$ and $m_2 \in M_2$ form a module when the addition of pairs and multiplication by elements of R are defined on coordinates: $(m_1, m_2) + (m'_1, m'_2) = (m_1 + m'_1, m_2 + m'_2)$ and $r(m_1, m_2) = (rm_1, rm_2)$. This new module is denoted by $M_1 \times M_2$ and called the direct sum (or direct product) of M_1, M_2. This definition can be extended on arbitrary finite number of modules (it is also possible to consider infinite families but the definitions of sum and product are then different).

In this book, we need some knowledge of modules over fields, the ring of integers and polynomial rings. We say that a module M is finitely generated if there are elements $m_1, \dots, m_k \in M$ such that every element $m \in M$ can be expressed as a linear combination of these elements, that is, if there are $r_1, \dots, r_k \in R$ such that $m = r_1 m_1 + \cdots + r_k m_k$. We write $M = \langle m_1, \dots, m_k \rangle$. If there is one element $m \in M$ such tat $M = \langle m \rangle$, then M is called **cyclic module**. Notice that if $M = \langle m \rangle$ is cyclic, then we have a surjective homomorphism $\varphi : R \to M$ such that $\varphi(r) = rm$. If I denotes the kernel of φ, then $R/I \cong M$. Thus a cyclic module can be also defined as a module isomorphic to a module R/I. If $R = \mathbb{Z}$ is the ring of integers, than the cyclic modules are $\mathbb{Z}/(n) = \mathbb{Z}_n$, which are finite cyclic groups when $n > 0$ or the infinite cyclic group $\mathbb{Z}$ when $n = 0$. This explains the terminology.

If M is a left module over a ring R, then the **annihilator** of M is the set of all $r \in R$ such that $rM = 0$ (that is, $rm = 0$ for each $m \in M$). The annihilator of M is an ideal in R, which is denoted by $\mathrm{Ann}_R(M)$. In fact, if $r_1, r_2 \in \mathrm{Ann}_R(M)$, that is, $r_1 M = r_2 M = 0$, then $(r_1 - r_2)M = 0$, so $r_1 - r_2 \in \mathrm{Ann}_R(M)$. Similarly, if $r \in \mathrm{Ann}_R(M)$, that is, $rM = 0$, then for any $r' \in R$, we have also $(r'r)M = 0$, so $r'r \in \mathrm{Ann}_R(M)$. Notice that the annihilator of the R-module $M = R/(a)$ is equal to (a). In fact, it is clear that $aM = 0$, so $a \in \mathrm{Ann}_R(M)$. On the other hand, if $r \in \mathrm{Ann}_R(M)$, that is, $rM = 0$, then in particular $r(1 + (a)) = r + (a) = 0$, so $r \in (a)$. Hence $\mathrm{Ann}_R(M) = (a)$. In the particular case when $M = R = R/(0)$, we have $\mathrm{Ann}_R(R) = (0)$.

A.7.1 Theorem. *If R is a principal ideal ring, then every finitely generated module M over R is a finite direct sum of cyclic R-modules. Moreover,*

$$M = R/(a_1) \times R/(a_2) \times \cdots \times R/(a_r),$$

where $a_1 \mid a_2 \mid \ldots \mid a_r$, $Ann(M) = (a_r)$ and the ideals $(a_1), (a_2) \ldots, (a_r)$ are uniquely defined by M.

We can not give a proof of this result here, but only note that we use it in two particular situations. Notice that it may happen that some $a_i = 0$, which corresponds to $R/(a_i) = R$. In our notations, we follow here a convention that $0 \mid a$ for any $a \in R$.

If $R = \mathbb{Z}$, then **A.7.1** says that every abelian group is a direct sum of finitely many cyclic groups. These cyclic group are either finite of the form $\mathbb{Z}/(a)$, $a > 0$ or infinite of the form $\mathbb{Z}$. If the group is finite, then there are only the summands of the first type. Each positive integer a can be factorized as a product of prime powers and each cyclic group $\mathbb{Z}/(a)$ can be split into a product of cyclic groups $\mathbb{Z}/(p^k)$ for prime numbers p and their exponents k such that $p^k \mid a$ and $p^{k+1} \nmid a$ according to **A.3.7**. The set of such cyclic groups is also uniquely determined by the isomorphism class of G (notice that the same prime p with the same exponent k may appear several times). We record this result as we refer to it occasionally:

A.7.2 Fundamental Theorem on Finite Abelian Groups. *Every finite abelian group G is a direct product*

$$G = \mathbb{Z}/(a_1) \times \mathbb{Z}/(a_2) \times \cdots \times \mathbb{Z}/(a_r),$$

where $a_1 \mid a_2 \mid \ldots \mid a_r$, $Ann(G) = (a_r)$ and the ideals $(a_1), (a_2) \ldots, (a_r)$ are uniquely defined by G. The cyclic groups $\mathbb{Z}/(a_i)$ can be represented as direct products of cyclic groups whose orders are prime powers. The number of such factors in the product and the orders of the cyclic groups in it are also uniquely determined by the group.

The second important case when we use modules over principal ideal rings is the case of polynomial rings over fields. As we know every ring $R = K[X]$, where K is a field is a principal ideal domain (see **A.3.2**). Consequently theorem **A.7.1** is true over R. As we know, the cyclic modules in this case are quotients $K[X]/(p(X))$, where $p(X)$ is a polynomial. If this is the zero polynomial, then the cyclic module is $K[X]$ itself. This module has an infinite dimension as a vector space over K (a basis is $1, X, X^2, \ldots$). If $p(X)$ is a polynomial of degree $n > 0$,then the quotient ring consists of (classes) of all remainders when polynomials are divided by $p(X)$ (the elements of $K[X]/(p(X))$ are cosets $r(X) + (p(X)) = \{r(X) + p(X)q(X), q(X) \in K[X]\}$ and each coset may be represented by a unique polynomial $r(X)$ of degree at most $n-1$). Thus $r(X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1}$ and $K[X]/(p(X))$ has dimension n and a basis $1, X, \ldots, X^{n-1}$ over K. Similarly to the case of integers, every polynomial $p(X)$ can be factored as a product of irreducible factors, so that using **A.3.7**, we can represent M uniquely as a product of cyclic modules $K[X]/(p^k)$, where p are irreducible polynomials. Thus in the case of the polynomial ring $K[X]$, the theorem **A.7.1** says the following:

A.7.3 *Every $K[X]$-module M, which is of finite dimension as a vector space over K is a direct product*

$$M = K[X]/(p_1) \times K[X]/(p_2) \times \cdots \times K[X]/(p_r),$$

where $p_1 \mid p_2 \mid \ldots \mid p_r$, $Ann(M) = (p_r)$ and the ideals (p_1), $(p_2) \ldots (p_r)$ are uniquely defined by M. The cyclic modules $K[X]/(p_i)$ can be represented as direct products of cyclic modules $K[X]/(p^k)$, where p are irreducible polynomials in $K[X]$. The number of such factors in the product and the ideals (p^k) are also uniquely determined by the module M.

Notice that if the polynomial p_r, which generates the annihilator of M is separable (without multiple zeros), then $M = K[X]/(p_r)$.

A.7.4 Group rings. If G is a finite group and R a ring, then it is possible to form a ring, denoted by $R[G]$ and called the group ring of G over R. Formally, this ring consists of all functions $\varphi : G \to R$. Such functions are added and multiplied in the following way: $(\varphi+\psi)(g) = \varphi(g)+\psi(g)$ and $\varphi\psi(g) = \sum_{h\in G} \varphi(h)\psi(h^{-1}g)$. In practice, we denote $\varphi(g) = r_g$ and write any element of $R[G]$ as a sum $\varphi = \sum_{g\in G} r_g g$. Such sums are added by adding the corresponding coefficients for $g \in G$ and multiplied in the "usual way" (according to the above definitions of addition and multiplication). This means that if $\psi = \sum_{g\in G} s_g g$, then the coefficient of g in the product $\varphi\psi$ is the sum of $r_{g'}s_{g''}$ such that $g'g'' = g$.

In Chapter 11, we defined the notation of G-module. If A is such a G-module, which is an R-module for a ring R with the property $g(ra) = r(ga)$ for each $r \in R$ and $g \in G$, then it becomes a module over the group ring $R[G]$ if we define $(\sum_{g\in G} r_g g)a = \sum_{g\in G} r_g(ga)$. Conversely, each $R[G]$-module A is a G-module (as in Chapter 11) and at the same time an R-module (and both structures are related by $(rg)a = g(ra) = r(ga)$ when $r \in R$, $g \in G$ and $a \in A$).

A.8 Group actions on sets

We say that a group G acts on a set X if for every pair $(g, x) \in G \times X$, we have an element $gx \in X$ so that $(gg')x = g(g'x)$ and $ex = x$ (e is the identity in G). Thus an action of G on X is a function from $G \times X$ to X satisfying these two assumptions, which can be best understood in terms of the transformations of the set X. If we fix g, then we get a function $\sigma_g : x \mapsto gx$ for $x \in X$(instead of the term function, we use often the term transformation in this case). The function σ_g is a bijection on the set X, since it has an inverse function $\sigma_{g^{-1}}$. In fact, we have $\sigma_g \circ \sigma_{g'}(x) = \sigma_g(\sigma_{g'}(x)) = \sigma_g(g'x) = g(g'x) = (gg')x = \sigma_{gg'}(x)$, that is, $\sigma_g \circ \sigma_{g'} = \sigma_{gg'}$ and $\sigma_e(x) = ex = x$, that is, $\sigma_e = id_X$ is the identity mapping on X. Hence, $\sigma_g \circ \sigma_{g^{-1}} = \sigma_{gg^{-1}} = \sigma_e = id_X$ and similarly, $\sigma_{g^{-1}} \circ \sigma_g = id_X$, which shows that σ_g and $\sigma_{g^{-1}}$ are inverses of each other.

If X is a set, then all bijective functions $\sigma : X \to X$ form a group under composition of functions, that is, if also $\tau : X \to X$ is a bijection, then the composition $\tau\sigma(x) = \tau(\sigma(x))$ for $x \in X$ is a bijection on X. The composition of functions is associative, the identity is the identity function $id(x) = x$ for $x \in X$, and the inverse of σ is the inverse function σ^{-1}. Denoting by $\mathcal{B}(X)$ the group of all bijections on X, we define a transformation group as any subgroup of $\mathcal{B}(X)$. Notice that, for simple combinatorial reasons, if X is a finite set, then every injective or surjective function $\sigma : X \to X$ is automatically bijective (that is, an injective function must be also surjective, and a surjective function must be injective). This easy observation is often useful as well as the following general property of functions, which we often use:

A.8.1 Lemma. *If $\sigma : X \to Y$ and $\tau : Y \to X$ are functions such that $\tau \circ \sigma = id_X$, then σ is injective and τ is surjective, so if also $\sigma \circ \tau = id_Y$, then both σ and τ are bijective.*

Proof. If $x, x' \in X$ and $\sigma(x) = \sigma(x')$, then $\tau \circ \sigma(x) = \tau \circ \sigma(x')$, so $x = x'$. Hence σ is injective (different $x.x'$ have different images by σ). If $x \in X$, then $x = \tau(\sigma(x))$, so τ is surjective (every element x of X is an image of an element $\sigma(x)$ of Y). ■

The observations above concerning actions of groups on sets can be now simply expressed by saying that any action of a group G on a set X defines a homomorphism from G to the transformation group $\mathcal{B}(X)$ such that $g \in G$ maps onto the transformation σ_g. Denoting such a homomorphism by $\Phi : G \to \mathcal{B}(X)$, we have $\Phi(g) = \sigma_g$. It is easy to see that also conversely, any homomorphism $\Phi : G \to \mathcal{B}(X)$ defines an action of G on X if we define

$gx = \Phi(g)(x)$. The properties $\Phi(gg') = \Phi(g)\Phi(g')$ and $\Phi(e) = Id$ of the homomorphism Φ immediately translate to $(gg')x = g(g'x)$ and $ex = x$ for $g, g' \in G$ and $x \in X$.

Let a group G act on a set X. The orbit of $x \in X$, denoted by Gx is the set of all images of x by the elements of G, that is, $Gx = \{gx, x \in X\}$. The stabilizer of $x \in X$ in G, denoted by G_x, is the subgroup of G consisting of those elements, which map x on itself, that is, $G_x = \{g \in G | gx = x\}$. If $g \in G$, we denote by X^g the set of all elements in X fixed by g, that is, $X^g = \{x \in X | gx = x\}$. We say that G acts transitively on X if for each pair $x, x' \in X$ there is $g \in G$ such that $x' = gx$.

A.8.2 *If G is a finite group acting on a finite set X, then*;

(*a*) *The orbits of G on X are disjoint and cover the set X and the number of elements in the orbit of $x \in X$ is equal to the index of the stabilizer of x in G, that is, $|Gx| = [G : G_x] = |G|/|G_x|$. Moreover, if $x' = hx$ for $h \in G$, then $G_{x'} = hG_xh^{-1}$. Thus, we have*

$$X = \bigcup_x Gx \quad \text{and} \quad |X| = \sum_x \frac{|G|}{|G_x|};$$

where x represent different orbits of G on X;

(*b*) (**Burnside's lemma**) *Denoting by $|G/X|$ the number of orbits of G on X, we have*

$$|G/X| = \frac{1}{|G|} \sum_{g \in G} |X_g|.$$

(*c*) *If X has p elements, where p is a prime and G acts transitively on X, then p divides the order of G.*

Proof. (a) It is clear that each element $x \in X$ belongs to an orbit (its own). Two different orbits are disjoint, since if $x \in Gx_1$ and $x \in Gx_2$ for some $x \in X$, then for any $x' \in Gx_1$, we have $x' = g'x_1$ and $x = g_1x_1 = g_2x_2$, that is, $x_1 = g_1^{-1}g_2x_2$, gives $x' = g'g_1^{-1}g_2x_2$, so $x' \in Gx_2$. Hence, we have $Gx_1 \subseteq Gx_2$. By symmetry, we also have the inclusion $Gx_2 \subseteq Gx_1$, which gives $Gx_1 = Gx_2$ (another argument is to use the fact that the orbits are equivalence classes of the relation $x \sim x'$ for $x, x' \in X$ declaring $x, x' \in X$ equivalent if and only if they belong to the same orbit – knowing this, we get that different orbits are disjoint, since different equivalence classes of an equivalence relation are disjoint). The number of elements in an orbit Gx is equal the number of different elements gx, where $g \in G$. Now $gx = g'x$ if and only if $g^{-1}g'x = x$, that is, $g^{-1}g' \in G_x$, which is equivalent to $g'G_x = gG_x$. Thus the number of different elements in Gx is equal to the number of cosets of G_x in G, that is, the index $[G : G_x]$ of G_x in G.

If $x' = hx$ for some $h \in G$, then

$$g \in G_{x'} \Leftrightarrow gx' = x' \Leftrightarrow ghx = hx \Leftrightarrow h^{-1}ghx = x \Leftrightarrow h^{-1}gh \in G_x \Leftrightarrow g \in hG_xh^{-1}.$$

(b) First note that

$$\sum_{g\in G}|X^g| = \sum_{x\in X}|G_x|,$$

since both these numbers are equal to the number of pairs $(g,x)\in G\times X$ such that $gx=x$ (imagine a "multiplication table" for multiplication of elements of G by the elements of X in which the intersection of the row g with the column x is gx and count the number of occurrences of $gx=x$ in two ways: by rows and by columns).

We have:

$$\sum_{g\in G}|X^g| = \sum_{x\in X}|G_x| = \sum_{x\in X}\frac{|G|}{|Gx|} = |G|\sum_{x\in X}\frac{1}{|Gx|}.$$

Now we observe that the last sum is simply the number of orbits, since each fraction $\frac{1}{|Gx|}$ appears as many times as the number of elements in the orbit of x, which means that each orbit contributes with 1 to this sum (the elements of X are distributed among all orbits which are disjoint and cover X). Thus

$$\sum_{g\in G}|X^g| = |G||G/X|,$$

which prove Burnside's lemma (which in reality was proved already by Cauchy and somewhat later by Frobenius).

(c) By our assumption, we have only one orbit $Gx=X$ for any $x\in X$, so by (a), we have $|Gx||G_x| = |G|$. Hence $p=|Gx|$ divides $|G|$. □

The formulae in A.8.2(a) is often used in the case of $X=G$ and the action of the group G is given by conjugation (that is, $g\cdot x = gxg^{-1}$). In this case, the equality

$$|G| = \sum_x \frac{|G|}{|G_x|}$$

is often called **class formulae**, since $\frac{|G|}{|G_x|} = [G:G_x] = |Gx|$ is the number of elements in the group G, which are conjugated to x. We use this formulae in such a way in Ex. 12.6. Notice that classes with only one element, that is, $|Gx|=1$ correspond to $G_x=G$, that is, they correspond to the case when $gxg^{-1}=x$ for every $g\in G$. These are the elements of the center $C(G)$ of G.

Very often, we consider $X=G$ and H is a subgroup of G acting by multiplication, say from the left. Then the orbit of $x\in G$ is the coset Hx and the formulae of **A.8.2**(a) is simply the splitting of G into the right cosets of H in G. We give a few important applications, which we use on different occasions in the exercises.

A.8.3 Cauchy's theorem. *Let G be a finite group whose order is divisible by a prime number p. Then the group G contains an element of order p.*

Proof. Consider the set X of all p-tuples $(g_1, g_2, \dots, g_p)$ such that $g_i \in G$ and $g_1 g_2 \cdots g_p = e$. The number of elements in X is of course n^p, where $n = |G|$.

Let $H = \langle\sigma\rangle$ be the cyclic group of order p generated by the permutation $\sigma = (1, 2, \dots, p)$ (the cycle of length p mapping $1 \mapsto 2 \mapsto \cdots \mapsto p \mapsto 1$). The group H acts on the set X, when the indices of $g_1, g_2, \dots, g_p$ are shifted one place to the right circularly (the last on the first): $\sigma(g_1, g_2, \dots, g_p) = (g_{\sigma(1)}, g_{\sigma(2)}, \dots, g_{\sigma(p)})$. In fact, if $g_1 g_2 \cdots g_p = e$, then $g_2 \cdots g_p g_1 = e$, since we can multiply the first equality by g_1^{-1} from the left and then by g_1 from the right.

If $x = (g_1, g_2, \dots, g_p) \in X$, then its orbit Hx contains p different elements unless all $g_1 = g_2 = \cdots = g_p$ when all shifts of x give the same element x, that is, the orbit Hx has only one element. We just want to show that there is $x = (g, g, \dots, g) \in X$ with $g \neq e$, that is, that the number of elements of X whose orbit has only one element is bigger than 1. Denote by r the number of orbits Hx of length 1 and by s the number of orbits Hx consisting of p elements.

According to **A.8.2**(a), the number of elements in X (n^p) is equal to the sum of the numbers of elements in all orbits. Thus $n^p = k + ps$. Since p divides the order n of the group G, the last equality shows that p divides k, so we really have $k > 1$. ■

We use also the formulae **A.8.2**(a) in the proof of the following theorem of Sylow, which has many applications also in Galois theory. Let G be a group anf p a prime number. If p divides the order of G and p^k is the highest power of p dividing it, then each subgroup of G of this order is called a p-Sylow subgroup of G. In general, a group whose order is a power of a prime p is called a **p-group**. The Sylow's subgroups play an important role and the main result about them is usually formulated as three Sylow's theorems (below (a), (b), (c)):

A.8.4 Sylow's Theorems *Let G be a finite group and p a prime number. Then*

(*a*) *G contains Sylow's subgroups;*

(*b*) *any two Sylow's subgroups of G are conjugated;*

(*c*) *the number n_p of p-Sylow's subgroups of of G divides their index and is congruent to 1 modulo p.*

Proof. (a) We use induction with respect to the order of G. If $|G| = 2$, then the group is cyclic of order 2 and the theorem is of course true. Assume that it is true for all groups of orders less than the order of a given group G. We prove (a) for G. Assume that G has proper subgroups, since otherwise it is a cyclic group of a prime order p and the theorem is automatically true for G (see **A.2.10**). Let p^k be the highest power of a prime number dividing the order of G. If G has a proper subgroup H of order divisible by p^k, then the theorem is true by induction, since a subgroup of H of order p^k is a subgroup of G of this order. Thus, assume that p^k does not divide the orders of all proper subgroups of G. Consider now the action of G by conjugation (so $X = G$, $H = G$ and $g \cdot x = gxg^{-1}$). As we noted

above, the stabilizer $G_x = \{g \in G \mid gxg^{-1} = x\}$ is the centralizer of the element $x \in G$. We know that $G_x = G$ (that is, G_x is not proper) if and only if x is in the center $C(G)$ of G. The class formulae of **A.8.2**(a) gives

$$|G| = \sum_x \frac{|G|}{|G_x|} = |C(G)| + \sum_x \frac{|G|}{|G_x|},$$

where in the sum to the right, we take only x representing the classes for which the group G_x is proper. Hence, the prime number p divides all terms $\frac{|G|}{|G_x|}$ for which G_x is a proper subgroup (since then $p^k \mid |G|$ and $p^k \nmid |G_x|$) and $\frac{|G|}{|G_x|} = 1$ each time x is in the center of G. Since p^k divides $|G|$ to the left, we get that p divides $|C(G)|$. Thus the order of $C(G)$ is divisible by p, which implies by Cauchy's theorem **A.8.3** that there is an element $g \in C(G)$ of order p. Hence the subgroup $\langle g \rangle$ has order p and is normal in G, since g is in the center of this group. The quotient group $G/\langle g \rangle$ has order $|G|/p$ less than the order of G and the highest power of p dividing this order is p^{k-1}. By the inductive assumption, the group $G/\langle g \rangle$ contains a subgroup of order p^{k-1}. Now the inverse image of this subgroup in G (see **A.2.8**) has order p^k, so it is a p-Sylow subgroup of G.

(b) Let H_1 and H_2 be two Sylow subgroups of a group G. We want to show that there is an element $x \in G$ such that $H_1 = xH_2x^{-1}$. Once again, we use the class formulae of **A.8.2**(a) but this time we choose $X = G$ and we act on X by the subgroup $H_1 \times H_2$ of $G \times G$ in the following way $(h_1, h_2)x = h_1 x h_2^{-1}$ for $(h_1, h_2) \in H_1 \times H_2$ and $x \in G$. It is easy to check that this definition really defines an action of $H_1 \times H_2$ on G:

$$((h_1, h_2)(h_1', h_2'))x = (h_1h_1', h_2h_2')x = (h_1h_1')x(h_2h_2')^{-1} = h_1(h_1'xh_2'^{-1})h_2^{-1} = (h_1, h_2)((h_1', h_2')x)$$

for $(h_1, h_2), (h_1', h_2') \in H_1 \times H_2$, $x \in G$ and, of course, $(e, e)x = x$ for the identity $(e, e) \in H_1 \times H_2$. The orbit of $x \in G$ is H_1xH_2 (this set is called double coset of H_1, H_2 in G). The isotropy group G_x of $x \in G$ consists of all (h_1, h_2) such that $h_1 x h_2^{-1} = x$, that is $h_1 = xh_2x^{-1}$. Such pairs (h_1, h_2) are exactly those belonging to the intersection $H_1 \cap xH_2x^{-1}$. Hence the number of elements in the orbit H_1xH_2 is equal

$$\frac{|H_1 \times H_2|}{|H_1 \cap xH_2x^{-1}|} = \frac{|H_1||H_2|}{|H_1 \cap xH_2x^{-1}|}$$

and the class formulae of **A.8.2**(a) says that

$$|G| = \sum_x \frac{|H_1||H_2|}{|H_1 \cap xH_2x^{-1}|},$$

where x represent different orbits of $H_1 \times H_2$ on G (double cosets). Now $|H_1||H_2|$ is divisible by $p^kp^k = p^{2k}$ and $|H_1 \cap xH_2x^{-1}|$ as a subgroup of H_1 is divisible by at most p^k. If

$H_1 \cap xH_2x^{-1}$ is a proper subgroup of H_1, then its order is at most p^{k-1}, which means that $\frac{|H_1||H_2|}{|H_1 \cap xH_2x^{-1}|}$ is divisible by at least $p^{2k-(k-1)} = p^{k+1}$. Since the order of G on the left is divisible exactly by p^k, we get a contradiction if all terms to the right are divisible by p^{k+1}. Hence it must be a term in which $H_1 \cap xH_2x^{-1}$ is not a proper subgroup of H_1, that is, it must exist $x \in G$ such that $H_1 = xH_2x^{-1}$.

(c) Since all Sylow p-subgroups H of G are conjugated, the number of different such groups is equal to the index of the normalizer $\mathcal{N}(H)$ in G (see p.227) (in fact, we have $xHx^{-1} = x'Hx'^{-1}$ if and only if $x^{-1}x'H = Hx^{-1}x'$, that is, $x^{-1}x' \in \mathcal{N}(H)$, which is equivalent to $x'\mathcal{N}(H) = x\mathcal{N}(\mathcal{H})$). Thus the number of Sylow's p-subgroups divides the order of G. Now in order to prove that this number is equal to 1 modulo p, we use the same action on G as in (b) and choose $H_1 = H_2 = H$ in (b). Since we want to find the number of Sylow's subgroups, which is equal to the index of $\mathcal{N}(H)$ in G, we have to find the quotient $|G|/|\mathcal{N}(H)|$. According to the class formula in (b), we have:

$$|G| = \sum_x \frac{|H||H|}{|H \cap xHx^{-1}|},$$

and we split the sum in those terms which correspond $x \in \mathcal{N}(H)$ and those for which $x \notin \mathcal{N}(H)$ (notice that $H \subseteq \mathcal{N}(H) \subseteq G$). In the first case, we have $xHx^{-1} = H$ so the term is equal $|H|$. The number of such terms is equal to the index of H in $\mathcal{N}(H)$, so this first sum is simply the order $|\mathcal{N}(H)|$. As in (b), each term $\frac{|H||H|}{|H \cap xHx^{-1}|}$ of the second type is divisible by p^{k+1} (since $H \cap xHx^{-1}$ is proper subgroup of H of order p^k and the nominator is $|H|^2 = p^{2k}$). Hence the sum of the terms of the second type is $p^{k+1}m$ for an integer m. Thus $|G| = |\mathcal{N}(H)| + p^{k+1}m$, which gives the number od Sylow's p-groups:

$$\frac{|G|}{|\mathcal{N}(H)|} = 1 + \frac{p^{k+1}m}{|\mathcal{N}(H)|} = 1 + pm'$$

for en integer m', since the number $\frac{p^{k+1}m}{|\mathcal{N}(H)|}$ is an integer (as a difference of two integers) and it must be divisible by p, since the order of $\mathcal{N}(H)$ as a subgroup of G is at most divisible by p^k. This proves that the number of Sylow's p-subgroups of G equals 1 modulo p. □

A.9 Permutations

If a set X is finite, the bijective functions on it are usually called permutations of X. The most common case is $X = \{1, 2, \ldots, n\}$ when $\mathcal{B}(X)$ (see **A.8**) is denoted by S_n and called the symmetric group. The order of S_n is $n!$. Thus a permutation of $1, \ldots, n$ is a bijective function $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$, which is sometimes denoted by

$$\sigma = \begin{pmatrix} 1 & \ldots & n \\ i_1 & \ldots & i_n \end{pmatrix},$$

when $\sigma(k) = i_k$ for $k = 1, \ldots, n$. Permutations can be conveniently denoted as a product of cycles. A cycle is a permutation such that for a subset $\{i_1, \ldots, i_k\}$ of $X_n = \{1, \ldots, n\}$, we have $\sigma(i_1) = i_2, \sigma(i_2) = i_3, \ldots, \sigma(i_k) = i_1$ and $\sigma(i) = i$ for $i \notin \{i_1, \ldots, i_k\}$. An arbitrary permutation σ can be written as a composition of cycles, since we can start with 1, take its image, the image of the image and so on. Finally, we have to return to 1 (if not from the beginning, we have $\sigma(1) = 1$). In this way, we get a cycle starting with 1. If all $1, \ldots, n$ are in the cycle, then σ is a cycle. Otherwise, we start with the least number, which is not in the cycle starting with 1 and construct a second cycle, which is disjoint from the first one. We continue the process so that every number is in a cycle. Notice that we usually omit the cycles of length 1, that is, those corresponding to $\sigma(i) = i$, but we denote by (1) the cycle corresponding to the unit (essentially, the unit is a composition of n cycles (i) for $i = 1, \ldots, n$). For example:

$$\sigma = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8 \\ 4\,7\,8\,5\,1\,6\,2\,3 \end{pmatrix} = (1,4,5)(2,7)(3,8).$$

The cycle permutations have many pleasant properties, which are important in studying of the permutation groups. We record the following useful facts:

A.9.1 (*a*) *If $\sigma \in S_n$ and $\tau = (a_1, \ldots, a_k) \in S_n$, then $\sigma\tau\sigma^{-1} = (\sigma(a_1), \ldots, \sigma(a_k))$.*

(*b*) *All cycles in S_n having the same length are conjugated.*

Proof. (a) Denote $\varrho = \sigma\tau\sigma^{-1}$. We have to show that $\varrho(\sigma(a_1)) = \sigma(a_2), \ldots, \varrho(\sigma(a_k)) = \sigma(a_1)$ and for every $a \neq \sigma(a_i)$, where $i = 1, \ldots, k$, we have $\varrho(a) = a$.

We check simply that $\varrho(\sigma(a_1)) = \sigma\tau\sigma^{-1}(\sigma(a_1)) = \sigma(\tau(a_1)) = \sigma(a_2)$ and, in general, $\varrho(\sigma(a_i)) = \sigma\tau\sigma^{-1}(\sigma(a_i)) = \sigma(\tau(a_i)) = \sigma(a_{i+1})$ for $i = 1, \ldots, k$, when the addition of these indices i is performed modulo k.

If $a \neq \sigma(a_i)$, then of course, $\sigma^{-1}(a) \neq a_i$ for all $i = 1, \ldots, k$, that is, τ does not move $\sigma^{-1}(a)$. Hence, we have $\varrho(\sigma(a)) = \sigma\tau\sigma^{-1}(a) = \sigma(\tau(\sigma^{-1}(a))) = \sigma(\sigma^{-1}(a)) = a$, that is, ϱ doesn't move a.

(b) Take two cycles of the same length $(a_1, \ldots, a_k)$ and $(b_1, \ldots, b_k)$. Choose a permutation $\sigma \in S_n$ such that $\sigma(a_i) = b_i$ for $i = 1, \ldots, k$ and σ is any bijection from the set $a \neq a_i$ on the set of $b \neq b_i$ Then, it follows from (a) that $\sigma(a_1, \ldots, a_k)\sigma^{-1} = (b_1, \ldots, b_k)$. ■

A permutation σ of $X = \{1, 2, \ldots, n\}$ is called even if for even number of pairs $i, j \in X$ such that $i < j$, we have $\sigma(i) > \sigma(j)$ (this number may be 0). Observe that we have $\binom{n}{2} = \frac{n(n-1)}{2}$ such pairs. The even permutations of X form a subgroup of S_n called the alternating group, which is denoted by A_n. Its index in S_n is 2, that is, its order is $n!/2$. Among many possible proofs of this, we choose an argument, which is useful in Chapter 15.

As we know, the group S_n acts on the set $X = R[X_1, \ldots, X_n]$ (R any ring) of polynomials in variables $X_1, \ldots, X_n$ by the formula: $\sigma(f(X_1, \ldots, X_n)) = f(X_{\sigma(1)} \ldots, X_{\sigma(n)})$.

Consider the following polynomial (the discriminant of $X_1, \ldots, X_n$) as an element of $\mathbb{Z}[X_1, \ldots, X_n]$:

$$\Delta(X_1, \ldots, X_n) = \prod_{1 \le i < j \le n} (X_i - X_j).$$

It has as many factors as the number of pairs i, j such that $i < j$. Consider $\sigma(\Delta(X_1, \ldots, X_n)) = \Delta(X_{\sigma(1)} \ldots, X_{\sigma(n)})$ for a permutation $\sigma \in S_n$. This polynomial has also $X_i - X_j$ as its factors but each time $\sigma(i) > \sigma(j)$, the corresponding factor $X_{\sigma(i)} - X_{\sigma(j)}$ in $\sigma(\Delta(X_1, \ldots, X_n))$ differs by sign from the factor $X_{\sigma(j)} - X_{\sigma(i)}$, which appears in $\Delta(X_1, \ldots, X_n)$. Hence a permutation σ is even if and only if $\sigma(\Delta) = \Delta$ and odd if and only if $\sigma(\Delta) = -\Delta$. If σ, τ are two even permutations, then $\sigma\tau(\Delta) = \sigma(\tau(\Delta)) = \Delta$, which shows that the even permutations form a group. Recall that is denoted by A_n. We have also that if both σ, τ are odd, then $\sigma\tau(\Delta) = \sigma(\tau(\Delta)) = \sigma(-\Delta) = \Delta$, so $\sigma\tau$ is an even permutation, that is, $\sigma\tau \in A_n$. This property implies that A_n has index 2 in S_n, that is, the subgroup A_n has two cosets in S_n: one is A_n and the second is σA_n for any odd permutation σ (for example $\sigma = (1, 2)$). In fact, if τ is also odd, then $\sigma A_n = \tau A_n$, since $\sigma^{-1}\tau \in A_n$ as a product of two odd permutations ($\sigma^{-1} \notin A_n$, since $\sigma \notin A_n$ as A_n is a subgroup). Thus the number of elements in A_n is half of the number of elements in S_n, that is, it is $n!/2$.

A.9.2 *The group A_n is the only subgroup of S_n having index 2.*

Proof. Let H be a subgroup of index 2 in S_n. We claim that all transpositions (a, b) are not in H. In fact, the subgroup H is normal in S_n as a subgroup of index 2. If a transpositions $t = (a, b) \in H$, then every other transposition is also in H, since it is conjugated to t. But the transpositions generate the whole group S_n, so we would have $H = S_n$, which is not true. Now a product of two elements which are not in H is an element belonging H, since H has index 2 in S_n. Thus any product of two transpositions is in H. But any even permutation is a product of even number of transpositions, so it is an element of H. Thus $A_n \subseteq H$, which means that $H = A_n$, since these groups have the same order. ■

A.9.3 Cayley's theorem. *Every group G can be embedded into a permutation group S_n. It is always possible to choose n as a prime number.*

Proof. Notice that the group S_n can be embedded into any group S_N, where $N \ge n$. For example S_n can be regarded as all permutations of the first n numbers among $1, \ldots, n, \ldots, N$. In particular, one may choose N as a prime number (see an application of this in Ex. 9.15).

A.9.4 *The group S_n is generated by the cycle $\sigma = (1, 2, \ldots, n)$ and the transposition $\tau = (1, 2)$.*

Proof. Let H be a subgroup of S_n generated by σ and τ. For $1 \le k \le n - 2$, we have $\sigma^k(1) = k + 1$ and $\sigma^k(2) = k + 2$. Hence $\sigma^k\tau\sigma^{-k} = (k + 1, k + 2)$. Thus the subgroup H contains all transpositions of any two consecutive numbers among $1, 2, \ldots, n$. But any

permutation in S_n can be obtained as a product of such transpositions (it is possible to get any permutation $a_1, \ldots, a_n$ from $1, \ldots, n$ by a chain of transpositions of two adjacent numbers). □

A.10 Some arithmetical functions

An arithmetical function is any function from the positive integers $\mathbb{N}$ to complex numbers. In this book, there are two functions which appear in many contexts: the Euler (totient) function φ and the Möbius function μ.

Arithmetical functions form a ring under usual addition and multiplication of functions: $(f+g)(n) = f(n) + g(n)$ and $(fg)(n) = f(n)g(n)$. But much more interesting is another structure of a ring on the set of arithmetical functions which takes into consideration the divisibility relation in the ring $\mathbb{Z}$. It is called Dirichlet convolution and is defined in the following way:

$$(f \star g)(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right) = \sum_{ab=n} f(a)g(b),$$

where the first sum is over all positive divisors of n, and the second, over all pairs a, b of positive divisors of n such that $ab = n$ (the last equality is only a change of the notation $d = a, b = n/d$). It is clear that the convolution is commutative, but possibly, the reader would like to write down the formulae showing the associativity and the distributivity of multiplication with respect to addition. Both are easy to check and the associativity follows immediately by showing that both $((f \star g) \star h)(n)$ and $(f \star (g \star h))(n)$ are equal to $\sum_{abc=n} f(a)g(b)h(c)$, where the sum is over all triples (a, b, c) of positive integers such that $abc = n$. The ring of arithmetical functions with addition of functions and the Dirichlet convolution as multiplication is often called the Dirichlet ring. It has identity ε defined by $\varepsilon(1) = 1$ and $\varepsilon(n) = 0$ when $n \neq 1$. In fact, $(\varepsilon \star f)(n) = \sum_{ab=n} \varepsilon(a)f(b) = f(n)$, since only the term corresponding to $a = 1, b = n$ matters. Notice that an arithmetical function f has an inverse in the Dirichlet ring, that is, there is an arithmetical function g such that $f \star g = \varepsilon$ if and only if $f(1) \neq 0$. In fact, if $f \star g = \varepsilon$, then $(f \star g)(1) = f(1)g(1) = 1$, which shows that $f(1) \neq 0$. Conversely, if $f(1) \neq 0$, then we can find the function g inductively (it is unique, if it exists since the units in every ring form a group) in the following way. First we find $g(1)$ solving the equation $f(1)g(1) = 1$. When this is done and we already have $g(k)$ for $k < n$, then we take the required equality $(f \star g)(n) = \sum_{ab=n} f(a)g(b) = \varepsilon(n) = 0$ when $n > 1$. In this equality, we know all the values of g for $b < n$ and the only value, we have to find is the one corresponding to the term $f(1)g(n)$. Since $f(1) \neq 0$, we can compute $g(n)$ using this equality.

An arithmetical function f is called **multiplicative** if $f(ab) = f(a)f(b)$ when a, b are relatively prime, that is, the only common positive divisor of both these numbers is 1. In other words, the greatest common divisor $\gcd(a, b) = 1$.

Recall that the Möbius function $\mu(n)$ is the arithmetical function defined in the following way: $\mu(1) = 1$, $\mu(n) = 0$ if n is divisible by a square of a prime number and $\mu(n) = (-1)^k$, when n is a product of k different prime numbers. Since $\mu(1) = 1$, the Möbius function has an inverse with respect to the convolution, that is, there is a unique arithmetic function f such that $\mu \star f = \varepsilon$. Computing a few values of f (as we did in general case above), there is an evident guess that $f = \mathbf{1}$, where $\mathbf{1}$ is defined by $\mathbf{1}(n) = 1$ for every positive integer n. We record this and give a proof:

A.10.1 (*a*) *The Möbius function is multiplicative.*

(*b*) *We have* $\mathbf{1} \star \mu = \varepsilon$, *that is,*

$$\mathbf{1} \star \mu(1) = \mu(1) = 1 \quad \text{and} \quad (\mathbf{1} \star \mu)(n) = \sum_{d|n} \mu(d) = 0 \quad \text{for } n > 1$$

Proof. (a) If a is divisible by k different primes and b by l different primes, then ab is divisible by $k + l$ primes. Hence, if $\gcd(a, b) = 1$, then $\mu(ab) = \mu(a)\mu(b)$ since both sides are equal either 0 (if a or b is divisible by a square of a prime) or $(-1)^{k+l}$ (if both a and b are square free).

(b) We check immediately that $(\mathbf{1} \star \mu)(1) = 1$ and for $n > 1$, we obtain:

$$(\mathbf{1} \star \mu)(n) = \sum_{d|n} \mu(d) = 1 + \sum_{p_{i_1} \cdots p_{i_k} | n} (-1)^k = 1 + \sum_{k=1}^{r} (-1)^k \binom{r}{k} = (1-1)^r = 0,$$

where $p_1 < \ldots < p_r$ are all different prime numbers dividing n and the sum is over all possible products of k of these primes for $k = 0, 1, \ldots, r$ with $i_1 < \ldots < i_k$. The term 1 corresponds to $d = 1$ (no primes in d, so $k = 0$), any remaining d contains at least one prime number. It is possible to argue in many different ways in order to check that $\mathbf{1} \star \mu(n) = 0$ when $n > 1$. For example, we note that there are r summands containing only one prime and they contribute with r summands equal -1. Then there $\binom{r}{2}$ products of 2 primes (contributing as many summands 1), $\binom{r}{3}$ products of 3 primes (contributing as many summands -1) and so on. This gives the expression of the sum as a sum of binomial coefficients with shifting signs depending on the number of primes in a divisor of n – even numbers of primes give 1, and odd numbers of primes in d give -1. ■

Using the Möbius function, it is possible to prove one of the fundamental properties of arithmetic functions, which we use on several occasions in the exercises:

A.10.2 Möbius inversion formula. *If f is an arithmetic function and*

$$g(n) = \sum_{d|n} f(d),$$

then

$$f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right).$$

Proof. The theorem says that if $g = \mathbf{1} \star f$, then $f = \mu \star g$, but this is evident, since $\mu \star \mathbf{1} = \varepsilon$, so $f = \varepsilon \star f = \mu \star \mathbf{1} \star f = \mu \star g$. □

In Chapter **10**, we use a multiplicative version of Möbius formula. Such a form sometimes follows immediately from **A.10.2** by replacing $f(n)$ and $g(n)$ by $\log f(n)$ and $\log g(n)$ (when these numbers are defined). But what we really need is a more general form of Möbius inversion:

A.10.3 Multiplicative Möbius inversion formula. *If $f : \mathbb{N} \to G$ is a function, where G is an abelian group (in multiplicative notation), then*

$$g(n) = \prod_{d|n} f(d),$$

then

$$f(n) = \prod_{d|n} g\left(\frac{n}{d}\right)^{\mu(d)}.$$

Proof. In the proof, we prefer the additive notation in G (for typographical reasons). We have:

$$\sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \sum_{m|\frac{n}{d}} f(m) = \sum_{md|n} \mu(d) f(m) = \sum_{m|n} f(m) \sum_{d|\frac{n}{m}} \mu(d).$$

But the last sum is 0 if $n/m > 1$ according to **A.10.1** and it is equal to 1, when $n/m = 1$, that is, when $m = n$, so the right hand side is equal $f(n)$. ■

The Möbius function is multiplicative, that is, $\mu(ab) = \mu(a)\mu(b)$ whenever a, b are relaatively prime. In fact, if there is a prime number p such that $p^2 \mid ab$, then p^2 divides a or b since these numbers are relatively prime. Thus both the left hand side $\mu(ab)$ and the right hand side $\mu(a)\mu(b)$ are equal to 0. If no square divides the product ab, then $a = p_1 \cdots p_k$ and $b = q_1 \cdots q_l$, where all p_i, q_j are different prime numbers. Hence by the definition of the Möbius function, we have $\mu(a)\mu(b) = (-1)^k(-1)^l = (-1)^{k+l} = \mu(ab)$.

Recall that **Euler's totient function** (or simply **Euler's function** when only this one is considered) φ is an arithmetic function such that $\varphi(n)$ equals the number of $1 \leq k \leq n$ such that $\gcd(k, n) = 1$. Those properties of the Euler function, which we use are gathered in the following theorem:

A.10.4 *(a) The Euler function is multiplicative. More exactly, we have $\varphi([a, b])\varphi((a, b)) = \varphi(a)\varphi(b)$;*

(b) If $n = p_1^{a_1} \cdots p_k^{a_k}$ is presentation of n as a product of prime numbers p_i for $i = 1, \ldots, k$, then

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\cdots\left(1 - \frac{1}{p_k}\right);$$

(*c*) *We have* $\sum_{d|n} \varphi(d) = n$, *that is,* $\mathbf{1} \star \varphi = Id$;

Proof. (a) By **A.3.7**, we have a group isomorphism $\mathbb{Z}_{ab} \cong \mathbb{Z}_a \times \mathbb{Z}_b$ (the residue of n modulo ab is mapped onto the pair of residues of n modulo a and b). The last isomorphism is in fact also a ring isomorphism, which is easy to check taking the products of the residues. Thus taking the invertible elements in the rings on both sides, we get an isomorphism $\mathbb{Z}_{ab}^* \cong \mathbb{Z}_a^* \times \mathbb{Z}_b^*$. As we know (see p.231), $\varphi(n) = |\mathbb{Z}_n^*|$ is the number of invertible elements in the ring $\mathbb{Z}_n$. Hence, we have $\varphi(ab) = |\mathbb{Z}_{ab}^*|$, $\varphi(a) = |\mathbb{Z}_a^*|$, $\varphi(b) = |\mathbb{Z}_b^*|$, so $\varphi(ab) = \varphi(a)\varphi(b)$.

(b) Since φ is mutiplicative, it is sufficient to show that $\varphi(p^a) = p^a\,(1 - 1/p) = p^a - p^{a-1}$ when p is a prime. But among p^a numbers from 1 to p^a, those which are not relatively prime to p^a are exactly those divisible by p and their number is $p^a/p = p^{a-1}$. Thus the number of those, which are relatively prime to p is $p^a - p^{a-1}$.

(c) There are many different proofs of the equality. We use an argument related to convolution on arithmetic functions. The formula in (b) can be easily expressed in terms of the Möbius function, since multiplying the factors $1 - 1/p_i$ on the right hand side, we get all possible terms of the type $\frac{\mu(d)}{d}$, where $d = p_{i_1}\cdots p_{i_r}$ is a divisor of n containing r different prime numbers dividing n for $r = 0, 1, \ldots, k$. Only such factors contribute nonzero terms to the sum on the right hand side in

$$\frac{\varphi(n)}{n} = \left(1 - \frac{1}{p_1}\right)\cdots\left(1 - \frac{1}{p_k}\right) = \sum_{d|n} \frac{\mu(d)}{d}.$$

But this equality says simply that $\varphi(n) = \sum_{d|n} \frac{n}{d}\mu(d) = (Id \star \mu)(n)$. Since $\mathbf{1}$ is the inverse of μ, we multiply both sides of the equality $\varphi = Id \star \mu$ by $\mathbf{1}$ and obtain the required equality $\mathbf{1} \star \varphi = Id$. □

A.11 Symmetric polynomials

A polynomial $f(X_1, \ldots, X_n) \in R[X_1, \ldots, X_n]$ over a ring R is called symmetric if it is unchanged by any permutation of its variables $X_1, \ldots, X_n$. This can be expressed in terms of the group action of the symmetric group S_n on the ring of polynomials: $\sigma(f(X_1, \ldots, X_n)) = f(X_{\sigma(1)} \ldots, X_{\sigma(n)})$. The polynomial f is symmetric if and only if $\sigma(f) = f$ for all $\sigma \in S_n$. The **elementary symmetric polynomials** are the polynomials $s_1 = X_1 + \cdots + X_n$, $s_2 = X_1X_2 + X_1X_3 + \cdots + X_{n-1}X_n, \ldots, s_n = X_1X_2\cdots X_n$. They are the the coefficients of the general polynomial of degree n:

$$(*) f(T) = \prod_{i=1}^{n}(T - X_i) = T^n - s_1T^{n-1} + s_2T^{n-2} + \cdots + (-1)^{n-1}s_{n-1}T + (-1)^n s_n$$

The following result has many applications in Galois theory:

A.11.1 Fundamental theorem on symmetric polynomials *If R is a (commutative) ring and $f(X_1, \ldots, X_n) \in R[X_1, \ldots, X_n]$ is a symmetric polynomial, then there is a polynomial $g \in R[X_1, \ldots, X_n]$ such that $f(X_1, \ldots, X_n) = g(s_1, \ldots, s_n)$.*

Thus the fundamental theorem on symmetric polynomials says that every symmetric polynomial is a polynomial of the elementary symmetric ones. The idea of the usual proof of this statement using mathematical induction with respect to the degree of the polynomial is very simple, but its formulation needs careful definition of an ordering of monomials, which we omit here (see e.g. [L], Chap.IV,§6). Such a proof gives a possibility to effectively find a polynomial g for a given polynomial f.

A.11.2 Discriminant of a polynomial. Let $\alpha_1, \ldots, \alpha_n$ be the zeros of a polynomial $f(X) = X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n \in K[X]$ in a splitting field L of $f(X)$ over K. The **discriminant** of $f(X)$ is then

$$\Delta(f) = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2.$$

We have $a_i = (-1)^i s_i$, where s_i are evaluated for $X_k = \alpha_k$, $k = 1, \ldots, n$. It is easy to see that the permutations of $\alpha_1, \ldots, \alpha_n$ do not affect the discriminant – it is fixed by all permutations in the group S_n. Since the Galois group $G(L/K)$ considered as a permutation group is a subgroup of S_n, this property of $\Delta(f)$ implies that it is an element of the field K (see **T.9.1**(b) and Ex. 9.23).

It is also possible to prove that $\Delta(f) \in K$ using a somewhat different argument applied to the "general discriminant"

$$\Delta(f(T)) = \prod_{1 \le i < j \le n} (X_i - X_j)^2 \in \mathbb{Z}[X_1, \ldots, X_n]$$

defined by the general equation above. The discriminant $\Delta(f(T))$ is a symmetric polynomial of $X_1, \ldots, X_n$. According to the main theorem on symmetric polynomials, there is a polynomial $g \in \mathbb{Z}[X_1, \ldots, X_n]$ such that $\Delta(f(T)) = g(s_1, \ldots, s_n)$. If now $f(X) \in K[X]$ and L is a splitting field of $f(X)$ over K, then $f(X) = \prod_{i=1}^{n}(X - \alpha_i)$, where $\alpha_i \in L$. If we replace X_i by α_i in $g(s_1, \ldots, s_n)$, we get $\Delta(f) = \prod_{1 \le i < j \le n}(\alpha_i - \alpha_j)^2 = g(a_1, \ldots, a_n) \in K$. (Formally, we take a homomorphism of $\mathbb{Z}[X_1, \ldots, X_n]$ onto $\mathbb{F}[\alpha_1, \ldots, \alpha_n]$, where $\mathbb{F}$ is the simple subfield of K.)

In this book, we use the polynomial g mainly for $n = 2, 3, 4$. For $n = 2$, see p.2, and for $n = 3$ see p.163. Already for $n = 4$, it is a little laborious to compute. In Maple, it is possible

to get the discriminant using the command `>discrim(f(T),T)`, where T is the variable in the polynomial $f(T)$. For $n = 4$, we gave the expression of $\Delta(f)$ by the coefficients on p.79.

A.12 Roots of unity

Roots of unity are complex numbers which are solutions of the equations $X^n = 1$ for $n = 1, 2, \ldots$. We meet these numbers in many places in this book, so let us recall some of their properties.

All complex solutions of the equation $X^n = 1$, that is, all n-th roots of 1 form a group of order n. This group (often denoted by U_n or C_n) is cyclic and consists of the numbers $\varepsilon_k = e^{\frac{2\pi ik}{n}} = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}$ for $k = 0, 1, \ldots, n-1$ (in fact, we know that every finite subgroup of a field is cyclic by **A.4.2**, so it is just a good illustration of this fact). This cyclic group has $\varphi(n)$ generators given by ε_k for k relatively prime to n (see **A.2.2**). A usual choice of a generator is ε_1 for which we have $\varepsilon_k = \varepsilon_1^k$ according to de Moivre's formula.

A.13 Transitive subgroups of permutation groups

As a permutation group, the Galois group $G(K_f/K)$ of an irreducible polynomial $f(X) \in K[x]$ is transitiv. A permutation group $G \subseteq S_n$ is called **transitive** if for any pair $i, j \in \{1, 2, \ldots, n\}$ there is a permutation $\sigma \in G$ such that $\sigma(i) = j$. This property is valid for Galois groups of irreducible polynomials, since by Ex. 7.4(a) there is always an automorphism which maps any given zero of $f(X)$ onto any other zero of this polynomial.

The symmetric group S_3 of all permutations of $1, 2, 3$ consists of $3! = 6$ elements. We can represent each permutation as an isometry of the plane mapping the equatorial triangle with vertices in the points 1, 2, 3 on itself. If $\{a, b, c\} = \{1, 2, 3\}$, then there are 3 rotations: the identity (1), the rotations $\pm 120^0$: $(1, 2, 3)$, $(1, 3, 2)$ and 3 symmetries in the three heights of the triangle: $(1, 2), (2, 3), (1, 3)$. There are only two transitive subgroups of S_3: the group S_3 itself and the subgroup of the rotations (all even permutations) $A_3 = \{(1), (1, 2, 3), (1, 3, 2)\}$. All these facts are very easy to check (e.g. by listing all the subgroups of S_3).

The symmetric group S_4 of all permutations of $1, 2, 3, 4$ consists of $4! = 24$ elements. We can represent each permutation as an isometry of the space mapping the tetrahedron with vertices in the points 1, 2, 3, 4 on itself. If $\{a, b, c, d\} = \{1, 2, 3, 4\}$, then each non-identity permutation can be written as a cycle or a composition of them:

6 symmetries (a, b) of order 2: in the planes through the vertices c, d and the middle of the side between a and b;

8 rotations (a, b, c) of order 3: around the axis through the vertex d perpendicularly to the plane through the points a, b, c;

3 rotations $(a, b)(c, d)$ of order 2: 180 degrees around the axis through the middles of the sides a, b and c, d. Notice that these rotations together with the identity (1) form a transitive

group of order 4. It is a transitive presentation of Klein's four group, which is usually denoted by V_4, that is,

$$V_4 = \{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}.$$

6 cycles (a,b,c,d) of order 4: compositions of the rotation (a,b,c) with the symmetry (c,d).

Together with the identity (1), we have 24 possible isometric mappings of the tetrahedron on itself. Notice that the even permutations are exactly the 12 rotations, and the odd permutations are the 6 symmetries and the 6 compositions of a rotation of order 3 and a symmetry.

Now observe that a every transitive subgroup of S_4 has at least 4 elements. As its order divides 24, the allowed orders are 4, 6, 8, 12, 24. Of course, S_4 and A_4 are transitive. By **A.9.2**, the even permutations A_4 are the only subgroup of S_4 of order 12.

In order to describe all transitive subgroups of S_4, notice that in any subgroup G, which contains at least one odd permutation σ, the half of the elements are odd permutations, and the other half are even. In fact, if G_0 denotes all even permutations in G, then G_0 is a (normal) subgroup of G and $G = G_0 \cup \sigma G_0$, since every permutation τ in G is either even or, if it is odd, then $\sigma^{-1}\tau$ is even (that is, in G_0).

The group S_4 has 3 subgroups of order 8. All are isomorphic with the square group D_4 and are transitive. In order to prove this, assume that G is a subgroup of order 8. Then it must consist of both even and odd permutations – all can not be even, since a group of order 8 can not be a subgroup of a group of order 12. The subgroup G_0 of G consisting of the even permutations (that is, rotations of the tetrahedron) must be $G_0 = V_4$, since all the remaining rotations have order 3 (can not belong to a group of order 4). The odd permutations in G can not all be of order 2. Those are exactly the symmetries of the tetrahedron. Among 4 such symmetries, there are at least 2 which shift the same vertex (of four possible), that is, they have form (a,b) and (a,c). Then the group G contains $(a,b)(a,c) = (a,c,b)$, which as an element of order 3. This order is not allowed by G. Thus G must contain an odd permutation σ of order 4. An easy direct computation shows that there are exactly 3 possibilities for σV_4, which give 3 possibilities for G:

$$D_4 = V_4 \cup \{(1,2,4,3), (1,3,4,2), (1,4), (2,3)\},$$

$$D_4' = V_4 \cup \{(1,2,3,4), (1,4,3,2), (1,3), (2,4)\},$$

$$D_4'' = V_4 \cup \{(1,3,2,4), (1,4,2,3), (1,2), (3,4)\}.$$

It is clear that these groups are transitive. Each group gives a description of all isometries of a square corresponding to a numbering of its vertices a,b,c,d according to the rotations of square given by the elements of order 4 belonging to it. Notice that the groups D_4, D_4', D_4''

are all isomorphic. They consist of all isometries of a square corresponding to a numbering of its vertices a, b, c, d (according to the rotations given by the elements of order 4 belonging to it). Recall that such a group contains 3 subgroups of order 4: V_4 (the rectangle group), the cyclic group of the rotations of the square:

$$C_4 = \{(1), (a, b, c, d), (a, d, c, b), (a, c)(b, d)\}$$

and a non-transitive representation of Klein's four group (the romb group):

$$V_4' = \{(1), (a, b), (c, d), (a, b)(c, d)\}.$$

There are no transitive subgroups G of S_4 of order 6. In fact, such a subgroup can not be cyclic, since there are no elements of order 6 in S_4. Thus it must be isomorphic to S_3. As we know such a group has 3 elements of order 2 and 2 elements of order 3. Among the elements of order 2 at least 2 must be symmetries (otherwise V_4 is a subgroup of G, which is impossible). They must shift a common vertex a. Otherwise, they are of the form $(a, b), (c, d)$ with different a, b, c, d. Then $(1), (a, b), (c, d), (a, b)(c, d)$ is a subgroup of G, which is impossible. If (a, b) and (a, c) are in G, then it is easy to check that G is the group of all permutations of a, b, c. It is not transitive on the set $\{1, 2, 3, 4\}$.

Any subgroup of order 4 is either cyclic or isomorphic to Klein's four group. A cyclic group of order 4 is generated by an element of order 4, which is a cycle (a, b, c, d). Of course, such a subgroups is transitive (since there are 6 such cycles and a any cyclic group of order 4 has two of them, there are 3 cyclic subgroups of order 4).

Finally, there is only one transitive subgroup of order 4 isomorphic to the group V_4. In fact, a non-cyclic subgroup of order 4 must contain 3 elements of order 2. A similar argument to that given above in connection with the subgroups of order 6 shows that it is impossible to get a transitive group with two symmetries. Thus we can only have the rotations giving V_4.

Summarizing, we have the following list of isomorphism types of transitive subgroups of S_4:

$$S_4, A_4, D_4, C_4, V_4.$$

We do not prove that the group S_5 has following 5 types of transitive subgroups :

$$S_5, A_5, G_5, D_5, C_5.$$

The order of every transitive subgroup must be divisible by 5 according to **A.8.2(d)**, so the allowed orders of transitive subgroups are $5, 10, 15, 20, 30, 60, 120$. As we know by **A.9.2**, the subgroup A_5 is the only one of order 60. It is not too difficult to exclude the orders 15 and 30 as orders of subgroups of S_5. A subgroups of order 5 are the cyclic groups of this order generated by cycles (a, b, c, d, e) of length 5. These are of course transitive and often denoted by C_5 (there are 6 such subgroups). Numbering the vertices of a regular pentagon and taking all the symmetries of it, we get a subgroup of S_5 of order 10, which is usually denoted by

D_5 and called the dihedral group (of order 10). These are all subgroups of order 10 in S_5 and they are transitive (each contains 4 cycles of length 5 and there 6 different subgroups of this type). Finally there are transitive subgroups of order 20 denoted by G_5 (sometimes by $GA(1,5)$ or F_{20} and called general affine group of order 20). They can be represented over the field $\mathbb{F}_5$ as affine transformations $f(x) = ax + b$, $a \in \mathbb{F}_5^*$, $b \in \mathbb{F}_5$ (replacing 0 by 5 in $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$, we get a corresponding permutation in S_5, for example, the mapping $f(x) = x + 1$ gives $(1, 2, 3, 4, 5)$ and $g(x) = 2x$ gives $(1, 2, 4, 3)$). There are 6 subgroups of S_5 of this type (and each contains one of the subgroups of type D_5, and this one contains one of type C_5).

The knowledge of transitive subgroups of S_n is used in computer programs in order to find Galois groups of (irreducible) polynomials. For example, in Pari/GP it is possible for irreducible polynomials up to degree 11 (in 2014).

A.14 Zorn's Lemma

A relation $\leq$ on a set X is called a **partial ordering** if for $x, y, z \in X$, we have

(a) $x \leq x$;

(b) $x \leq y$ and $y \leq z$ imply $x \leq z$;

(c) $x \leq y$ and $y \leq x$ imply $x = y$.

When $x \leq y$, then we also write $y \geq x$.

A typical example is the set of real numbers $\mathbb{R}$ (or any of its subsets) with the usual relation $\leq$. Another common example is the set $\mathcal{S}(M)$ of all subsets of a set M with the inclusion $\subseteq$ as the relation $\leq$.

If X is a set with a partial ordering $\leq$, then we say that an element $x^* \in X$ is **maximal** if the relation $x^* \leq x$ for $x \in X$ implies that $x = x^*$. An element $y_0 \in X$ is called an upper bound for a subset Y of X if $y \leq y_0$ for all $y \in Y$. A subset Y of X is called a **chain** if for any two elements $y_1, y_2 \in Y$, we have $y_1 \leq y_2$ or $y_2 \leq y_1$.

A.14.1 Zorn's Lemma. *Let X be a nonempty partially ordered set. If every chain in X has an upper bound, then there exists a maximal element in X. More exactly, for each $x \in X$, there exists a maximal element x^* such that $x \leq x^*$.*

Zorn's Lemma is equivalent to the Axiom of Choice (see [Ciesielski?]).

As an example and an important tool, which we use in order to prove the existence of algebraic closure of any field, we prove the following result:

A.14.2 *Every proper ideal in a commutative ring with identity is contained in a maximal ideal.*

Proof. Let R be a ring and I_0 a proper ideal (that is, $I_0 \neq R$). Let X be the set of all ideals in R, which contain I_0. The set X is nonempty, since $I_0 \in X$. We consider X with the inclusion as a partially ordered set. Let Y be a chain in X and let $J = \bigcup_{I \in Y} I$. We claim that J is a proper ideal. Let $r_1, r_2 \in J$, so that $r_1 \in I_1 \in Y$ and $r_2 \in I_2 \in Y_2$, where $I_1 \subseteq I_2$ or $I_2 \subseteq I_1$. Thus $r_1 - r_2 \in I_1$ or $r_1 - r_2 \in I_2$, which gives $r_1 - r_2 \in J$. If $r \in R$ and $r' \in J$, that is, $r' \in I$ for some $I \in Y$, then $rr' \in I \subseteq J$. Thus J is an ideal that contains I_0 (since $I_0 \subseteq I \in Y$). The ideal J is proper, since $1 \notin J$. Moreover, the ideal J is an upper bound for Y. By Zorn's Lemma, there exists a maximal element $I^\star$, which means that I^* is a maximal ideal containing I_0. □

A.15 Dual abelian groups

Let A, B, C be abelian groups and let $\varphi : A \times B \to C$ be a bilinear map, that is,

$$\varphi(a_1 + a_2, b) = \varphi(a_1, b) + \varphi(a_2, b), \qquad \varphi(a, b_1 + b_2) = \varphi(a, b_1) + \varphi(a, b_)).$$

By the **left kernel** of φ, we mean the subgroup of A:

$$\ker_l(\varphi) = \{a \in A | \varphi(a, B) = 0\}$$

The **right kernel** of φ is defined similarly. For every element $a \in A$, we have a homomorphism $\varphi_a : B \to C$ such that $\varphi_a(b) = \varphi(a, b)$. Denote $A' = \ker_l(\varphi)$ and $B' = \ker_r(\varphi)$. If $b \in B'$, then $\varphi_a(b) = 0$. Thus φ_a induces a homomorphism, which we denote with the same symbol $\varphi_a : B/B' \to C$. Now note that $a \mapsto \varphi_a$ is a homomorphism defined on A/A', since $\varphi_a = 0$ if $a \in A'$. Thus, we have a homomorphism, which maps $\bar{a}$ onto φ_a, where $\varphi_a(\bar{b}) = \varphi(a, b)$:

$$A/A' \to \mathrm{Hom}(B/B', C) \tag{A.1}$$

In fact, this is an injection, since $\varphi_a = 0$ if and only if $\varphi_a(b) = 0$ for each $b \in B$, which is equivalent $a \in A'$, so $\bar{a} = 0$. Similarly, we have an injection

$$B/B' \to \mathrm{Hom}(A/A', C) \tag{A.2}$$

in which $\bar{b}$ maps on φ_b, where $\varphi_b(\bar{a}) = \varphi(a, b)$. The **dual** of an abelian group X with respect to C is defined as $\mathrm{Hom}(X, C)$. It will be denoted by X^*_C or, when C is clear from the context, simply by X^*. If X is a finite group and C is finite cyclic, then $|X| = |X^*|$. In fact,

A.15.1 Lemma. *Let $\varphi : A \times B \to C$ be a bilinear mapping such that $A/\ker_l(\varphi)$ or $B/\ker_r(\varphi)$ is finite. Assume that C is a finite cyclic group. Then both these groups are finite and each is isomorphic to the dual group of the other one with respect to C.*

Proof. Since we have injections (A.1) and (A.2), it is clear that if one of the groups $A/\ker_l(\varphi)$ or $B/\ker_r(\varphi)$ is finite, then the other is also finite. Moreover, the same injections show that

$$|A/A'| \leq |(B/B')^*| \leq |(A/A')^*|$$

References

[B] G.M. Bergman, Exercises supplementing those in Ian Stewart's "Galois Theory", 3rd Edition, https://math.berkeley.edu/~gbergman/ug.hndts/#m114_IStwrt_GT

[BR] T.R. Berger, I. Reiner, A proof of the normal basis theorem, Am. Math. Monthly, 82 (1975), 915-918.

[CL] A. Chambert-Loir, A Field Guide to Algebra, UTM, Springer, 2005.

[Ch] N. G. Chebotarev, Grundzüge der Galois'schen Theorie (mit Hans Schwerdtfeger), P. Noordhoff, 1950.

[C] D. A. Cox, Galois Theory, Second Edition, Wiley, 2012.

[D] R.A. Dean, A rational polynomial whose group is the quaternions, Am. Math. Monthly, 88(1981), 42-45.

[GV] D. Gay, W. Y. Vélez, On the degree of the splitting field of an irreducible binomial, Pacific J. Math. 78 (1978), 117120.

[L] S. Lang, Algebra, Third Edition, Addison-Wesley, 1993.

[MM] G. Malle, B. H. Matzat, Inverse Galois Theory, Springer, 1999.

[R] S. Roman, Field Theory, Second Edition, Graduate Texts in Mathematics, Springer, 2006.

[S] A. Schinzel, Polynomials with Special Regard to Reducibility, Encyclopedia of Mathematics and its Applications 77, Cambridge University Press, 2000.

[T] J.-P. Tignol, Galois' Theory of Algebraic Equations, World Scientific, 2001.

List of notations

Index