ALGEBRA 1: groups, rings and fields

Groups

The set of pairs (a, b), where a is an element of A and b is an element of B is called a **product** of A and B and is denoted by $A \times B$. A mapping $f : A \to B$ from a set A to a set B is called an **injective mapping** or **injection** or **one-to-one mapping** (these are synonyms), if it maps different elements of the set A to different elements of the set B. A mapping is called a **surjective mapping** or a **surjection** or an **onto mapping** if for every element x of set B there exists at least one element of A that is mapped to x. A mapping is called **bijective mapping** or **bijection** or a **one-to-one mapping** if it is surjective and injective.

Let A be some set, either finite or infinite. Let $S(A)$ denote the set of all bijective mappings from A to itself. If f, g are two such mappings then they can be "multiplied" using composition $f \circ g$:

$$f \circ g(a) = f(g(a)).$$

A set $S(A)$ endowed with this operation is called "permutation group (or substitution group)" or more precisely "the group of permutations of A". Identity permutation is denoted by 1_A (or Id_A as well).

$S(A)$ is also called a **symmetric group**. If A is a finite set of n elements then $S(A)$ is denoted by S_n.

Permutations can be represented by tables; for example, a permutation $1 \mapsto 3$, $2 \mapsto 4$, $3 \mapsto 1$, $4 \mapsto 2$ of $1, 2, 3, 4$ can be written down as $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$. The numbers are written in the ascending order in the upper line, their images are written in the lower line.

Exercise 1.1. Compute the composition

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}.$$

Exercise 1.2. a. How many permutations of $1, 2, \ldots, 5$ are there? How many of them leave 1 unchanged?

b. How many of them map 1 to 5?

c. How many permutations are there such that $\sigma(1) < \sigma(2)$?

d. How many permutations are there such that $\sigma(1) < \sigma(2) < \sigma(3)$?

Exercise 1.3. How many elements are there in $S(A)$ if A is a finite set of n elements?

Exercise 1.4. Is it true that $f \circ g = g \circ f$ for any f, g?

For any permutation $f \in S(A)$ ("$\in$" means that the element belongs to the set) there exists a unique "inverse permutation" f^{-1}, i.e. a permutation such that $f \circ f^{-1} = f^{-1} \circ f = 1_A$.

A **cyclic permutation** of a set $a, b, c, d, \ldots, w$ maps a to b, b to c, c to d and so on. Such a permutation is denoted by $(a, b, c, d, \ldots, w)$. The number of elements in the brackets is its **order**. **Transposition** is a cyclic permutation of order 2; it permutes two elements and leaves all other elements unchanged.

Exercise 1.5. Let $\sigma = (123)$, $\tau = (34)$. Calculate $\tau \circ \sigma \circ \tau^{-1}$.

Exercise 1.6. Prove that every permutation is a product of transpositions.

Exercise 1.7 (*). Is it possible that a product of even number of transpositions be an identity permutation?

Hint. What happens to a polynomial $(x_1 - x_2)(x_1 - x_3)\dots(x_1 - x_n)(x_2 - x_3)\dots$ (a product of $(x_i - x_j)$ for all $i > j$) when x_i and x_j are permuted?

A permutation group $S(A)$ is endowed with the following structure: operation of multiplication of permutations, operation of taking inverse of a permutation, the identity permutation. It is useful to axiomatize this structure.

Definition 1.1. Let G be a set with the following operations defined on it: $f, g \mapsto f \cdot g$ ("multiplication"), $f \mapsto f^{-1}$ ("taking inverse") and let the "identity element" 1_G be defined as well. Let the following axioms be satisfied:

a. "Associativity": $(f \cdot g) \cdot h = f \cdot (g \cdot h)$ for all f, g, h.

b. "Identity": $f \cdot 1_G = 1_G \cdot f = f$ for all f.

c. "Inverse element": $f \cdot f^{-1} = f^{-1} \cdot f = 1_G$ for all f.

In this case we call G a **group**.

A subset of G which is closed under these operations is called a **subgroup of** G .

Exercise 1.8. Consider a group G. Prove that for any two elements f and g of it

a. If $fg = f$ or $gf = f$ then $g = 1$;

b. If $fg = 1$ or $gf = 1$ then $g = f^{-1}$.

Remark. This means that to define a group structure on a set G it suffices to define an operation of multiplication. Identity element and operation of taking inverse are uniquely determined by it and can be then reconstructed.

Exercise 1.9. Are these sets (with indicated operations) groups?

a. Natural numbers with an operation of addition;

b. Integer numbers with an operation of addition;

c. Integer numbers with an operation of multiplication;

d. Rational numbers with an operation of multiplication;

e. Real numbers with an operation of addition;

f. Real numbers with an operation of multiplication;

g. (*)Planar motions with an operation of composition;

h. Numbers strictly greater than -1 and strictly less than 1 with an operation defined by the formula $u * v = (u + v)/(1 + uv)$ (check that the operation is defined correctly);

i. Figures (sets of points) on a plane with an operation of union;

j. **(*)**Figures (sets of points) on a plane with an operation of symmetric difference: $A * B$ contains points that belong to precisely to one of the figures (A or B);

k. **(*)**Mappings from a fixed set C into a fixed group G with an operation $(f \cdot g)(s) = f(s)g(s)$.

"Product of groups" G_1 and G_2 is a set of pairs (g_1, g_2), $g_1 \in G_1, g_2 \in G_2$ with an operation

$$(g_1, g_2) \cdot (g_1', g_2') = (g_1 \cdot g_1', g_2 \cdot g_2')$$

A mapping $f : G \to G'$ from a group G into a group G' is called a **homomorphism** if it preserves the multiplication: $f(g_1 \cdot g_2) = f(g_1) \cdot f(g_2)$. A homomorphism is called a **monomorphism**, if it is injective, an **epimorphism** if it is surjective and an **isomorphism** if it is bijective. Groups G, G' are **isomorphic** if there exists an isomorphism between them. An isomorphism of a group into itself is called an **automorphism**.

Exercise 1.10. Prove that if $f : G \to G'$ is a homomorphism of groups then for any $g \in G$ $f(1_G) = 1_{G'}$ and $f(g^{-1}) = (f(g)^{-1})$.

Definition 1.2. If a homomorphism $G \to S(A)$ of a group G into a group $S(A)$ of permutations of a set A is defined then one says that G **acts on a set** A (and indeed every element of G permutes the elements of A somehow). The action of G on A can be thought of as a mapping $G \times A \xrightarrow{\rho} A$, $a, g \mapsto \rho(g, a)$. Sometimes the notation for an action of a group on a set is even simpler: $a, g \mapsto g(a)$.

Exercise 1.11. Prove that every group admits an injective homomorphism into a permutation group (of a not necessarily finite set).

Hint. Think about what the meaning of the following phrase can be: "Group G acts on itself by multiplication on the left".

Exercise 1.12. Is it true that

a. every group that consists of two elements is isomorphic to permutation group S_2;

b. every group that consists of six elements is isomorphic either to permutation group S_3 or to the product of two non-trivial (i.e. those that have more than one element) groups.

Exercise 1.13 (*). Prove that permutation group S_n is not isomorphic to the product of two non-trivial groups.

Exercise 1.14. Let G be a group and $g \in G$ its element. Is it true that the sequence $g, g^2, g^3, \ldots$ is periodic? Is it true if G is a finite group?

Let n be a natural number. It is said that $g \in G$ is an **element of order** n in a group G if $g^n = 1_G$ but $g^k \neq 1_G$ for any $k < n$.

Exercise 1.15 (!). Consider a finite group of n elements. Prove that n is divisible by the order of every element of that group.

Hint. Consider the action of the group on itself by multiplication on the left.

Exercise 1.16 (*). Consider a group with an even number of elements. Prove that it contains an element of order 2.

Exercise 1.17 (*). Is it true that

a. the group D_{12} of rotations of a regular 12-gon is isomorphic to a product $D_6 \times S_2$ where D_6 is a group of rotations of a regular hexagon;

b. the group D_6 is isomorphic to a product $D_3 \times S_2$ where D_3 is a group of rotations of a triangle.

A group is called **commutative** or an **Abelian group** if $f \cdot g = g \cdot f$ for all f, g. Two elements f, g **commute** if $f \cdot g = g \cdot f$.

Exercise 1.18. Which groups out of those considered in the exercise 1.9 are commutative?

Exercise 1.19 (*). a. A **center** of a group G is a set consisting of all the elements $g \in G$ such that $gg' = g'g$ for all $g' \in G$. Prove that center is a subgroup.

b. Consider a group G such that there exist an element in it of order > 2. Consider a subgroup G' such that all elements $g \in G$ that do not belong to G' have order 2. Give an example of such a situation (or prove that it is not possible). Is G always finite when the mentioned conditions hold?

c. In the conditions of a previous question prove that G' is an abelian group

d. Let G' contain a center G. Prove that a group G is uniquely (up to an isomorphism) determined by the G' subgroup if the condition from (2) holds. (G' is called then a dihedral group)

e. Consider a dihedral group G corresponding to an abelian group G' as shown above. Let G' be a product of S_2 and some other abelian group: $G' = S_2 \times G''$. Prove that G is a product of S_2 and a dihedral group.

Rings and fields

Consider real numbers, integer numbers and finite decimal fractions. There are the following operations defined on these structures

a. Addition which is commutative and makes a group out of a set (addition is designated as "+"; taking an inverse element is designated as "-")

b. Multiplication which is also commutative but does not make a group out of any of the considered sets because some elements are non-invertible (multiplication is designated by a dot; the dot is often omitted: one writes xy instead of $x \cdot y$).

It is useful to axiomatize these structures.

Definition 1.3. Let R be a set with two operations $a, b \mapsto a + b$ (addition) and $a, b \mapsto a \cdot b$ (multiplication). Let elements 0 and 1 (zero and identity) be defined in R. If the following holds then R is called a **ring**:

a. R is a commutative group with respect to the operation of addition, 0 is a the identity element in this group

b. 1 is an identity with respect to multiplication: $1 \cdot a = a \cdot 1 = a$ for all a.

c. Associativity for multiplication: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

d. Distributivity: $a \cdot (b + c) = a \cdot b + a \cdot c$.

If the multiplication is commutative then one says that a ring R is commutative. If, moreover, the multiplication is invertible for all $a \neq 0$, i.e. $R\backslash\{0\}$ is a group with respect to multiplication then R is called a **field**.

In this chapter as well as in several following chapters we will consider only commutative rings and we will omit the word "commutative" for brevity; unless it is stated otherwise explicitly all the rings are assumed to be commutative.

Exercise 1.20. Are the following sets (equipped with natural operations unless they are specified explicitly) the rings:

a. natural numbers

b. integer numbers

c. even integer numbers

d. rational numbers

e. irrational numbers

f. finite decimal fractions

g. pairs of integer numbers with the coordinatewise addition and multiplication

h. pairs of integer numbers with the coordinatewise addition and multiplication defined by the formula $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$

i. **(*)** pairs of rational numbers with the coordinatewise addition and multiplication defined by the formula $(a, b) \cdot (c, d) = (ac + 2bd, ad + bc)$.

j. **(*)**figures on the plane (addition is symmetric difference, multiplication is intersection).

k. **(*)**mappings from a fixed set C into a fixed group G with an operation $(f \cdot g)(s) = f(s)g(s)$.

Exercise 1.21. Which rings from the exercise 1.20 are fields?

Exercise 1.22. Consider a ring R. Consider a set of sequences

$$a = (a_0, a_1, \dots, a_i, \dots, 0, 0, \dots)$$

consisting of elements of R with the finite number of non-zero elements. Define the operations on this set as follows

$$(a + b)_i = a_i + b_i,$$

$$(a \cdots b)_i = \sum_{j=0}^{i} a_j b_{i-j}.$$

Prove that this set is a ring (check in particular that multiplication is associative).

The ring defined in the exercise 1.22 is called a **ring of polynomials of single variable** on R, it is denoted by $R[x]$. Elements of $R[x]$ are called "polynomials". They are usually written down in the form $a_0 + a_1 x + \cdots + a_i x^i$ (for all $j > i$, a_j are zero).

In the algebra course we will suppose the notion of a real number known, (for example, you can think about real numbers as of infinite decimal fractions with usual operations defined on the

fractions). The rigorous definition is given in the course of geometry, topology and analysis. All we need in the algebra course is

Important note: Real numbers form a field.

This "important note" is also proven in the course of geometry, topology and analysis. Besides that, we need the following property :

Exercise 1.23 (*). Prove that every equation of the form

$$x^{2n+1} + a_{2n}x^{2n} + a_{2n-1}x^{2n-1} + \cdots + a_1x + a_0 = 0$$

has a real solution.

You should try solving this exercise when you are familiar with the notion of a real number.

Exercise 1.24 (*). Will the ring defined in the exercise 1.20 9 be a field if we change "rational numbers" for "real numbers" in the definition?

Exercise 1.25. Consider a fixed natural number n. Natural numbers divided by n have remainders 0, 1, 2, $\dots n-1$. Let us denote the operation of taking remainders by $\mod n$. Two numbers that have the same remainders $\mod n$ are called equal modulo n. Let us define addition and multiplication on a set of numbers $\mod n$ in such a way that

$$(x \mod n) + (y \mod n) = ((x+y) \mod n),$$
$$(x \mod n) \cdot (y \mod n) = (xy \mod n)$$

would hold for all pairs of integer numbers x, y. Prove that this definition is correct and the set of remainders form a ring.

Exercise 1.26 (*). Prove that the set of remainders $\mod n$ with the addition and multiplication defined as above form a field iff n is a prime number.

Remark. If you cannot solve this problem right away, put it away: the same problem will be reintroduced without an asterisk after defining some useful intermediate notions.

Exercise 1.27. Build the field which consists of

a. 2 elements

b. 3 elements

c. (*)4 elements.

Exercise 1.28 (*). Prove that there is no field that consists of 6 elements

Exercise 1.29. Prove that if p is a prime number then a field that consists of p elements is unique up to isomorphism.

Definition 1.4. Characteristic of a field k is 0 if $1 \in k$ has infinite order with respect to addition, otherwise it is equal to the order p of an element $1 \in k$ if it is finite.

Exercise 1.30. Prove that if the characteristic p of a field k is not zero then p is a prime number.

Exercise 1.31 (*). Consider a field of characteristic p. Prove that Frobenius mapping $x \mapsto x^p$ preserves multiplication and addition (just like with the groups such a mapping is called a homomorphism).

Hint. Use the binomial theorem.

Exercise 1.32 (*). Deduce Fermat's smaller theorem from that: x^p is equal to x modulo p for any integer number x.

Let $P = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ be a polynomial with the coefficients in the field k. A **root** P is an element α of a field k such that $P(\alpha) = 0$.

Exercise 1.33. Let α be the root of a polynomial P over a field k. Prove that a polynomial P can be divided by $z - \alpha$ in the ring $k[z]$

Hint. Use the long division of polynomials:

$$\begin{array}{rl|l} x^2 + 2x - 12 & & x+5 \\ \cline{3-3} x^2 + 5x & & x-3 \\ \cline{1-1} \quad -3x - 12 & & \\ \quad -3x - 15 & & \\ \cline{1-1} \qquad\qquad 3 & & \end{array}$$

Exercise 1.34. Prove that nonzero polynomial of degree n over a field cannot have more than n different roots.

Hint. Use the previous exercise.

Let P be a nonzero polynomial over a field k. A polynomial P is called **irreducible** if it cannot be represented as a product of polynomials of smaller degree.

Consider the set of remainders modulo P in a ring $k[x]$.

Exercise 1.35. Prove that this is a ring (we denote it by $k[x] \mod P$).

Complex numbers

The set of integer numbers is denoted by $\mathbb{Z}$ and the set of real numbers is denoted by $\mathbb{R}$. Let $\mathbb{C}$ be a set of pairs of real numbers (a, b) with addition defined by the formula $(a, b)+(c, d) = (a+c, b+d)$ and with multiplication defined by formula

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc).$$

Elements of $\mathbb{C}$ are called complex numbers.

Exercise 1.36. Check that $\mathbb{C}$ is a ring. Prove that an equation $x^2 + 1 = 0$ has a solution in $\mathbb{C}$. How many solutions does it have?

Exercise 1.37. Let us take a solution of an equation $x^2 + 1$ in $\mathbb{C}$ and denote it by $\sqrt{-1}$. Prove that any complex number can be uniquely represented in the form $a + b\sqrt{-1}$, $a, b \in \mathbb{R}$.

Exercise 1.38. Build an isomorphism $\mathbb{C} \cong (\mathbb{R}[x] \mod P)$ where P is a polynomial $P = x^2 + 1$.

Exercise 1.39. Consider a complex number $z := a + b\sqrt{-1}$. A number conjugate to z is the number $\overline{z} := a - b\sqrt{-1}$. Prove that complex conjugation preserves multiplication and addition in $\mathbb{C}$ (such mappings are called automorphisms of the field $\mathbb{C}$).

Exercise 1.40. Consider a complex number $z := a + b\sqrt{-1}$. Prove that $z\overline{z}$ is real (it means that in the representation of a complex number (x, y) the component y is zero).

Exercise 1.41. Consider a complex number $z := a + b\sqrt{-1}$. Prove that $z\overline{z} = a^2 + b^2$. That means in particular the this number is always nonnegative and equals zero only if $z = 0$. $z\overline{z}$ is often written down as $|z|^2$ since the length of a vector (a, b) on a plane equals $\sqrt{a^2 + b^2}$ (the distance between z 0, $|z|$ is called a modulus of z).

Exercise 1.42. Deduce from the previous problem that complex numbers form a field.

Hint. $z^{-1} = \overline{z}|z|^{-2}$

Exercise 1.43. Prove "triangle inequality": $|z_1| - |z_2| \leqslant |z_1 + z_2| \leqslant |z_1| + |z_2|$

Exercise 1.44. Prove that $|z_1 z_2| = |z_1||z_2|$.

Exercise 1.45 (!). Let $z = a + b\sqrt{-1}$ be a complex number with the modulus equal to 1: $|z| = 1$. Let us regard the multiplication by z as a transformation of a plane $\mathbb{R}^2$ associated naturally with $\mathbb{C}$. Prove that if $z \neq 1$ then this transform is planar motion with a single fixed point $0 \in \mathbb{R}^2$.

Exercise 1.46 (!). It is known from geometry that a planar motion with the only fixed point $0 \in \mathbb{R}^2$ is a rotation by some angle φ around 0. Given φ, how a and b can be found in task 1.45?

Remark. The angle φ is called an **argument** of complex number z.

Exercise 1.47 (!). Prove the formula $\cos(\varphi + \psi) = \cos\varphi \sin\psi + \sin\varphi \cos\psi$.

Hint. Use the previous problem.

Exercise 1.48 (!). Prove that an equation $z^n = 1$ has precisely n complex solutions.

Hint. Use the trigonometric interpretation of complex numbers.

Exercise 1.49 (*). Consider a polynomial P of a degree less than n and let $\zeta_1, \ldots, \zeta_n$ be "the roots of n-th degree from 1" or, simply put, let $\zeta_1, \ldots, \zeta_n$ be all complex $z^n = 1$. Prove that the mean $\frac{1}{n}\sum P(\zeta_i)$ of values of P in all the points ζ_i equals $P(0)$.

Hint. Use the trigonometric interpretation of complex numbers.

Exercise 1.50 (*). Consider a polynomial P of a degree less than n. Let Ξ be a regular n-gon on a complex plane $\mathbb{C} = \mathbb{R}^2$. Prove that the value of P in the center of Ξ equals to the mean of values of P in the vertices of Ξ.

Hint. Use the previous problem.

Remark. Archimedes defined the perimeter of a circle as a limit of perimeters of polygons inscribed into it. If we follow Archimedes then we can define the mean of a function f defined on a circle as a limit (by n) of means $\frac{1}{n}\sum f(\zeta_i)$ where z_i are vertices of regular n-gons inscribed into the circle. One can deduce from the previous problem that the mean of values of a polynomial function P on a unity circle $|z| = 1$ equals the value of P in its center.

Exercise 1.51. Calculate the group of automorphisms of $\mathbb{C}$

a. (*)which translate $\mathbb{R} \subset \mathbb{C}$ into itself.

b. which translate the subfield $\mathbb{R} \subset \mathbb{C}$ into itself and do not move its elements.

Exercise 1.52 (!). Let us change the definition of complex numbers. Instead of

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc).$$

let us put

$$(a, b) \cdot (c, d) = (ac + bd, ad + bc).$$

Let us denote the obtained structure by $\mathbb{R}_2$. Is $\mathbb{R}_2$ a ring? Is it a field? Find all solutions of an equation $z^2 = 1$ in $\mathbb{R}_2$. Find all the solutions of an equation $z^2 = 0$ in $\mathbb{R}_2$.

Exercise 1.53 (!). Let us change the definition of complex numbers. Instead of

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc).$$

let us put

$$(a, b) \cdot (c, d) = (ac, ad + bc).$$

Let us denote the obtained structure by $\mathbb{R}_\varepsilon$. Is $\mathbb{R}_\varepsilon$ a ring? Is it a field? Is it isomorphic to $\mathbb{R}_2$ from the previous problem? Find all the solutions of an equation $z^2 = 1$.

Exercise 1.54 (*). Find all the solutions of an equation $z^2 = z$ in two previous problems.

Exercise 1.55 (*). Let $P = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial of degree n with n roots lying outside the unit circle. Prove that $\frac{a_k}{a_0} < C_n^k$ where $C_n^k = \frac{n!}{k!(n-k)!}$ is a binomial coefficient.

ALGEBRA 2: divisibility in rings and Euclid's algorithm

Greatest common divisor

Let R be a ring.

Definition 2.1. Divisors of zero in ring R are the elements x, y such that $xy = 0$. R is called an **integral domain** if there are no divisors of zero in R.

Throughout this section all rings are supposed to be integral domains.

Definition 2.2. An invertible element in R is called a **unit** of ring R.

Exercise 2.1. Gauss integers are complex numbers of a form $x + y\sqrt{-1}$ where x, y are integers. Prove that they form a ring. It is denoted by $\mathbb{Z}[\sqrt{-1}\,]$.

Exercise 2.2. Describe all the unities in the ring of Gauss integers.

Hint. If a complex number z is invertible in $\mathbb{Z}[\sqrt{-1}\,]$ then $z\overline{z}$ is also invertible in $\mathbb{Z}[\sqrt{-1}\,]$.

Exercise 2.3. Let us fix a positive integer n. Consider a set of all complex numbers of the form $x + y\sqrt{-n}$ where x, y are integers. Prove that this is a ring.

Exercise 2.4 (*). Fix a positive integer n. Consider a set of all complex numbers of the form $\frac{x+y\sqrt{-3}}{2}$ where x, y are either both even or both odd. Prove that this is a ring and describe all unities. We will denote this ring by $\mathbb{Z}[\widetilde{\sqrt{-3}}]$.

Definition 2.3. Let R be a ring and $x, y \in R$ be elements of R. If $x = yz$ in R then one says that x is **divisible** by y in R and y **divides** x. The relation of divisibility is denoted by $x \vdots y$.

Definition 2.4. Let R be a ring and $x, y \in R$ be the elements of R. **Greatest common divisor** (GCD) of x, y is an element $z \in R$ such that z divides x and y and for all z' which divides x, z' divides z. x and y are called **coprime** if 1 is the greatest common divisor of x, y.

Strictly speaking, if one considers an arbitrary ring GCD may not exist for every pair of elements.

Exercise 2.5. Prove that if GCD exists then it is unique up to a unit: if z and z' are greatest common divisors x and y in a ring R, then $z = ez'$, where e is a unit of ring R.

Exercise 2.6. Let $\mathbb{Q}(2)$ be a set of all rational numbers, represented as fractions of the form $\frac{p}{q}$ with odd denominator q. Prove that this set is closed under multiplication and addition and forms a subring in the ring of rational numbers.

Exercise 2.7. Give an example of a non-invertible element in $\mathbb{Q}(2)$.

Exercise 2.8. Describe all unities of the ring $\mathbb{Q}(2)$.

Exercise 2.9 (!). Prove that in $\mathbb{Q}(2)$ for any two elements there exists a greatest common divisor of them.

Hint. Prove that any element of $\mathbb{Q}(2)$ can be represented in the form $e2^n$, where e is a unit.

Definition 2.5. Let p be an element of a ring R. It is called **prime**, if for any q, r with $p = qr$ either q, or r is a unit of the ring R.

Exercise 2.10. What are prime elements of $\mathbb{Q}(2)$?

Divisibility in the ring of integer numbers

Exercise 2.11. Let x, y be positive integer numbers and $z = (x - ky)$ be the remainder when x is divided by y. Prove that if $\mathrm{GCD}(y, z)$ exists then $\mathrm{GCD}(x, y)$ exists as well and $\mathrm{GCD}(x, y) = \mathrm{GCD}(y, z)$.

Definition 2.6. The Euclid's algorithm takes two positive integer numbers x, y, $x > y$ and return a positive integer number z.

a. If x is divisible by y then algorithm stops and returns y.

b. If x is not divisible by y then algorithm loops, taking numbers $x_1 = y$, $y_1 = x - ky$ where $x - ky$ is the remainder when x is divided by y.

Exercise 2.12. Prove that the Euclid's algorithm terminates after finite number of iterations.

Exercise 2.13. Prove that the number returned by the Euclid's algorithm applied to integer numbers x, y is $\mathrm{GCD}(y, z)$

Exercise 2.14. Solve the problem 1.26 from ALGEBRA 1 (unless you have already solved it).

Exercise 2.15. Prove that the Euclid's algorithm applied to numbers x, y can be represented as a linear combination of x with y integer coefficients: $z = ax + by$.

Exercise 2.16. Let x, y be coprime integer numbers and p be a prime number. Suppose that xy is divisible by p^α for some natural number α. Prove that either x is divisible by p^α, or y is divisible by p^α.

Exercise 2.17 (!). Deduce that prime multipliers decomposition is unique: if a positive integer number x can be represented in two ways as a product of prime numbers then these two ways only differ by an order of multipliers.

Hint. Present x as a product $p_i^{\alpha_i}$ where p_i are different prime numbers and use the previous problem to prove that α_i can be defined in unique fashion.

Unique factorization ring

Definition 2.7. Let R be a ring. Two decompositions of $r \in R$ into prime multipliers $r = p_1 p_2 \dots p_k$, $r = q_1 q_2 \dots q_k$ are called equivalent if $r = q_1 q_2 \dots q_k$ can be obtained after by permuting p_i and by multiplying p_i by ring unit. It is said that R is a **unique factorization ring**, if for any $r \in R$ there exists decomposition of r into the product of prime elements which is unique up to equivalence.

Exercise 2.18 (!). Let a ring R admits decomposition into prime multipliers and for each pair of elements x, y there exists a GCD in this ring. Let z be represented in R as a linear combination of x, y: $z = ax + by$ where $a, b \in R$. Prove that R is a unique factoriazation ring.

Hint. Use the hint to the problem 2.17.

Exercise 2.19. Consider a positive number n. Consider a ring $\mathbb{Z}[\sqrt{-n}] \subset \mathbb{C}$ of complex numbers of the form $z = x + y\sqrt{-n}$ where x and y are integer. Prove that $|z|^2$ is integer for all $z \in \mathbb{Z}[\sqrt{-n}]$.

Exercise 2.20. Prove that z is a unit in $\mathbb{Z}[\sqrt{-n}]$ iff $|z|^2 = 1$.

Hint. $|z^{-1}|^2 = (|z|^2)^{-1}$.

Exercise 2.21. Let z be an element of $\mathbb{Z}[\sqrt{-n}]$ such that $|z|^2$ is prime in $\mathbb{Z}$. Prove that z is prime in $\mathbb{Z}[\sqrt{-n}]$.

Hint. $|zz'|^2 = |z|^2|z'|^2$.

Exercise 2.22 (!). Consider the ring $\mathbb{Z}[\sqrt{-3}]$. Prove that 2 and $1 \pm \sqrt{-3}$ are primes. Deduce that $\mathbb{Z}[\sqrt{-3}]$ is not a unique factorization ring.

Hint. Use the equality $2^2 = 4$.

Division with remainder in rings

Definition 2.8. Let R be a ring. It is said that **division with remainder is defined** in R if for every pair x, y, $y \neq 0$ in R there are elements $z, k \in R$ defined such that $z = x - ky$. In this case z is called **remainder** and k is called **factor**.

Examples. Division with remainder is defined in the ring of integer numbers. Division with remainder is defined as well in the ring of polynomials $k[t]$ over a field k:

$$\begin{array}{rl} x^2 + 2x - 12 & \big| \overline{x + 5} \\ \underline{x^2 + 5x} & \big| \overline{x - 3} \\ -3x - 12 & \\ \underline{-3x - 15} & \\ 3 & \end{array}$$

Definition 2.9. Let division with remainder be defined in the ring R. **Euclid's algorithm in** R is applied to a pair x, y of non-zero elements in R and is defined recursively. If x is divisible by y Euclid's algorithm stops and returns y. If x is not divisible by y then Euclid's algorithm is applied to y, z, where z is a remainder when x is divided by y. This process can be infinite, a priori.

Exercise 2.23 (!). Let division with remainder be defined in a ring R. Suppose that Euclid's algorithm applied to a pair $x, y \in R$ stopped in some finite number of steps and returned $z \in R$. Prove that

a. $z = ax + by$ for some $a, b \in R$.

b. z is the greatest common divisor of x and y.

Hint. Proof for the arbitrary ring is the same as in the case of ring of natural numbers.

Definition 2.10. Let R be a ring. It is said that **there exists a Euclid's algorithm in** R or that R **is Euclidean** if division with remainder is defined in R and for all $x, y \in R$ Euclid's algorithm stops in finite number of steps.

Exercise 2.24 (!). Let there exists a prime multipliers decomposition and an Euclid's algorithm in a ring R. Prove that R is a unique factorization ring.

Hint. Use the previous problems.

Exercise 2.25. Prove that the ring $k[t]$ of polynomials over a field k.

Exercise 2.26. Prove that an equation $x \cdot y = 0$ has a solution (for $x, y \neq 0$) in $k[t] \mod P$ if and only if a polynomial P is irreducible.

The integer part $[z]$ of a complex number $z = x + y\sqrt{-1}$ is defined as $[x + 0.5] + [y + 0.5]\sqrt{-1}$ where $[\,]$ denotes an operation of taking an integer part of a real number (if one interprets complex numbers as points on a plane $\mathbb{R}^2$ then $[z]$ is a point with integer coordinates closest to z). Division with remainder in the ring of Gauss integers $\mathbb{Z}[\sqrt{-1}\,]$ is defined as follows: the factor of z_1 and z_2 equals $[\frac{z_1}{z_2}]$ and the remainder equals $z_1 - [\frac{z_1}{z_2}]z_2$.

Exercise 2.27. Prove that $\left|z_1 - \left[\frac{z_1}{z_2}\right] z_2\right| < |z_2|$.

Exercise 2.28. Prove that in the ring of Gauss integers $\mathbb{Z}[\sqrt{-1}\,]$ Euclid's algorithm always terminates.

Hint. Use the previous problem. Deduce that with every step of the Euclid's algorithm a quantity $\min(|z_1|^2, |z_2|^2)$ decreases.

Let $R = \mathbb{Z}[\sqrt{-n}]$ or $R = \widetilde{\mathbb{Z}[\sqrt{-3}]}$. For any $z \in \mathbb{C}$ let us denote by $[z]_R$ a point of a complex plane corresponding to point from R closest to z. If there are several such points let us take a point with greatest $Re[z]_R$, if still there are several such points, let us take one with the greatest $Im[z]_R$. Define the division of z_1 by z_2 with remainder in such a way that the factor of z_1 and z_2 is $[\frac{z_1}{z_2}]_R$ and the remainder is $z_1 - [\frac{z_1}{z_2}]_R z_2$.

Exercise 2.29 (*). Prove that if $n = 1$ then it is the usual division with remainder in $\mathbb{Z}[\sqrt{-1}\,]$

Exercise 2.30 (*). Let $|z - [z]_R| < 1$ for all $z \in \mathbb{C}$. Prove that with every step of the Euclid's algorithm a quantity $|z_2|^2$ decreases.

Exercise 2.31 (*). Let for any point $z \in \mathbb{C}$ there exist $r \in R$ such that $|r - z| < 1$. Prove that R is Euclidean.

Exercise 2.32 (*). Prove that the following rings are Euclidean: $\mathbb{Z}[\sqrt{-2}]$, $\widetilde{\mathbb{Z}[\sqrt{-3}]}$.

Exercise 2.33. Decompose the number 2 into prime multipliers in $\mathbb{Z}[\sqrt{-1}\,]$.

Hint. Use the problem 2.21.

Exercise 2.34 (*). Decompose the numbers 3, 5, 7 into prime multipliers in $\mathbb{Z}[\sqrt{-1}\,]$.

Exercise 2.35 (*). Prove that a prime number in $\mathbb{Z}$ of the form $p = 4k + 3$ is prime in $\mathbb{Z}[\sqrt{-1}\,]$.

Hint. Prove that p cannot be represented as a sum of squares.

Exercise 2.36. Let $z = a + b\sqrt{-1}$ be a Gauss integer which is not divisible by $1 + \sqrt{-1}$. Suppose that a and b are coprime. Prove that z and $\overline{z}$ are coprime.

Hint. Prove that if a and b are coprime in $\mathbb{Z}$ then 2 can be represented as a linear combination $a+b\sqrt{-1}$, $a-b\sqrt{-1}$.

Exercise 2.37 (!). Let a, b, c be coprime numbers such that $a^2+b^2=c^2$. Prove that $c=|z|^2$ for some $z \in \mathbb{Z}[\sqrt{-1}\,]$.

Hint. Use the fact that $c^2=(a+b\sqrt{-1})(a-b\sqrt{-1})$ and a, b are coprime. Apply the uniqueness of prime multipliers decomposition in $\mathbb{Z}[\sqrt{-1}\,]$ and deduct that every prime multiplier of $a+b\sqrt{-1}$, $a-b\sqrt{-1}$ appears twice in the decomposition.

Exercise 2.38 (!). Find all triples of integer numbers a, b, c such that $a^2+b^2=c^2$ ("find" means "write a formula that gives all such triples when one substitutes its variables with integer numbers").

Hint. Use the previous problem.

Exercise 2.39 (*). Find all triples of coprime numbers a, b, c such that $a^2+2b^2=c^2$.

Exercise 2.40. Use the uniqueness of prime multipliers decomposition in $\mathbb{Z}[\sqrt{-2}]$

Exercise 2.41 (**). Find all triples of coprime numbers a, b, c such that $a^2+3b^2=c^2$.

ALGEBRA 3: vector spaces and linear mappings

Vector spaces

Recall that abelian (or commutative) group is a group where group operation is commutative:

$$f \cdot g = g \cdot f$$

Group operation in abelian groups is often denoted by + and called "addition"; unity is denoted by 0 in this case and is called "zero".

Definition 3.1. Linear or **vector** space V over field k is an abelian group with an operation $k \times V \mapsto V$ ("multiplication of vector by element of a field") which is in accordance with the group operation in the following sense:

a. For any $\lambda \in k$, $u, v \in V$, $\lambda(u+v) = \lambda u + \lambda v$. For any $\lambda_1, \lambda_2 \in k$, $u \in V$, $(\lambda_1+\lambda_2)u = \lambda_1 u + \lambda_2 u$ (distributivity of multiplication with respect to addition).

b. For any $\lambda_1, \lambda_2 \in k$, $u \in V$, $\lambda_1(\lambda_2 u) = (\lambda_1\lambda_2)u$ (associativity of multiplication).

c. For any $v \in V$, $1v = v$ where $1 \in k$ is a unity.

Elements of vector space are called vectors and group operation is called the addition of vectors.

Exercise 3.1. Consider a field k. Prove that k is a vector space over itself.

Exercise 3.2. Prove that the group k^* of invertible elements in k with multiplication as group operation acts on any vector space over k.

Remark. This group is called the multiplicative group of field k.

Exercise 3.3. Prove that a group of parallel transports of a plane has a structure of vector space over $\mathbb{R}$.

Exercise 3.4. Consider a vector space V over k. Prove that $0_k(v) = 0_V$ for any $v \in V$. Here 0_k is the zero in k and 0_V is the unity in V.

Exercise 3.5. Consider a field and its subfield k. Prove that is a vector space over k.

Exercise 3.6. Consider a field k.

a. Denote a set of n-tuples $(a_1, a_2, \dots, a_n)$ of elements of k by k^n. Define a natural addition on k^n and action of k^* on it and prove that you obtained a vector space.

b. Consider a set S. Denote by $k[S]$ a set of all collections of elements of k

$$\langle a_{s_1}, a_{s_2}, \dots \rangle$$

each element of a collection corresponding to precisely one element of S such that a_s are zero except a finite number of them. Introduce a structure of vector space over k on $k[S]$.

Vector space $k[S]$ is called a vector space, **generated** by a set S. Set S can be naturally embedded into $k[S]$ – every element of $s \in S$ corresponds to a vector $[s] \in k[S]$ such that all $a_{s'}$ are zeros except a_s which is 1.

Definition 3.2. Let A, B be two sets and let G act on them. It is said that a mapping $\kappa :\ A \to B$ **is compatible with action** G if $\kappa(g(a)) = g(\kappa(a))$.

Recall that a homomorphism of abelian groups is a mapping that preserves the group operation

$$f :\ G_1 \to G_2, \quad f(g+g') = f(g) + f(g') \tag{3.1}$$

Definition 3.3. Homomorphism of vector spaces over k is a mapping which preserves addition of vectors (cf. (3.1)) and is compatible with the action of k^*.

In other words a homomorphism of vector spaces is a mapping $f :\ V_1 \to V_2$ which satisfies conditions $f(v_1+v_2) = f(v_1)+f(v_2)$, $f(\lambda v) = \lambda f(v)$. Monomorphism, epimorphism, isomorphism and automorphism of vector spaces are defined in the same fashion as for groups (as well as rings, fields and all other algebraic structures). When talking about vector spaces one says "linear operator" or "linear mapping" instead of "homomorphism".

Recall that identity mapping of a vector space V is denoted by Id_V. Id_V is obviously an automorphism.

Exercise 3.7. Prove that a linear mapping $\varphi :\ V_1 \to V_2$ is bijective if and only if it is **invertible**, i.e. there exists a linear mapping $\psi :\ V_2 \to V_1$ such that

$$\psi \circ \varphi = \mathsf{Id}_{V_1}, \varphi \circ \psi = \mathsf{Id}_{V_2}\,. \tag{3.2}$$

Are these conditions sufficient each on its own ?

Exercise 3.8. The fact that two vector spaces V, V' are isomorphic is denoted by $V \cong V'$. Prove that

a. If $V \cong V'$ and $V' \cong V''$ then $V \cong V''$.

b. If $V \cong V'$ then $V' \cong V$.

c. It is always true that $V \cong V$.

Exercise 3.9. Prove that the set of homomorphisms from V_1 to V_2 form a vector space (it is often denoted by $\mathrm{Hom}(V_1, V_2)$).

Exercise 3.10. Prove that the set of automorphisms V forms a group (this group is often denoted by $GL(V)$). Is this a commutative group?

Definition 3.4. Subgroup $V' \subset V$ of a vector space V is called a **vector subspace** or **linear subspace of** V if it is preserved under the action of k^* (in other words for any $\lambda \in k$, $v, v' \in V'$ it is true that $\lambda(v) \in V'$, $v + v' \in V'$).

Vector subspace is itself a vector space over the same field.

Exercise 3.11. Consider a set S. Prove that a set of all mappings $\mathrm{Map}(S, k)$ from S to k is a vector space.

Exercise 3.12 (*). Consider a vector space W and a set S. Prove that any mapping $S \to W$ can be extended in a unique way to a linear mapping $k[S] \to W$. Is it true if we allow for the infinite non-zero elements of a field in the definition of $k[S]$?

Exercise 3.13. Let $k[t]$ be a set of polynomials $a_n t^n + a_{n-1}t^{n-1} + ... + a_0$ with coefficients belonging to a field k. Prove that this is a linear space.

Exercise 3.14. Consider a set $\mathrm{Map}(k,k)$ of all mappings from the field k to k. For any polynomial $P = a_n t^n + a_{n-1}t^{n-1} + ... + a_0$ and every $\lambda \in k$ define $\Psi_P(\lambda) = P(\lambda)$. We obtain the mapping $\Psi:\ k[t] \to \mathrm{Map}(k,k)$, $P \mapsto \Phi_P$. Prove that it is a homomorphism.

Exercise 3.15 (*). Let k be a finite field. Prove that $\Psi:\ k[t] \to \mathrm{Map}(k,k)$ is not a monomorphism. Prove that it is an epimorphism.

Exercise 3.16 (*). Let k be an infinite field. Prove that $\Psi:\ k[t] \to \mathrm{Map}(k,k)$ is a monomorphism.

Exercise 3.17 (*). Prove that it is not an epimorphism.

Consider a set A and a binary relation $\sim$ on A (that is, we state for certain pairs of elements $a, b \in A$ that $a \sim b$). It is said that $\sim$ is an **equivalence relation** if the following holds:

a. For any element $a \in A$ it is true that $a \sim a$.

b. If $a \sim b$ and $b \sim c$ then $a \sim c$ (transitivity).

c. If $a \sim b$ then $b \sim a$ (symmetry).

An equivalence relation $\sim$ having been defined an **equivalence class** of an element $a \in A$ is a set of all elements $a' \in A$ such that $a' \sim a$. It is easy to check that if $a \sim a'$ then the equivalence class of a is the same as the equivalence class of a'. So we can talk just about an equivalence class without mentioning a particular element a. A relation $a = b \mod n$ is an example of an equivalence relation of the set of natural numbers. The problem 3.8 can be reformulated as follows: "$V \cong V'$ is an equivalence relation".

Remark. We work with equivalence relation in Geometry 1 when considering Cauchy sequences, although we do not introduce this notion explicitly.

Exercise 3.18. Let V be a vector space and $V' \subset V$ be a subspace. Consider the following equivalence relation on V: $a \sim b$ iff $a + v = b$ for some $v \in V'$. Prove that the set of equivalence classes forms linear space.

Definition 3.5. This space is called a **quotient space** and is denoted by V/V'.

Exercise 3.19. Consider a natural mapping $V \to V/V'$ which maps an element to its equivalence class. Prove that this is a homomorphism and an epimorphism.

Exercise 3.20. Let $\varphi:\ V_1 \to V_2$ be a linear mapping and $V_0 \subset V_1$ be a set of elements that are mapped to zero.

a. Prove that V_0 is a linear subspace in V_1.

b. Prove that an image of φ – that is, a subset of all $v \in V_2$ of the form $\varphi(v')$, $v' \in V_1$ – is a linear subspace in V_2.

Definition 3.6. V_0 is called a **kernel of** φ.

Exercise 3.21. Let $\varphi:\ V_1 \to V_2$ be a linear operator. Prove that an image of φ is isomorphic to a quotient space V_1/V_0 where V_0 is a kernel of φ.

Linear hull, basis, dimension

Exercise 3.22. Let V be a vector space over the field k and $x_1, \ldots, x_n$ be vectors from V. Any vector of the form $v = \lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_m x_n$ is called **linear combination** of vectors $x_1, \ldots, x_n$ where λ_1 are arbitrary elements from k. Prove that linear combinations of vectors $x_1, \ldots, x_n$ form a linear subspace of V.

Definition 3.7. This subspace is called a **linear hull** of $x_1, \ldots, x_n$ and is denoted $\langle x_1, x_2, \ldots, x_n \rangle$. $\langle x_1, x_2, \ldots, x_n \rangle$ is called a subspace **generated** by vectors $x_1 \ldots, x_n$.

Exercise 3.23. Construct an epimorphism from k^n into $\langle x_1, x_2, \ldots, x_n \rangle$.

Hint. Map an n-tuple $(0, 0, 0, \ldots, 1, \ldots, 0) \in k^n$ (unity is in the l-th position) to x_l.

Definition 3.8. Vectors $x_1, \ldots, x_n$ are called **linear independent** vectors, if for any linear combination $v = \lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_m x_n$ such that there is at least one $\lambda_i \neq 0$, it is true that $v \neq 0$

Exercise 3.24. Let $x_1, \ldots, x_n$ be vectors from vector space V and φ be an epimorphism constructed in the exercise 3.23. Prove that φ is injective iff $x_1, \ldots, x_n$ are linearly independent vectors.

Definition 3.9. Let $x_1, \ldots, x_n$ be linearly independent vectors from a vector space V such that $V = \langle x_1, x_2, \ldots, x_n \rangle$. $x_1, \ldots, x_n$ is called a **basis of** the vector space V.

Exercise 3.25. Construct a basis of k^n.

Exercise 3.26. Prove that a vector space with a basis $x_1, \ldots, x_n$ is isomorphic to k^n.

Exercise 3.27. Let v be a non-zero vector from $V \cong k^n$, $\langle v \rangle$ be a subspace generated by it and $V/\langle v \rangle$ is a quotient space. Prove that $V/\langle v \rangle$ is isomorphic k^{n-1}.

Hint. Consider a subspace $V_l \subset V \cong k^n$, generated by n-tuples of the form

$$\langle \lambda_1, \lambda_2, \ldots, \lambda_{l-1}, 0, \lambda_{l+1}, \ldots, \lambda_n \rangle$$

(there is a 0 on the l-th position). This space is isomorphic to k^{n-1}. Prove that for some $l = 1, 2, \ldots, n$ the natural projection $V_l \to V/\langle v \rangle$ is an isomorphism.

Exercise 3.28. Let $x_1, \ldots, x_l$ be linearly independent vectors from $V \cong k^n$. Prove that $V/\langle x_1, x_2, \ldots, x_l \rangle$ is isomorphic to k^{n-l}

Hint. Use an inductive argument.

Exercise 3.29. Let $V_1 \subset V_2$ be a subspace of $V_2 \cong k^n$. Suppose that $V_1 \cong k^m$. Prove that $m \leqslant n$.

Exercise 3.30. Let $x_1, \ldots, x_l$ be a basis of $V \cong k^n$. Prove that $l = n$.

Exercise 3.31 (!). Let vector spaces k^l and k^m be isomorphic. Prove that $l = m$.

Definition 3.10. Vector space V over k is called a **finite-dimensional** if it is isomorphic to k^n. Number n is called a **dimension** of V. This is denoted by $\dim V = n$. It follows from the previous exercise that n is uniquely defined.

Exercise 3.32. Let $x_1, x_2, \dots, x_l$ be linearly independent vectors in a linear space V such that $V' := V/\langle x_1, x_2, \dots, x_l\rangle$ is a non-zero space. Let $x_{l+1} \in V$ be a vector such that its natural projection on V' is non-zero. Prove that $x_1, x_2, \dots, x_l, x_{l+1}$ are linearly independent vector.

Exercise 3.33 (!). Let V be a linear space which is not finite-dimensional. Prove that there exists an infinite sequence of linearly independent vectors $x_1, x_2, \dots, x_l, \dots \in V$.

Hint. Use the previous exercise.

Exercise 3.34 (!). Let $V \subset V'$ be a subspace of a finite dimensional vector space. Prove that V is finite-dimensional. Deduce that $\dim V \leqslant \dim V'$

Hint. Use the previous exercise.

Exercise 3.35. Let $V = V'/V''$ be a quotient space of finite dimensional space. Prove that V' is finite-dimensional. Prove that $\dim V \leqslant \dim V'$. Deduce that $\dim V' = \dim V + \dim V''$.

Hint. Use a proof by contradiction: consider an infinite sequence of linearly independent vectors from V and lift them to V'.

Exercise 3.36. Let $f : V \to V'$ be homomorphism of vector spaces of the same dimension n. Suppose that f is an injection or surjection. Prove that f is an isomorphism.

Linear forms, bilinear forms

Definition 3.11. Let V be a linear space over k. A **linear form** or **bilinear form** over V is a homomorphism of linear spaces V and k. The space of linear forms over V is denoted by V^*.

Exercise 3.37. Consider a finite-dimensional linear space V. Prove that $\dim V = \dim V^*$.

Exercise 3.38. Let k be a field and S be an arbitrary set. Is it true that $(k[S])^* \cong \mathrm{Map}(S, k)$?

Exercise 3.39 (!). Consider a natural map $V \stackrel{ev}{\to} V^{**}$, $v \mapsto (\lambda \mapsto \lambda(v))$, the vector $v \in V$ maps a form $\lambda \mapsto \lambda(v)$ to V^*. Let V be finite dimensional. Prove that $V \stackrel{ev}{\to} V^{**}$ is an isomorphism.

Hint. Prove that this is an injection and use the exercise 3.36.

Exercise 3.40 (**). Consider a infinite-dimensional linear space V. Prove that $V \stackrel{ev}{\to} V^{**}$ is not an isomorphism.

Definition 3.12. Let U, V, W be linear spaces over a field k. A mapping $U \times V \stackrel{\mu}{\to} W$, $u, v \mapsto \mu(u, v)$ is called **bilinear** if for every u the mappings $\mu(u, \cdot) : V \to W$ and $\mu(\cdot, u) : U \to W$ are linear.

Exercise 3.41. Prove that a sum of bilinear mappings is bilinear. Prove that a structure of vector space can be defined on the set of bilinear mappings $U \times V \to W$.

A space of bilinear mappings is denoted $\mathrm{Hom}(U \otimes V, W)$. The reason for that is the following:

Exercise 3.42 (*). Consider vector spaces U and V. Consider the set $U \times V$ and the vector space generated by it $k[U \times V]$. Let us denote the element of $k[U \times V]$ corresponding to the pair $\langle u, v\rangle \in U\times$ by $u \otimes v$. Consider the subspace generated by the vectors of the form $au \otimes v - a(u \otimes v)$, $u \otimes av - a(u \otimes v)$, $(u_1 + u_2) \otimes v - u_1 \otimes v - u_2 \otimes v$, $u \otimes (v_1 + v_2) - u \otimes v_1 - u \otimes v_2$ and denote the quotient space by $U \otimes V$. Prove that for any W the subspace $\mathrm{Hom}(U \otimes V, W)$ is isomorphic to the set of bilinear mappings from $U \times V$ to W.

The space $U \otimes V$ is called a **tensor product** of spaces U and V.

Exercise 3.43 (*). The dimensions of U, V, W are a, b, c. Find the dimension of $\mathrm{Hom}(U \otimes V, W)$.

Definition 3.13. Let V be a vector space over k. Bilinear form over V is a bilinear mapping $V \times V \xrightarrow{\mu} k$. A bilinear symmetric form is a form that satisfies the equality $\mu(x, y) = \mu(y, x)$. Bilinear antisymmetric form is a form is a form that satisfies the equality $\mu(x, y) = -\mu(y, x)$. We will denote the space of bilinear symmetric forms by S^2V^*, the space of bilinear antisymmetric forms by Λ^2V^* and the space of all bilinear forms by $(V \otimes V)^*$.

Definition 3.14. It is said that the characteristic of a field k is not 2 if the number $2 = 1 + 1$ is invertible in k.

Remark. Apparently, this is not true in a field of two elements.

Up to the end of this section we suppose that the characteristic of a field we are talking about is not 2.

Definition 3.15. If U, V are vector spaces then the product $U \times V$ of sets U and V is endowed with a natural structure of vector space. This product considered as a vector space is called a **direct sum of** U **and** V and is denoted $U \oplus V$.

Exercise 3.44. Consider two subspaces U, V of a vector space W such that intersection of U and W contains only $0 \in V$ and the linear hull over U and V is W. Prove that W is isomorphic to $U \oplus V$.

Remark. Notation that is used in that case: $W = U \oplus V$.

Exercise 3.45. Consider the symmetrization mapping that turns any bilinear form into symmetric form $\mathsf{Sym}(\mu)(x, y) = \frac{1}{2}(\mu(x, y)+\mu(y, x))$ and alternation mapping $\mathsf{Alt}(\mu)(x, y) = \frac{1}{2}(\mu(x, y)-\mu(y, x))$. Prove that these mappings are linear operators

$$(V \otimes V)^* \xrightarrow{\mathsf{Sym}} S^2V^*, \quad (V \otimes V)^* \xrightarrow{\mathsf{Alt}} \Lambda^2V^*$$

Prove that the sum

$$\mathsf{Sym} \oplus \mathsf{Alt} : \ (V \otimes V)^* \to S^2V^* \oplus \Lambda^2V^*$$

is an isomorphism.

Exercise 3.46 (*). Let $\dim V = n$. Find dimension of S^2V^* and Λ^2V^*.

Exercise 3.47. Let μ be a bilinear symmetric form. Prove that $\mu(u+v, u+v) = \mu(v, v)+\mu(u, u)+ 2\mu(u, v)$.

Exercise 3.48 (!). Let μ be a non-zero bilinear symmetric form over V. Prove that $\mu(x, x) \neq 0$ for some $x \in V$.

Hint. Use the previous exercise.

Definition 3.16. Consider V a linear space with a symmetric or antisymmetric bilinear form $\mu: V \times V \to k$ defined on it. For any $v \in V$, μ defines a linear form $\mu(v, \cdot): V \to k$. We say that v belongs to the radical **radical** of μ if this form equals zero.

Exercise 3.49 (*). Prove that a radical is a linear subspace of V.

Radical is denoted by $\mathsf{rad}\,\mu$.

Exercise 3.50 (*). Prove that $\mu(v + r, v' + r') = \mu(v, v')$ where $r, r' \in \mathsf{rad}\,\mu$.

Remark. It follows that μ is naturally defined on the quotient space $V/\mathsf{rad}\,\mu$.

Definition 3.17. A symmetric (or antisymmetric) form μ is called **non-degenerate** if its radical is zero. Non-degenerate bilinear antisymmetric form is called **symplectic**.

Exercise 3.51. Consider a non-degenerate symmetric (or antisymmetric) bilinear form μ defined on a finite-dimensional vector space V. Define the mapping $V \to V^*$, $v \mapsto \mu(v, \cdot)$ that maps v to the form $t \mapsto \mu(v, t)$. Prove that it is an isomorphism.

Hint. Prove that it is a monomorphism of spaces of the same dimension.

Exercise 3.52. Let μ be non-degenerate symmetric (or antisymmetric) bilinear form on the finite-dimensional space V and $\lambda: V \to k$ be a linear functional. Prove that there exists a vector $v \in V$ such that $\lambda(t) = \mu(v, t)$.

Hint. Use the previous exercise.

Definition 3.18. Let V be a space with a symmetric (or antisymmetric) bilinear form μ and be $V_1 \subset V$ its linear subspace. Define an **orthogonal complement** $V_1^\perp$ to be a set of all vectors $v \in V$ such that $\mu(v, v_1) = 0$ for all $v_1 \in V_1$.

Exercise 3.53 (!). Let μ be non-degenerate on V and on V_1. Suppose that V_1 is finite-dimensional. Then $V = V_1 \oplus V_1^\perp$.

Hint. That V_1 and $V_1^\perp$ do not intersect can be shown explicitly. It remains to prove that every vector $v \in V$ can be represented as the sum of vectors from V_1 and $V_1^\perp$. Consider $\mu(v, \cdot)$ as a functional over V_1. Use the previous exercise and find the vector $v_1 \in V_1$ such that a form $\mu(v - v_1, \cdot)$ is zero on V_1. It follows that $v - v_1 \in V_1^\perp$.

Exercise 3.54 (!). Deduce the following statement from the previous exercise. Let μ be a symmetric bilinear non-degenerate form on a vector space V. Then there exists a basis $x_1, \ldots, x_n$ in V such that $\mu(x_i, x_j) = 0$ for all $i \neq j$ and $\mu(x_i, x_i) \neq 0$ for all i.

Hint. Find a vector x such that $\mu(x, x) \neq 0$. Use the decomposition $V = \langle x \rangle \oplus \langle x \rangle^\perp$ from the previous exercise and apply an inductive argument.

Exercise 3.55 (*). Let μ be a bilinear symmetric form on V Then there exists a basis $x_1, \ldots, x_n$ in V such that $\mu(x_i, x_j) = 0$ for all $i \neq j$. Such basis is called an **orthogonal basis**.

Exercise 3.56 (*). Let μ be a symplectic form on the space V. Prove that V dimensions is even. Prove a basis $x_1, ..., x_{2n}$ in V such that

$$\mu(x_{2r-1}, x_{2r}) = -\mu(x_{2r}, x_{2r-1}) = 1$$

when $r = 1, 2, ..., n$ and $\mu(x_i, x_j) = 0$ for all other pairs (i, j).

Hint. The proof is analogous to the symmetric case .

Definition 3.19. Let V be a vector space over $\mathbb{R}$ and μ be a bilinear symmetric form on it. A form μ is called **positive** if $\mu(x, x) > 0$ for all non-zero vector x.

Exercise 3.57. Let μ be a positive bilinear form on V. Then there is a basis $x_1, \ldots, x_n$ in V such that $\mu(x_i, x_j) = 0$ for all $i \neq j$ and $\mu(x_i, x_i) = 1$ for all i.

Definition 3.20. Such basis is called **orthonormal**.

Exercise 3.58 (*). Let x, y be arbitrary vectors in a space V and μ be a positive bilinear form. Prove the inequality

$$\frac{\mu(x, x) + \mu(y, y)}{2} \geqslant \mu(x, y).$$

Exercise 3.59 (*). Prove the **Cauchy inequality**:

$$\sqrt{\mu(x, x)\mu(y, y)} \geqslant \mu(x, y).$$

Exercise 3.60 (*). Prove the **triangle inequality**

$$\sqrt{\mu(x, x)} + \sqrt{\mu(y, y)} \geqslant \sqrt{\mu(x + y, x + y)}.$$

ALGEBRA 4: algebraic numbers

Algebraic numbers

Definition 4.1. Let $k \subset K$ be a field contained in the field K (one says that k is a **subfield** of K and K is an **extension** of k). Element $x \in K$ is **algebraic over** k if x is a root of a non-zero polynomial with coefficients from k.

One often means complex numbers which are algebraic over $\mathbb{Q}$ (that is, roots of polynomials with rational coefficients)when saying simply "algebraic numbers" .

Exercise 4.1. Let k be a subfield in K and x be an element in K. Consider K as a linear space over k. Let $K_x \subset K$ be a linear subspace of K generated by the powers of x. Prove that K_x is finite dimensional iff x is algebraic.

Exercise 4.2. Let k be a subfield in K, x be an algebraic element of K nd $K_x \subset K$ be a linear subspace generated by powers of x. Consider an operation m_v of multiplication by a non-zero vector $v \in K_x$ defined on K. Prove that m_v is a k-linear mapping that preserves a subspace $K_x \subset K$.

Exercise 4.3. Consider the previous problem, prove that the restriction of m_v on $K_x \subset K$ is invertible.

Exercise 4.4 (!). Conclude that K_x is a subfield of K.

Definition 4.2. Finite extension of a field k is a field $K \supset k$ which is finite dimensional vector subspace over k.

Exercise 4.5. Let $K_1 \supset K_2 \supset K_3$ be fields such that K_1 is finite dimensional over K_2 which is finite dimensional over K_3. Prove that K_1 is a finite extension of K_3.

Exercise 4.6 (!). Conclude that the sum, the product and the factor of elements which are algebraic over k are also algebraic over k.

Exercise 4.7. Prove that any finite field is a finite extension of a field of remainders modulo p for some prime p. Conclude that a finite field has p^n elements (for some p, n, p is prime).

Exercise 4.8 (*). Prove that there exists a non-algebraic complex number.

Exercise 4.9 (**). Prove that the number $0,0100100001000000001...$ (there are 2^i zeros after the ith one) is non-algebraic.

Exercise 4.10 (*). Let the complex number x be algebraic. Prove that its conjugate $\overline{x}$ is also algebraic.

Hint. Use the fact that complex conjugation is an automorphism of $\mathbb{C}$ that preserves $\mathbb{Q}$.

Exercise 4.11 (*). Let the complex number $x = a + b\sqrt{-1}$ be algebraic. Prove that real numbers a and b are algebraic.

Algebraic closure

Exercise 4.12. Let $P(t), Q(t) \in k[t]$ be polynomials of a positive degree over a field k which are co-prime. Prove that 1 can be represented as a linear combination of P and Q over $k[t]$:

$$1 = Q(t)A(t) + P(t)B(t).$$

Hint. Use the algorithm of Euclid for polynomials.

Exercise 4.13. Let $P(t)$ be an irreducible polynomial (it cannot be represented as a product of polynomials of a positive degree with coefficients from k) and a product $Q(t)Q_1(t)$ is divisible by $P(t)$ where $Q(t)$, $Q_1(t)$ are non-zero polynomials. Prove that either $Q(t)$ or $Q_1(t)$ is divisible by $P(t)$.

Hint. Suppose $Q(t)$ is not divisible by $P(t)$. Use the previous exercise to represent 1 as a linear combination of $Q(t)$ and $P(t)$:

$$1 = Q(t)A(t) + P(t)B(t).$$

Then $1 \cdot Q_1(t) = Q(t)Q_1(t)A(t) + P(t)B(t)Q_1(t)$ is divisible by $P(t)$.

Exercise 4.14. Let $P(t)$ be a polynomial over k. Consider a ring $k[t]$ of polynomials of t and a quotient space $k[t]/Pk[t]$ of all polynomials factored by polynomials that are divisible by P. Prove that $k[t]/Pk[t]$ is a ring (with respect to naturally defined multiplication and addition).

Exercise 4.15. Prove that multiplication by a polynomial $Q(t)$ acts on $k[t]/Pk[t]$ as an endomorphism (an endomorphism is a homomorphism from a space to itself).

Exercise 4.16. Suppose that multiplication by $Q(t)$ maps all elements $k[t]/Pk[t]$ to zero. Prove that Q is divisible by P in the ring $k[t]$.

Exercise 4.17. Suppose that $P(t)$ is irreducible. Suppose that $Q(t)$ is a polynomial that is not divisible by $P(t)$. Prove that the operator m_Q of multiplication by $Q(t)$ on the space $k[t]/Pk[t]$ is a monomorphism.

Hint. Suppose v belongs to the kernel of m_Q and $Q_1(t)$ is a polynomial representing v. Then QQ_1 is divisible by P by the previous exercise statement. Use the algorithm of Euclid for polynomials to deduce that either Q is divisible by P or Q_1 is divisible by P.

Exercise 4.18 (*). Let $A: V \longrightarrow V$ be a linear operator. Prove that there exists a polynomial $P(t) = t^n + a_n t^{n-1} + ...$ such that $P(A) = 0$. Is it possible in general to find an irreducible polynomial $P(t)$ such that $P(A) = 0$?

Exercise 4.19 (!). Let $P(t)$ be irreducible. Prove that $k[t]/Pk[t]$ is a field.

Hint. Use the previous exercise to prove that if Q is not divisible by P then multiplication by $Q(t)$ defines an invertible linear operator on $k[t]/Pk[t]$.

Definition 4.3. Let $P(t)$ be an irreducible polynomial. We say that the field $k[t]/Pk[t]$ is an **extension obtained by adding the root** $P(t)$.

Definition 4.4. Algebraic extension of a field k is a field $K \supset k$ such that all elements of K are algebraic over k.

Exercise 4.20. Prove that any finite extension is algebraic.

Exercise 4.21 (*). Prove that not every algebraic extension is finite.

Definition 4.5. Let k be a field. The field k is called **algebraically complete** if any polynomial of a positive degree $P \in k[t]$ has a root in k.

Definition 4.6. Algebraic closure of a field k is an algebraic extension $\overline{k} \supset k$ which is algebraically complete.

Exercise 4.22 (*). Let K be an extension of the field k and $z \in K$ is a root of a non-zero polynomial $P(t)$ with coefficients which are algebraic over k. Prove that z is algebraic over k.

Exercise 4.23 (*). Suppose K is an algebraic extension of the field k such that any polynomial $P(t) \in k[t]$ has a root in K. Prove that any polynomial $P(t) \in k[t]$ can be represented as a product of linear polynomials from $K[t]$.

Exercise 4.24 (*). Take the statement of the previous exercise and prove that K is algebraically complete.

Hint. Let $P \in K[t]$ be an irreducible polynomial with coefficients K. Add its root α to K. Using the exercise 4.22 we obtain that α is algebraic over k. Then α is a root of a polynomial from $k[t]$. Every such polynomial can be represented as a product $\prod(t - \alpha_i)$, $\alpha_i \in K$ as follows from the previous exercise. Deduce that $\alpha \in K$.

Exercise 4.25 (*). Prove that any field k has an algebraic closure.

Hint. Take any algebraic extension of the field k. If it is algebraically complete then the proof is over. Otherwise there exists a polynomial $P(t) \in k[t]$ which has no roots in K. Add its root to K and obtain a field K_1. Now consider K_1 instead of K and prove the statement for it. After having applied this argument as many times as it would be necessary consider the union of all algebraic extensions of k. We have obtained a field that contains a root of any polynomial from $k[t]$. Use the previous exercise to ensure that this field is algebraically closed.

Exercise 4.26 (**). In the proof sketch for the previous exercise we have used implicitly the Zorn's lemma. Find a proof for a countable field k that does not use Zorn's lemma and therefore does not depend on the axiom of choice.

Exercise 4.27 (**). Can you prove existence of an algebraic closure for an arbitrary field without using the axiom of choice?

Exercise 4.28 (**). Prove that algebraic closure of a field is unique up to isomorphism.

ALGEBRA 5: Algebras over a field

Algebras over a field

From now on we work with a fixed field k.

Recall that a mapping $(V_1 \times V_2) \xrightarrow{\mu} V_2$ of vector spaces is called **bilinear**, if for any $v_1 \in V_1$, $v_2 \in V_2$, the mappings

$$\mu(v_1, \cdot) : V_2 \longrightarrow V_3, \ \mu(\cdot, v_2) : V_1 \longrightarrow V_3$$

(one argument is fixed, another takes values in V_2, V_1 respectively) are linear. It is said that bilinear mapping is a mapping which is "linear in both arguments". A symbol of tensor multiplication is used to denote bilinear mappings, for example, the mapping just mentioned is denoted

$$\mu : V_1 \otimes V_2 \longrightarrow V_3.$$

Definition 5.1. Let A be a vector space over a field k and $\mu : A \otimes A \longrightarrow A$ be a bilinear operation ("multiplication"). (A, μ) is called an **algebra over** k, if μ is associative:

$$\mu(a_1, \mu(a_2, a_3)) = \mu(\mu(a_1, a_2), a_3)).$$

Multiplication in an algebra is usually denoted like this: $a \cdot b$. If there is an element 1 in an algebra such that $\mu(1, a) = \mu(a, 1) = a$ for all $a \in A$ then this element is called a **unit**, and an algebra is called **algebra with unit**. A **homomorphism** $r : A \longrightarrow A'$ of algebras is a linear mapping which preserves multiplication and an **isomorphism** of algebras is an invertible homomorphism. **Subalgebra** of an algebra is a linear subspace which is closed under multiplication.

Exercise 5.1. Consider an algebra with unit such that for all a, b it is true that $\mu(a, b) = \mu(b, a)$. Prove that this is a (commutative) ring.

Exercise 5.2. Give an example of an algebra without a unit.

Exercise 5.3. Prove that unit is unique.

Exercise 5.4 (*). Give an example of non-commutative algebra with unit.

Exercise 5.5. Let V be a vector space and $\mathrm{End}(V)$ be a space of linear homomorphisms from V to V with an operation of composition. Prove that $\mathrm{End}(V)$ is an algebra.

Definition 5.2. $\mathrm{End}(V)$ is called a **matrix algebra** and is denoted $\mathrm{Mat}(V)$.

Exercise 5.6. Is $\mathrm{Mat}(V)$ commutative?

Exercise 5.7. Consider an isomorphism of matrix algebras $\mathrm{Mat}(V) \cong \mathrm{Mat}(V')$.

a. Suppose that V, V' are finite-dimensional. Prove that V, V' are isomorphic. Find a set of all isomorphisms $a : V \longrightarrow V'$ which are compatible with a given isomorphism $\mathrm{Mat}(V) \cong \mathrm{Mat}(V')$.

b. **(*)**Prove that $V \cong V'$ for any V, V' (possibly infinite- dimensional). Use Zorn's Lemma. [1]

[1]We mean the following statement. Suppose that a system S of subsets of V is defined, and suppose that it satisfies the following conditions:

(a) For any $V_\alpha \in S$ which is not equal to all V, there is a subset $V_{\alpha'}$ in S which contains V_α but is not equal to it.

(b) Consider a collection $S' \subset S$ of subsets of V such that any $V_\alpha, V_{\alpha'} \in S'$ are contained one in another: either $V_\alpha \subset V_{\alpha'}$, or $V_{\alpha'} \subset V_\alpha$. Then a union $V_{\alpha_i} \in S'$ also belongs to S

If these conditions hold V is contained in S. Zorn's lemma is a corollary of the axiom of choice.

c. **(**)**Is it possible to prove (b) without axiom of choice?

Exercise 5.8 (!). Consider an algebra A with unit. Prove that A can be realized as a subalgebra of $\operatorname{Mat} V$ for some vector space V (possibly infinite dimensional).

Hint. Take $V = A$.

Definition 5.3. An algebra A with a unit is called a **division algebra**, if $A\backslash 0$ is a multiplication group. In other words A is called a division algebra, if all non-zero elements A are invertible.

Exercise 5.9. Let $\mathbb{H}$ be a four dimensional vector space over $\mathbb{R}$ with a basis $1, I, J, K$. Prove that there exists a unique algebra structure on $\mathbb{H}$ such that

1. $1 \cdot a = a$ for all $a \in \mathbb{H}$,
2. $I^2 = J^2 = K^2 = -1$,
3. $I \cdot J = -J \cdot I = K$.

Definition 5.4. Algebra $\mathbb{H}$ is called a **quaternion algebra**.

Exercise 5.10 (!). Consider "complex conjunction" map $z \longrightarrow \overline{z}$, defined on $\mathbb{H}$ as follows

$$a + bI + cJ + dK \longrightarrow a - bI - cJ - dK.$$

Prove that $\overline{z_1 z_2} = \overline{z}_2 \overline{z}_1$.

Exercise 5.11. Prove that $z\overline{z} = a^2 + b^2 + c^2 + d^2$, if $z = a + bI + cJ + dK$.

Exercise 5.12 (!). Prove that $\mathbb{H}$ is a division algebra.

Hint. Use the argument that was used to prove invertibility of complex numbers.

Exercise 5.13. Replace the equality $I^2 = J^2 = K^2 = -1$ with $I^2 = -1$, $J^2 = K^2 = 1$ in the statement of the problem 5.9, replace the second equality with $I \cdot J \cdot K = -1$. Prove that you still get an algebra structure on $\mathbb{R}^4$ (this algebra is called the **algebra of para-quaternions**). Is it a division algebra?

Exercise 5.14 (*). Prove that the algebra of para-quaternions is isomorphic to $\operatorname{Mat}(\mathbb{R}^2)$.

Exercise 5.15. Prove that a finite-dimensional algebra A with unity is a division algebra iff it has no divisors of zero.

Algebras defined by generators and relations

Consider a vector space V over k. A multilinear form φ on V is a mapping $V \times V \times V \times \ldots \longrightarrow k$ which is linear in each of its arguments. We denote it like this:

$$\varphi : V \otimes V \otimes V \otimes \ldots \longrightarrow k.$$

If φ, ψ are multilinear i-form and multilinear j-form then the mapping

$$\varphi \otimes \psi : \underbrace{V \times V \times V \times \ldots}_{i+j} \longrightarrow k,$$

defined as

$$(\varphi \otimes \psi)(v_1, v_2, \ldots, v_{i+j}) = \varphi(v_1, \ldots, v_i)\varphi(v_{i+1}, \ldots, v_{i+j})$$

is apparently multilinear. This defines multiplication on the space of multilinear forms.

Exercise 5.16. Prove that a direct sum $\oplus_i \mathcal{M}^i V$ of spaces of i-linear forms $\mathcal{M}^i V$ forms an algebra with respect to multiplication as defined above.

Exercise 5.17. Let V be finite-dimensional. Prove that any element of the algebra of multilinear forms can be represented as a linear combination of products of elements of V^* (we say that the algebra is **generated by** V^*).

Definition 5.5. Let V, W be vector spaces over k. Consider a space $U = \langle V \times W \rangle$, freely generated by pairs of vectors $v, w \in V, W$. We will denote vectors from U which correspond to v, w as $v \otimes w$. Let us take a quotient of U by a subspace generated by the following elements:

$$\begin{aligned} (\lambda v) \otimes w - \lambda(v \otimes w), \qquad & v \otimes (\lambda w) - \lambda(v \otimes w), \qquad & \lambda \in k \\ (v + v') \otimes w - v \otimes w - v' \otimes w, \qquad & v \otimes (w + w') - v \otimes w - v \otimes w'. \end{aligned}$$

The quotient space we obtain is called a **tensor product of** V **and** W and is denoted $V \otimes W$.

Exercise 5.18 (!). Prove that $(V \otimes W)^*$ is naturally isomorphic to a space of bilinear forms over (V, W).

Exercise 5.19. Find a number of dimensions of $V \otimes W$ when $\dim V = n$, $\dim W = m$. Prove that $V \otimes W^*$ is naturally isomorphic to a space of homomorphisms from W to V.

Exercise 5.20 (!). Prove that $U \otimes (V \otimes W)$ is canonically isomorphic to $(U \otimes V) \otimes W$.

Remark. This statement allows to omit brackets: we write $U \otimes V \otimes W$ which can be interpreted with any possible bracketing.

Remark. A tensor product V with itself i times is denoted as $V^{\otimes i}$. An isomorphism of associativity constructed above allows to endow $\bigoplus_i V^{\otimes i}$ with associative multiplication

$$V^{\otimes i} \times V^{\otimes j} \longrightarrow V^{\otimes j+j}$$

Definition 5.6. The **free** (or **tensor**) algebra, generated by V is an algebra $\bigoplus_i V^{\otimes i}$ with multiplication as defined above. This algebra is denoted as $T(V)$. $V^{\otimes 0}$ is naturally interpreted as k. It follows that $T(V)$ is an algebra with unit.

Exercise 5.21 (!). Let V be a finite-dimensional vector space. Prove that $T(V)$ is isomorphic to the algebra of multilinear forms on V^*.

Exercise 5.22 (*). Consider a linear mapping from V into some algebra A. Prove that is can be uniquely extended to a homomorphism of algebras $T(V) \longrightarrow A$.

Exercise 5.23 (!). Let $\langle x_i \rangle$ be a basis in V. Prove that all the monomials of the form $x_{i_1} x_{i_2} x_{i_3} \cdots$ define a basis in $T(V)$.

Exercise 5.24 (!). Consider a vector space V over k (a "generator space") and a subspace $W \subset T(V)$ (a "relations space"). Consider a quotient space of $T(V)$ over the space $T(V)WT(V)$ generated by the vectors of the form vwv' where $w \in W$. Let this space be nonempty. Prove that this quotient space carries a natural structure of an algebra with unit.

Definition 5.7. In the previous problem setting let x_i be a basis in V and w_i be a basis in W. Every relation $w_i = 0$ can written down using a non-commutative polynomial of the form

$$\sum_I \alpha_{i_1,\dots,i_n} x_{i_1} x_{i_2} \cdots = 0$$

where the sum is taken over some set of multiindices and $\alpha_{i_1,\dots,i_n}$ are coefficients from the field k. An algebra $T(V)/T(V)WT(V)$ is called an **algebra defined by generators** v_i **and relations** w_i.

Exercise 5.25. Prove that any algebra with unit A can be defined by generators and relations. Prove that if A is finite-dimensional then generator space V and relation space W can be made finite-dimensional too.

Hint. Take $A = V$.

Definition 5.8. An algebra is called **finitely generated** if it can be defined by generators and relations in such a way that relations generator space is finite-dimensional V. An algebra is called **finitely presented** if it can be defined in such a way that relations space W is also finite-dimensional.

Exercise 5.26. Give an example of an algebra that is not finitely presented.

Exercise 5.27 (*). Is it true that any finitely generated algebra is finitely presented?

Exercise 5.28. Prove that algebra $\mathrm{Mat}(\mathbb{R}^2)$ is finitely presented.

Exercise 5.29. Define an algebra of Laurent polynomials $k[t, t^{-1}]$ by generators and relations.

Definition 5.9. Let V be a vector space with a bilinear symmetric form $g : V \otimes V \longrightarrow \mathbb{R}$. Consider an algebra $Cl(V)$, generated by V and defined by relations of the form

$$v_1 \cdot v_2 + v_2 \cdot v_1 = g(v_1, v_2) \cdot 1,$$

where v_1, v_2 passes through V. This algebra is called a **Clifford algebra** over the field k.

Exercise 5.30. Define complex numbers as a Clifford algebra over $\mathbb{R}$.

Exercise 5.31. Find all Clifford algebras over $\mathbb{R}$ for $\dim V = 1, 2$.

Exercise 5.32 (!). Define quaternions and para-quaternions as a Clifford algebra over $\mathbb{R}$.

Exercise 5.33 (*). Let the dimension of V is n. What is the dimension of $Cl(V)$ as a vector space?

Exercise 5.34 (**). Define an algebra $\mathrm{Mat}(\mathbb{R}^{2^n})$ as a Clifford algebra.

ALGEBRA 6: Grassmann algebra and determinant

Grassmann algebra

Definition 6.1. An algebra A is called **graded**, if A can be represented in the form $A = \oplus_{i=1}^{\mathbb{Z}} A^i$ and the multiplication satisfies the following condition: $A^i \cdot A^j \subset A^{i+j}$. $\oplus_i A^i$ is often written as $A^\bullet$, which means a direct sum over all possible indices. Some A^i subspaces can be empty. Algebra unit (if it exists) always belongs to A^0.

Exercise 6.1. What is the natural grading of $T(V)$?

Definition 6.2. A subspace $W \subset A^\bullet$ of a graded algebra is called **graded** or **homogeneous**, if W is a direct sum of components of the form $W^i \subset A^i$.

Exercise 6.2 (!). Consider a graded subspace $W \subset T(V)$. Prove that algebra defined by the relations space W is graded.

Exercise 6.3. Consider a vector space V and its basis $\langle x_i \rangle$. Consider a subspace $W \subset V \otimes V$ generated by vectors of the form $x \otimes y - y \otimes x$. Prove that an algebra of polynomials $k[x_1, \dots, x_n]$ is defined by generators V and relations W. Describe a natural grading inherited from $T(V)$.

Definition 6.3. The algebra obtained is called **symmetric algebra of space** V, and is denoted as $\mathsf{Sym}^\bullet(V)$.

Exercise 6.4. Let $\dim V > 1$. Are there an injective algebra homomorphism $\mathsf{Sym}^\bullet(V) \longrightarrow T(V)$.

Definition 6.4. Consider a vector space V and a graded subspace $W \subset V \otimes V$ generated by vectors of the form $x \otimes y + y \otimes x$ and vectors of the form $x \otimes x$. The graded algebra defined by the generators space V and relations space W is called a **Grassmann algebra** and is denoted as $\Lambda^\bullet(V)$. The space $\Lambda^i(V)$ is called an **i-th exterior power** of the space V and the operation of multiplication in Grassmann algebra is called **exterior multiplication**. Exterior multiplication is usually denoted as $\wedge$.

Remark. Elements of Grassmmann algebra can be thought of as "anticommutative polinomials" on V.

Remark. Grassmann algebra is a particular case of Clifford algebra defined in Algebra 5.

Exercise 6.5. Prove that $\Lambda^1 V$ is isomorphic to V.

Exercise 6.6. Consider a finite-dimensional space V. Prove that $\Lambda^2(V)^*$ is isomorphic to a space of bilinear antisymmetric forms on V.

Exercise 6.7. Consider a subalgebra $\Lambda^{2\bullet}(V) \subset \Lambda^\bullet(V)$ that consists of linear combinations of vectors of even grading. Prove that this subalgebra is commutative.

Definition 6.5. Vector $\Lambda^\bullet(V)$ is called **even**, if it belongs to an even grading component and **odd** if it belongs to an odd component. A **parity** $\tilde{x}$ of a vector x is defined to be zero for an even x and 1 for an odd x. .

Exercise 6.8 (!). Prove that $xy = (-1)^{\tilde{x}\tilde{y}} yx$.

Exercise 6.9 (*). Find all elements $\eta \in \Lambda^2(V)$ such that $\eta^2 = 0$.

Exercise 6.10 (!). Let $x_1, x_2, \dots$ be a basis in $V \cong \Lambda^1 V$. Denote the product of vectors that belong to the basis in $\Lambda^\bullet(V)$ as $x_{i_1} \wedge x_{i_2} \wedge x_{i_3} \wedge \cdots$. Prove that vectors of the form $x_{i_1} \wedge x_{i_2} \wedge x_{i_3} \wedge \cdots$ where $i_1 < i_2 < i_3 < \dots$, define a basis in $\Lambda^\bullet(V)$.

Exercise 6.11 (!). Let V be a d-dimensional vector space. Find $\dim \Lambda^i(V)$. Prove that $\Lambda^d V$ is one-dimensional.

Definition 6.6. The space $\Lambda^d V$ is called a **space of determinant vectors in** V.

Exercise 6.12 (!). Let V be a d-dimensional vector space, $x_1, x_2, \dots, x_d$ be its basis and $\det := x_1 \wedge x_2 \wedge x_3 \cdots \wedge x_d$ be a determinant vector in $\Lambda^d V$. Consider a permutation $I = (i_1, i_2, \dots, i_d)$ and consider a vector $I(\det) := x_{i_1} \wedge x_{i_2} \wedge x_{i_3} \cdots \wedge x_{i_d}$. Prove that $I(\det) = \pm \det$. Prove that this correspondence defines a homomorphism from a permutation group S_n into $\{\pm 1\}$. Prove that this homomorphism maps a product of an odd number of transpositions to -1 and a product of even number of transpositions to 1.

Definition 6.7. A homomorphism constructed above $S_n \xrightarrow{\sigma} \mathbb{Z}/2\mathbb{Z}$ is called a **sign** of a permutation. The additive notation is used here for historical reasons. It is said that a permutation is **even** if its sign is 0 and is **odd** if its sign is 1.

Exercise 6.13. Consider a permutation decomposed into cycles as follows:

$$I = (i_{1,1}, i_{2,1} \dots i_{k_1,1})(i_{1,2}, i_{2,2} \dots i_{k_2,2}) \dots$$

where cycles are of length k_1, k_2 etc. Prove that I is even iff there is an even number of even k_i-s.

From now till the end of the section we suppose that the field k we are using is of characteristic 0.

Definition 6.8. Let $\eta \in V^{\otimes i}$ be a vector of a i-th tensor power of the space V. Consider a natural action of S_i on $V^{\otimes i}$. Define $\mathsf{Alt}(\eta)$ as

$$\mathsf{Alt}(\eta) := \frac{1}{i!} \sum_{I \in S_i} (-1)^{\sigma(I)} I(\eta).$$

This operation is called **alternation**. It is said that a vector $\eta \in V^{\otimes i}$ is **totally antisymmetric** if $\eta = \mathsf{Alt}(\eta)$.

Exercise 6.14. Let $\eta = \frac{1}{i!} \sum_{I \in S_i} I(\eta)$. Prove that $I(\eta) = \eta$ for any permutation $I \in S_i$.

Exercise 6.15 (!). Consider a totally antisymmetric vector $\eta \in V^{\otimes i}$. Prove that $I(\eta) = (-1)^{\sigma(I)} \eta$ for any permutation $I \in S_i$.

Exercise 6.16 (!). Prove that $\mathsf{Alt}(\mathsf{Alt}(\eta)) = \mathsf{Alt}(\eta)$ for any η.

Exercise 6.17. Consider a tensor $x_{i_1} x_{i_2} \cdots x_{i_k} \in V^{\otimes_i}$. Prove that

$$\mathsf{Alt}(x_{i_1} x_{i_2} \dots x_{i_k}) = -\mathsf{Alt}(x_{i_1} x_{i_2} \dots x_{i_l} x_{i_l - 1} \dots x_{i_k})$$

(x_{i_l} is permuted with $x_{i_l - 1}$ in the second expression).

Exercise 6.18. Prove that the map $x_{i_1}x_{i_2}\dots x_{i_k} \longrightarrow \mathsf{Alt}(x_{i_1}x_{i_2}\dots x_{i_k})$ vanishes on all tensors of the form awb, where w belongs to the relations space of $\Lambda^\bullet(V)$. Deduce that there exists a natural map $\Lambda^i(V) \longrightarrow R^i$ from $\Lambda^i(V)$ to the space of totally antisymmetric tensors.

Exercise 6.19 (!). Prove that the natural map constructed above $\Lambda^i(V) \longrightarrow R^i$ is a bijection.

Exercise 6.20 (!). We put $\Lambda^i(V)$ into one-to-one correspondence with the space of totally antisymmetric tensors. It defines a multiplicative structure on antisymmetric tensors. Prove that this multiplicative structure can be defined like this: take two totally antisymmetric tensors $\alpha, \beta \in T(V)$, multiply them in $T(V)$ and apply Alt to the result.

Exercise 6.21. Consider two algebras A and B over a field k. Define a multiplicative structure on $A \otimes B$ like this: $a \otimes b \cdot a' \otimes b' = aa' \otimes bb'$. Prove that this multiplication indeed defines an algebra structure on $A \otimes B$.

Definition 6.9. A tensor product of algebras A and B is a space $A \otimes B$ with multiplicative structure defined above. If the algebras are graded, then the grading on the tensor product is defined by the formula $(A \otimes B)^n = \oplus_{i+j=n} A^i \otimes B^j$.

Exercise 6.22 (!). Let V_1, V_2 be vector spaces. Prove that $\mathsf{Sym}^\bullet(V)$ is isomorphic (as an algebra) to $\mathsf{Sym}^\bullet(V_1) \otimes \mathsf{Sym}^\bullet(V_1)$. Prove that $\Lambda^\bullet(V_1 \oplus V_2)$ and $\Lambda^\bullet(V_1) \otimes \Lambda^\bullet(V_2)$ are isomorphic as vector spaces. Is this isomorphism an isomorphism of algebras?

Exercise 6.23. Prove that $\dim \Lambda^\bullet(V) = 2^{\dim V}$.

Hint. Use the previous problem.

Exercise 6.24 (*). Consider a mapping

$$V \otimes \Lambda^i(V) \xrightarrow{\wedge} \Lambda^{i+1}(V),$$

defined by the formula $x \otimes \eta \mapsto x \wedge \eta$. For some fixed η we get a linear operator $L_\eta : V \longrightarrow \Lambda^{i+1}(V)$. Prove that for $\eta \neq 0$ an inequality $\dim \ker L_\eta \leqslant i$ holds.

Exercise 6.25 (*). Suppose in the previous problem setting an equality $\dim \ker L_\eta = i$ holds. Prove that in this case η can be represented as $\eta = x_1 \wedge x_2 \wedge \dots \wedge x_i$ for some vectors $x_1, \dots, x_i \in V$.

Exercise 6.26 (*). Let $P \in \mathsf{Sym}^i(V^*)$ be a symmetric i-form on V. Suppose that $P(v, v, v, \dots) = 0$ for all $v \in V$. Is it possible that P is non-zero?

Determinant

Exercise 6.27. Consider a one-dimensional vector space V over k. Prove that $\operatorname{End} V$ is naturally isomorphic to k.

Exercise 6.28 (!). Consider a linear space V and a linear operator $A \in \operatorname{End}(V)$. Prove that A on $V \cong \Lambda^1 V$ can be uniquely extended to a grading preserving homomorphism from $\Lambda^\bullet V$ to itself.

Definition 6.10. Consider a d-dimensional vector space V over k and a linear operator $A \in \operatorname{End}(V)$. Consider a endomorphism induced by A defined on a space of determinant vectors:

$$\det A \in \operatorname{End}(\Lambda^d(V))$$

Since $\Lambda^d(V)$ is one-dimensional, $\operatorname{End}(\Lambda^d(V))$ is naturally isomorphic to k. This allows to treat $\det A$ as a number, i.e. an element of k. This number is called a **determinant** of a linear operator A.

Exercise 6.29 (!). Consider a set of d vectors $x_1, \dots, x_d$ in a vector space V. Prove that their product $x_1 \wedge x_2 \wedge \dots$ in $\Lambda^\bullet(V)$ is zero iff these vectors are linearly dependent.

Exercise 6.30. Consider an operator $A \in \operatorname{End}(V)$ which has a non-zero kernel (such an operator is called **singular** of **degenerate**). Prove that $\det A = 0$.

Exercise 6.31. Let an operator $A \in \operatorname{End}(V)$ be invertible (such an operator is called **nonsingular** or **nondegenerate**). Prove that $\det A \neq 0$.

Exercise 6.32 (!). Prove that det defines a homomorphism from a group $GL(V)$ of invertible matrices to k^*, a multiplicative group of all nonzero elements of k.

Exercise 6.33 (!). Consider vector spaces V and V', and endomorphisms A, A'. Then $A \oplus A'$ defines an endomorphism $V \oplus V'$. Prove that $\det(A \oplus A') = \det A \det A'$.

Exercise 6.34. Consider a finite-dimensional vector space V, endowed with a positive bilinear symmetric form g. Recall that an endomorphism $A \in \operatorname{End} V$ is called **orthogonal** if it preserves g, i.e. for any $x, y \in V$ it is true that $g(Ax, Ay) = g(x, y)$. Prove that an orthogonal operator is always invertible. Consider an orthogonal operator in $\mathbb{R}^2$. What values can $\det A$ can take?

Exercise 6.35 (*). Consider a vector space V endowed with

a. nondegenerate bilinear symmetric form g

b. nondegenerate bilinear antisymmetric form g

c. **(**)** nondegenerate bilinear form (i.e. an isomorphism $g: V \longrightarrow V^*$).

Consider a linear operator $A \in \operatorname{End}(V)$ that preserves g. Prove that A is invertible in any of the aforementioned cases and find all the values that $\det A$ can take.

ALGEBRA 7: matrices and determinants

We suppose that all vector spaces are vector spaces over a field k.

Exercise 7.1. Let $v_1, \dots, v_n \in V$, $w_1, \dots, w_m \in W$ be bases in vector spaces V and W. Consider a homomorphism e_i^j from V to W that maps v_i to w_j and maps v_k to zero for $k \neq i$. Prove that e_j^i form a basis in the space of homomorphisms $\mathrm{Hom}(V, W)$.

Definition 7.1. In the previous problem setting consider a homomorphism $\gamma \in \mathrm{Hom}(V, W)$. Consider $\gamma = \gamma_j^i e_j^i$, $\gamma_j^i \in k$. The matrix

$$\begin{pmatrix} \gamma_1^1 & \dots & \gamma_n^1 \\ \vdots & \ddots & \vdots \\ \gamma_1^m & \dots & \gamma_n^m \end{pmatrix}$$

is called the **matrix of the homomorphism** γ.

Exercise 7.2. Consider homomorphisms $a \in \mathrm{Hom}(U, V)$, $b \in \mathrm{Hom}(V, W)$ defined by the matrices (a_j^i), (b_l^k). Prove that the composition of a and b is defined by the matrix $c_k^i = \sum_j a_j^i b_k^j$.

Remark. Note that the matrix product formula makes sense for matrices of elements of an arbitrary ring.

Exercise 7.3. Consider the space A of square matrices of the size $n \times n$, with the multiplication $A \times A \longrightarrow A$ defined by the formula $(a_j^i) \circ (b_l^k) \longrightarrow \sum_j a_j^i b_k^j$. Prove that this is an algebra with unit. Prove that this algebra is isomorphic to the algebra of linear operators from k^n to k^n.

Definition 7.2. This algebra is called the **matrix algebra** and is denoted $\mathrm{Mat}(n)$. The unit element of this algebra (the diagonal matrix with $a_i^i = 1$) is called the **identity matrix** and is denoted Id.

Exercise 7.4. Consider a linear operator $f \in \mathrm{Hom}(V, V)$ and let $v_1, \dots, v_n$ be a basis of V and (f_j^i) be the matrix of f. Consider another basis $v_1', \dots, v_n'$ of V. Prove that there exists a unique operator g that maps v_i to v_i', and g is invertible. Let (g_j^i), $((g^{-1})_j^i)$ be the matrices of g and g^{-1}. Prove that f is defined by the matrix $h_j^i := (g_j^i) \circ (f_j^i) \circ ((g^{-1})_j^i)$ in the basis $v_1', \dots, v_n'$.

Definition 7.3. In that case the matrices (h_j^i), (f_j^i) are said to be **equivalent**.

Exercise 7.5. Find all the matrices equivalent to $c\,\mathsf{Id}$ where $c \in k$.

Exercise 7.6 (!). Consider a matrix $E(i, j)$

$$\begin{pmatrix} 0 & \dots & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & 1 & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & \dots & 0 \end{pmatrix},$$

which has 1 on the position i, j and has 0 everywhere else. What are the values of i, j, i', j' that make the matrices $E(i, j)$ and $E(i', j')$ equivalent?

Exercise 7.7 (!). Consider a matrix A which is equivalent to $E(i, j)$. Prove that all rows of A are proportional. Prove that all columns of A are proportional.

Exercise 7.8 (*). Prove that if all rows and columns of A are proportional, then A is equivalent to $E(i,j)$.

Definition 7.4. Consider a vector space V and an endomorphism $A \in \mathrm{End}(V)$ over it (i.e. a homomorphism from V to itself) and its dual space V^*. An operator $A^* : V^* \longrightarrow V^*$ that maps a linear functional $\gamma \in V^*$ to the linear functional $A^*(\gamma)(v) = \gamma(A(v))$ is called a **conjugate operator** for A.

Exercise 7.9. Consider a finite-dimensional vector space V and its dual space V^*. Construct the natural isomorphism between $\Lambda^k(V)^*$ and $\Lambda^k(V^*)$.

Remark. "Natural" means that it does not require any extra choice (choice of base, for example). In this situation, a natural isomorphism $\Lambda^k(V)^* \cong \Lambda^k(V^*)$ is permutable with the standard action of $GL(V)$ on $\Lambda^k(V)^*$, $\Lambda^k(V^*)$. The spaces V and V^* are isomorphic, but one can prove that there is no $GL(V)$-invariant isomorphism $V \cong V^*$. In other words it is *impossible* to construct a natural homomorphism $V \cong V^*$.

Exercise 7.10 (!). Consider a vector space V, an endomorphism $A \in \mathrm{End}(V)$ and the conjugate operator A^*. Prove that $\det A^* = \det A$.

Hint. Use the previous problem.

Definition 7.5. Consider a square matrix (A^i_j) and a matrix (B^i_j), that is constructed from (A^i_j) by reflecting it over the diagonal: $B^i_j = A^j_i$. Then (B^i_j) is called the **transposed matrix** of (A^i_j), and is denoted $(A^i_j)^\perp$.

Exercise 7.11 (!). Consider a basis $v_1, \dots, v_n$ in V and a dual basis $v^1, \dots, v^n$ in V^* (v^i maps v_i to 1 and maps other v_js to zero). Consider an operator $A \in \mathrm{End}(V)$ and its matrix (A^i_j). Prove that A^* is given as the matrix $(A^i_j)^\perp$.

Definition 7.6. Consider a nondegenerate bilinear symmetric form g defined on a vector space V. An operator $A \in \mathrm{End}(V)$ is called **orthogonal with respect to** g (or simply **orthogonal**) iff $g(Av, Av) = g(v, v)$ for any $v \in V$.

Exercise 7.12 (!). Prove that any orthogonal operator is invertible.

Exercise 7.13 (!). Consider a linear operator $A \in \mathrm{End}(V)$ on a vector space endowed with a nondegenerate bilinear symmetric form g. Identify V and V^* using g. Then the dual operator A^* can be considered as an endomorphism of V. Prove that a linear operator A is orthogonal iff $A^{-1} = A^*$.

Exercise 7.14 (!). Prove that the determinant of an orthogonal operator equals ± 1.

Definition 7.7. A nondegenerate bilinear antisymmetric form (see ALGEBRA 3) is called a **symplectic form**.

Exercise 7.15 (*). Consider a vector space V with a symplectic form ω defined on it. An operator $A \in \mathrm{End}(V)$ is called **symplectic**, if it preserves ω, i.e. if $\omega(Av, Av) = \omega(v, v)$. Prove that any symplectic operator has the determinant 1.

Exercise 7.16 (!). Consider a two-dimensional vector space V over $\mathbb{R}$ and let A be the matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Consider the matrix

$$A' = \begin{pmatrix} d & b \\ -c & a \end{pmatrix}.$$

Prove that $AA' = \Delta\,\mathsf{Id}$, where $\Delta \in k$ is the number $ad - bc$. Prove that A is invertible iff $\Delta \neq 0$.

Exercise 7.17 (!). In the previous problem setting prove that Δ equals to A determinant .

Exercise 7.18. Consider a two-dimensional vector space V over $\mathbb{R}$ endowed with a positive bilinear symmetric form. Let A be an orthogonal operator and its matrix in an orthonormal basis has a form

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

It follows from the Problem 7.14 that $\det A = \pm 1$.

a. Suppose $\det A = 1$. Prove that $b = -c$, $a = d$ and $a^2 + b^2 = 1$.

b. Suppose $\det A = -1$. Prove that $b = c$, $a = -d$ and $a^2 + b^2 = 1$.

Exercise 7.19 (*). Use the statement of the previous problem to describe (in terms of 2x2 matrices) the group of movements of a plane which preserve the origin. Prove that this is a dihedral group (cf. ALGEBRA 1).

Definition 7.8. Consider a matrix (A^i_j). It is said that the matrix (B^i_j) is obtained from (A^i_j) using the **row-wise Gauss transformation**, if $(B^i_j) = (A^i_j) \circ E$, where E is the matrix either of the following form:

$$\begin{pmatrix} 1 & \cdots & \cdots & \cdots & \cdots \\ \cdot & 1 & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & 0 & \cdots & 1 & \cdots \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \cdots & 1 & \cdots & 0 & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & 1 & \cdot \\ \cdots & \cdots & \cdots & \cdots & 1 \end{pmatrix}, \tag{7.1}$$

or of the following form:

$$\begin{pmatrix} 1 & \cdots & \cdots & \cdots & \cdots \\ \cdot & 1 & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & 1 & \cdots & \lambda & \cdots \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \cdots & 0 & \cdots & 1 & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & 1 & \cdot \\ \cdots & \cdots & \cdots & \cdots & 1 \end{pmatrix} \tag{7.2}$$

(dots denote zeroes). If $(B^i_j) = E \circ (A^i_j)$, where E is as above, then one says that (B^i_j) is obtained from (A^i_j) using the **column-wise Gauss transformation**.

Exercise 7.20. Prove that the row-wise Gauss transformation can be described in terms of the following matrix operations: (B^i_j) is obtained from (A^i_j) by permuting of rows or by adding the j-th row multiplied by λ to the i-th. What operations can be used to describe the column-wise Gauss transformation?

Exercise 7.21. Prove that a matrix of the form (7.1) has determinant -1 and that a matrix of the form (7.2) has determinant 1.

Exercise 7.22 (!). Prove that a Gauss transformation of the form (7.2) does not change the determinant but a transformation of the form (7.1) multiplies it by -1.

Definition 7.9. A matrix (A^i_j) is called **upper triangular**, if $A^i_j = 0$ when $i < j$:

$$\begin{pmatrix} * & * & * & \dots & * & * & * \\ 0 & * & * & \dots & * & * & * \\ 0 & 0 & * & \dots & * & * & * \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & * & * & * \\ 0 & 0 & 0 & \dots & 0 & * & * \\ 0 & 0 & 0 & \dots & 0 & 0 & * \end{pmatrix}.$$

A matrix is called **diagonal**, if $A^i_j = 0$ when $i \neq j$.

Exercise 7.23 (!). Consider an upper triangular matrix (A^i_j) of the size $n \times n$. Prove that $\det(A^i_j)$ equals to the product of all the diagonal coefficients:

$$\det(A^i_j) = \prod_i A^i_i.$$

Exercise 7.24.
a. Prove that any matrix can be brought into upper triangular form using row-wise Gauss transformations;

b. Prove that any matrix can be brought into diagonal form using row-wise and column-wise Gauss transformations.

Remark. Since Gauss transformations preserve the determinant (up to ± 1), one can compute the determinant of a square matrix by bringing it to diagonal form and multiplying the coefficients on the diagonal.

Exercise 7.25 (*). Consider a Euclidean ring A (cf. ALGEBRA 2) such that any element $a \in A$ admits decomposition into prime factors. Solve the Problem 7.24 for matrices with elements from A.

Hint. First consider matrices (a^i_j) of the size 1×2, then prove the statement by induction for matrices of the size $1 \times n$ (which is the same as $n \times 1$). Prove that after the matrix is brought into upper triangular form, the only non-zero element will be $\mathrm{GCD}(a^1_1, \dots, a^1_n)$. Consider now an arbitrary matrix of the size $m \times n$ and permute the columns and the rows in such a way that a^1_1 be non-zero. To prove (b) apply the Gauss transformation to rows, columns then once more to rows, once more to columns etc. and obtain a matrix where $a^1_1 \neq 0$ and such that all other elements of the first column and the first row are zeroes.

Grassmann algebra and minors of matrices

Exercise 7.26 (!). Consider a basis $v_1, \ldots, v_n$ of a vector space V, then $v_{i_1} \wedge v_{i_2} \wedge \cdots \wedge v_{i_k}$, $i_1 < i_2 < \cdots < i_k$ is the corresponding basis in $\Lambda^k(V)$. Consider a matrix $A \in \operatorname{End} V$, and $A(i_1, i_2, \ldots, i_k; i'_1, i'_2, \ldots i'_k)$, the coefficients of the matrix of the endomorphism induced by A on $\Lambda^k(V)$ in the basis described above. Prove that $A(i_1, i_2, \ldots, i_k; i'_1, i'_2, \ldots, i'_k)$ is the determinant of the matrix which is obtained from A after all rows except i_1-th, i_2-th, $\ldots$, i_k-th and all columns except i'_1-th, i'_2-th, $\ldots$, i'_k-th has been removed from it.

Remark. This determinant is called the **minor** of the matrix A.

Hint. Take the composition of A with an operator that maps v_{i_l} to $v_{i'_l}$, and reduce the problem to the case $i_l = i'_l$. Prove that the coefficients $A(i_1, i_2, \ldots, i_k; i'_1, i'_2, \ldots, i'_k)$ do not depend on rows except the i_1-th, i_2-th, $\ldots$, i_k-th rows, and on columns except the i'_1-th, i'_2-th, $\ldots$, i'_k-th columns. Then put $A^i_j = 0$ if i and j do not belong to $\{i_1, i_2, \ldots, i_k\}$. Thus you have reduced the problem to the case when $V = V_1 \oplus V_2$ and A is of the form $B \oplus 0_{V_2}$ where $B \in \operatorname{End}(V_1)$ and 0_{V_2} acts on V_2 by mapping all vectors to 0. In this situation one can apply the formula $\Lambda^*(V) = \Lambda^*(V_1) \otimes \Lambda^*(V_2)$ to get the desired result.

Definition 7.10. Consider a linear operator $A \in \operatorname{End}(V)$. Consider the endomorphism induced by A on $\Lambda^*(V)$. Consider the biggest number N such that this endomorphism is non-zero on $\Lambda^N(V)$. This number N is called the **rank of the linear operator** A (denoted $\mathsf{rk}\, A$). If A is represented by a matrix (A^i_j) then $\mathsf{rk}\, A$ is called the rank of this matrix.

Exercise 7.27 (!). Consider an operator A that induces the zero action on $\Lambda^k(V)$. Prove that A induces the zero action on $\Lambda^l(V)$ for any $l > k$.

Exercise 7.28. Prove that the rank of a matrix is the size of its biggest non-zero minor.

Exercise 7.29. Prove that the rank of an operator A is the biggest number N such that there are vectors $v_1, \ldots, v_N$ such that $A(v_1), \ldots, A(v_N)$ are linearly independent.

Exercise 7.30 (!). Prove that the rank of an operator A is the dimension of its image.

Exercise 7.31. Consider a matrix of rank 1. Prove that all its rows are proportional. Prove that all its columns are proportional.

Exercise 7.32. Prove that $\mathsf{rk}\, A = \mathsf{rk}\, A^*$.

Hint. Use the Problem 7.9.

Definition 7.11. A bilinear form $\mu : V_1 \otimes V_2 \longrightarrow k$ is called **nondegenerate pairing** if for every non-zero $v_1 \in V_1$ there is a vector $v'_1 \in V_2$ such that $\mu(v_1, v'_1) \neq 0$ and for any non-zero $v_2 \in V_2$ there is a vector $v'_2 \in V_1$ such that $\mu(v_2, v'_2) \neq 0$.

Exercise 7.33. Consider finite-dimensional vector spaces V_1, V_2. Prove that a nondegenerate pairing $\mu : V_1 \otimes V_2 \longrightarrow k$ defines an isomorphism between V_1 and V_2^* and any isomorphism between those spaces is defined in this way.

Exercise 7.34 (!). Consider an n-dimensional vector space V. Construct the natural isomorphism

$$\Lambda^k(V)^* \cong \Lambda^{n-k}(V) \otimes \det V^*$$

($\det V$ denotes the one-dimensional vector space $\Lambda^n(V)$).

Hint. Use the previous problem.

Exercise 7.35. Consider an n-dimensional vector space V with the basis $v_1, v_2, \dots, v_n$ and an operator $A \in \operatorname{End} V$. Consider the basis $w_1, w_2, \dots, w_n$ in $\Lambda^{n-1}(V)$ where $w_k = v_1 \wedge v_2 \wedge \dots v_{k-1} \wedge v_{k+1} \wedge \dots$ (there are all v_i in the product except one). Consider the matrix (A^i_j) of A and consider $\check{A}^i_j$, the minor that is obtained from A after i-th row and j-th column have been removed. Prove that A acts on $\Lambda^{n-1}(V)$ as the matrix $(\check{A}^i_j)$.

Exercise 7.36. In the previous problem setting consider a nondegenerate bilinear pairing

$$V \otimes \Lambda^{n-1}(V) \longrightarrow \det V,$$

defined by the form $v \otimes w \longrightarrow v \wedge w$. Choose the isomorphism $k \cong \det V$ such that $v_1 \wedge v_2 \wedge \dots \wedge v_n$ is mapped to 1. This gives a nondegenerate pairing defined on V and $\Lambda^{n-1}(V)$. Prove that the basis in $\Lambda^{n-1}(V)$ dual to $v_1, v_2, \dots, v_n$ is $w_1, -w_2, w_3, -w_4, \dots$. Prove that A acts on $\Lambda^{n-1}(V)$ by the matrix $((-1)^{i+j}\check{A}^i_j)$ in this basis.

Exercise 7.37. Consider a nondegenerate bilinear pairing $\mu : V \otimes V' \longrightarrow k$ and endomorphisms $A \in \operatorname{End} V$ and $B \in \operatorname{End} V'$ such that $\mu(Av, Bv') = \mu(v, v')$ for all $v, v' \in V, V'$. Choose dual bases in V, V' and suppose (α^i_j) and (β^i_j) are the matrices of A and B. Prove that $(\alpha^i_j) \circ (\beta^i_j)^\perp = \mathsf{Id}$.

Exercise 7.38 (!). Consider an $A \in \operatorname{End} V$ where V is an n-dimensional vector space with a basis $v_1, v_2, \dots, v_n$ and (A^i_j) is the matrix of the operator A. Prove that A is invertible iff $\det A \neq 0$. Prove that

$$A^{-1} = \frac{1}{\det A}((-1)^{i+j}\check{A}^i_j)^\perp.$$

Hint. Prove that for the natural pairing form

$$V \otimes \Lambda^{n-1}(V) \xrightarrow{\mu} \det V,$$

it holds that $\mu(A(v), A(w)) = \det A \mu(v, w)$, where $A(w)$ denote the natural action of A on $\Lambda^{n-1}(V)$. Then use the previous problem for $(A^i_j) = (\alpha^i_j)$, $\frac{1}{\det A}((-1)^i \check{A}^i_j) = (\beta^i_j)^\perp$.

Remark. We have obtained the well-known formula for calculation of the inverse matrix by expansion by minors. The geometric meaning of this formula can be explained as follows: minors of a matrix are (by definition) the matrix coefficients of the action of this matrix on $\Lambda^{n-1}(V)$ and the natural pairing between V and $\Lambda^{n-1}(V)$ is multiplied by $\det A$ by the action of A. This allows for the calculation of A^{-1} using $\det A$ and $\check{A}$.

Calculation of determinant

Exercise 7.39 (!). Consider the matrix (A^i_j) of a linear operator A. Prove that $\det A$ is equal to

$$\sum_{\sigma \in S_n} \mathsf{sgn}(\sigma) A^1_{\sigma_1} A^2_{\sigma_2} \dots A^n_{\sigma_n}$$

where $(\sigma_1, \sigma_2, \dots, \sigma_n) \in S_n$ is a permutation, the sum is over the elements of the group of all permutations and sgn is the sign of the permutation σ.

Hint. Use the explicit formula (one that uses the sum over the elements of S_n) from ALGEBRA 6 for the tensor $v_1 \wedge v_2 \wedge \cdots \wedge v_n$

Remark. The determinant is usually defined using this formula.

Exercise 7.40. Consider the matrix (A^i_j) of a linear operator A. Prove that $\det A$ can be calculated as follows:

$$A^1_1 \check{A}^1_1 - A^1_2 \check{A}^1_2 + A^1_3 \check{A}^1_3 \dots$$

where $\check{A}^i_j$ are minors that are obtained after removing the i-the row and j-th column.

Remark. This procedure is called **determinant expansion along a row**.

Exercise 7.41 (*). (Vandermonde determinant) Consider the matrix

$$\begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ t_1 & t_2 & t_3 & \dots & t_n \\ t_1^2 & t_2^2 & t_3^2 & \dots & t_n^2 \\ \dots & \dots & \dots & \dots & \dots \\ t_1^{n-1} & t_2^{n-1} & t_3^{n-1} & \dots & t_n^{n-1} \end{pmatrix},$$

where $n > 1$. Prove that its determinant is $\prod_{i<j}(t_i - t_j)$.

Exercise 7.42 (*). Consider the matrix

$$\begin{pmatrix} t & x_1 & x_2 & x_3 & \dots & x_n \\ t^2 & x_1^2 & x_2^2 & x_3^2 & \dots & x_n^2 \\ t^4 & x_1^4 & x_2^4 & x_3^4 & \dots & x_n^4 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ t^{2^n} & x_1^{2^n} & x_2^{2^n} & x_3^{2^n} & \dots & x_n^{2^n} \end{pmatrix},$$

and denote its determinant as $P_n(t, x_1, ...x_n)$. Suppose that this matrix is over the field $\mathbb{Z}/2\mathbb{Z}$. Prove that $P_n(t, x_1, \dots, x_n)$ becomes zero if one takes $t = \sum \alpha_i x_i$ to be an arbitrary linear combination of x_i. Deduce from Bézout's theorem that

$$P_n(t, x_1, \dots, x_n) = Q(x_1, \dots, x_n) \prod (t - \sum \alpha_i x_i),$$

where $\alpha_i \in \mathbb{Z}/2\mathbb{Z}$, and $Q \in \mathbb{Z}/2\mathbb{Z}[x_1, \dots, x_n]$ is a polynomial.

Hint. Use long division of P_n by $t - \sum \alpha_i x_i$. If you get a non-zero value, then if you substitute t for $t = \sum \alpha_i x_i$ in $P(t)$ then you will also get a non-zero value.

Exercise 7.43 (*). Prove in the previous problem setting that $Q = P_{n-1}(x_n)$.

Exercise 7.44 (*). Deduce from the previous problem that $Q(x_1, \dots, x_n) \neq 0$.

Exercise 7.45 (*). (Dickson's theorem) Consider the polynomial

$$F_n(t) = \prod (t - \sum \alpha_i x_i) \in \mathbb{Z}/2\mathbb{Z}[x_1, \dots, x_n].$$

Prove that

$$F_n(t) = t^{2^n} + \sum_{i=0}^{n-1} c_{n,i} t^{2^i},$$

where $c_{n,i} \in \mathbb{Z}/2\mathbb{Z}[x_1, \dots, x_n]$ are polynomials in $x_1, \dots, x_n$.

Hint. Use the previous problem and problem 7.42.

Remark. Polynomials $c_{n,i} \in \mathbb{Z}/2\mathbb{Z}[x_1, \ldots, x_n]$ are called **Dickson's invariants**.

Exercise 7.46 (*). Consider the coefficients Q_r (which are $c_{n,i}$ according to Dickson's theorem) of the polynomial $F_n(t)$ as elements of the symmetric algebra $S^*(V)$ where V is the vector space over the field $\mathbb{Z}/2\mathbb{Z}$ with basis $x_1, \ldots, x_n$. Consider the action of the group $GL(V)$ of invertible linear operators on V and extend it naturally (by multiplicativity) over the symmetric algebra. Prove that Q_r is invariant with respect to $GL(V)$:

$$Q_r(x_1, x_2, \ldots, x_n) = Q_r(h(x_1), h(x_2), \ldots, h(x_n))$$

where $h \in GL(V)$ is an arbitrary invertible endomorphism.

Remark. Consider the subring of $GL(V)$-invariant polynomials in the polynomials ring $S^*(V)$. Dickson (1911) proved that this ring is the ring of polynomials with generators $c_{n,i}$. Consult

> A PRIMER ON THE DICKSON INVARIANTS, Contemporary Mathematics 19 (1983), 421-434. `http://www.math.purdue.edu/∼ wilker/papers/dickson.pdf`

for details.

ALGEBRA 8: Linear algebra: characteristic polynomial

Characteristic polynomial

Definition 8.1. Consider a linear operator $A \in \operatorname{End} V$ over a vector space V. Consider a vector $v \in V$ such that $A(v) = \lambda v$. This vector is called an **eigenvector** and λ is called an **eigenvalue** of the operator A.

Exercise 8.1. Consider a 2-dimensional vector space V over $\mathbb{R}$, endowed with non-degenerate bilinear symmetric form g, nd let $A \in \operatorname{End} V$ be an orthogonal automorphism that is not equal to $\pm Id$. Prove that if g is positive definite or negative definite (such forms are called **definite forms**) then A does not have eigenvectors. Prove that if g is not definite then A has two linearly independent eigenvectors. What eigenvalues can A have in that case?

Exercise 8.2. Consider a set of fractions on the form $\frac{P(t)}{Q(t)}$ where P, Q are polynomials over k and $Q \neq 0$. Consider an equivalence relation generated by the relation defined as follows: $\frac{P(t)}{Q(t)} \sim \frac{P'(t)}{Q'(t)}$, if

$$P(t) = Z(t)P'(t), \qquad Q(t) = Z(t)Q'(t)$$

Define addition and multiplication on equivalence classes in the usual manner:

$$\frac{P(t)}{Q(t)} + \frac{P'(t)}{Q'(t)} = \frac{P(t)Q'(t) + P'(t)Q(t)}{Q(t)Q'(t)}, \qquad \frac{P(t)}{Q(t)}\frac{P'(t)}{Q'(t)} = \frac{P(t)P'(t))}{Q(t)Q'(t)}$$

Prove that this structure is a field.

Definition 8.2. This field is called the **field of rational functions of one variable** or just the **field of rational fractions**. It is denoted $k(t)$.

Exercise 8.3. Prove that this field is not an algebraic extension of k.

Exercise 8.4. Consider a n-dimensional vector space V over k and some other field $K \supset k$. Consider the tensor product $K \otimes_k V$ endowed with the natural action of the multiplicative group K^*. Prove that this is a vector space. Prove that this vector space is finite-dimensional over K if V is finite-dimensional over k. Find the dimension of $K \otimes_k V$ over K assuming the dimension of V over k is known.

Consider a vector space V over k and a linear operator $A \in \operatorname{End} V$ on it. Consider the tensor product of V by the vector space $k(t)$ over k, $V \otimes_k k(t)$. The A action can be naturally extended to a linear operator on $V \otimes k(t)$. We will abuse the notation and denote the corresponding operator $A \in \operatorname{End}_{k(t)}(V \otimes_k k(t))$ as A.

Exercise 8.5 (!). Consider a linear operator $A \in \operatorname{End} V$ on a n-dimensional vector space V over k, and let $\det(t \cdot Id - A) \in k(t)$ be the determinant of the operator $t \cdot Id - A$ that acts on $V \otimes_k k(t)$. Prove that this is a polynomial over k of degree n with the leading coefficient 1.

Definition 8.3. This polynomial is called the **characteristic polynomial of the operator** A and is denoted $\mathsf{Chpoly}_A(t)$.

Exercise 8.6 (!). Let λ be a root of the characteristic polynomial of A. Prove that it is an eigenvalue of A. Prove that all A eigenvalues are the roots of $\mathsf{Chpoly}_A(t)$.

Hint. An operator $\lambda Id - A$ has a non-trivial kernel iff λ is a root of $\mathsf{Chpoly}_A(t)$.

Exercise 8.7. Consider eigenvectors $v_1, \dots, v_n$ that correspond to distinct eigenvalues. Prove that $v_1, \dots, v_n$ are linearly independent.

Exercise 8.8. Consider a linear operator $A \in \operatorname{End} V$ on a n-dimensional vector space. Suppose that the characteristic polynomial has n distinct roots. Prove that A is **diagonalisable**, that is its matrix is diagonal in some basis.

Exercise 8.9 (*). Consider a finite-dimensional vector space V over $\mathbb{C}$. Consider the set of all linear operators on V as a vector space with the natural topology on it. Prove that the set of diagonalisable operators is dense in $\operatorname{End} V$. Prove that the set of non-diagonalisable operators is nowhere dense.

Exercise 8.10 (!). Prove that $\mathsf{Chpoly}_A(t) = \mathsf{Chpoly}_{BAB^{-1}}(t)$ for any invertible linear operator B.

Definition 8.4. Consider a linear operator $A \in \operatorname{End} V$ on an n-dimensional vector space and his characteristic polynomial $\mathsf{Chpoly}_A(t) = t^n + a_{n-1}t^{n-1} + a_{n-2}t^{n-2} + \dots$. The coefficient a_{n-1} is called the **trace** of A and is denoted $\mathsf{tr}\, A$.

Exercise 8.11 (!). Consider an operator A defined by a matrix A^i_j. Prove that $\mathsf{tr}\, A = \sum A^i_i$ (the sum of all numbers standing on the diagonal of the matrix).

Exercise 8.12 (*). Prove that $\mathsf{tr}\, AB = \mathsf{tr}\, BA$ for any linear operators A, B.

Remark. If B is invertible, this follows from 8.10.

Exercise 8.13. Consider a finite-dimensional vector space V. Consider the homomorphism $V \otimes V^* \longrightarrow \operatorname{Hom}(V, V)$ that maps $v \otimes \lambda \in V \otimes V^*$ to $v' \longrightarrow \lambda(v') \otimes v \in \operatorname{Hom}(V, V)$. Prove that it is an isomorphism.

Exercise 8.14 (*). Consider $A \in \operatorname{End} V$ a linear operator on a finite-dimensional vector space and $A \otimes A^*$, an operator induced by A on $V \otimes V^*$. Consider the tensor $\mathsf{Id} \in V \otimes V^*$ that corresponds to the identity operator under the isomorphism $\operatorname{Hom}(V, V) \cong V \otimes V^*$ and the natural pairing $V \otimes V^* \xrightarrow{\mu} k$. Prove that $\mathsf{tr}\, A = \mu(A \otimes A^*(\mathsf{Id}))$.

Upper triangular matrices

Exercise 8.15. Let $V' \subset V$ b k-dimensional subspace of a vector space and $A \in \operatorname{End} V$ be an operator that preserves V' (that is, A maps V' to itself). Choose a basis $e_1, \dots, e_n$ in V such that $e_1, \dots, e_k \in V'$. Prove that A has the following form in this basis:

$$\begin{pmatrix} * & * & * & \dots & * & * & * \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ * & * & * & \dots & * & * & * \\ 0 & 0 & 0 & \dots & * & * & * \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & * & * & * \end{pmatrix}.$$

(lower left rectangle $k \times (n-k)$ is filled with zeroes and other coefficients are arbitrary).

Definition 8.5. Consider an n-dimensional vector space V. A sequence of subspaces $0 = V_0 \subset V_1 \subset V_2 \subset \cdots \subset V_n = V$ is called a **flag** (or a **full flag**), if $\dim V_i = i$. The basis $e_1, \ldots, e_n$ is called **adapted to the flab**, if $e_i \in V_i$. We say that a linear operator $A \in \operatorname{End} V$ **preserves the flag** $\{V_i\}$, if $A(V_i) \subset V_i$.

Exercise 8.16 (!). Let $A \in \operatorname{End} V$ be a linear operator. Prove that A preserves some flag $\{V_i\}$ iff A can be represented by an upper-triangular matrix in in a basis $e_1, \ldots, e_n$ adapted to $\{V_i\}$.

Exercise 8.17 (!). Let V be a vector space over an algebraically closed field. Prove that $A \in \operatorname{End} V$ preserves a flag $0 = V_0 \subset V_1 \subset V_2 \subset \cdots \subset V_n = V$ (and consequently can be represented by an upper-triangular matrix in some basis).

Hint. Take as V_1 a vector subspace spanned by an eigenvector and apply induction.

Exercise 8.18 (*). Consider an invertible linear operator $A \in \operatorname{End} V$ on an n-dimensional space that has n pairwise disjoint eigenvalues. Consider a subalgebra R_A in $\operatorname{End} V$ generated by A. Prove that $\dim R_A = n$.

Hint. Use the Vandermonde determinant.

Exercise 8.19 (*). Consider two commuting linear operators. Prove that the can be represented by two upper-triangular matrices in the same basis $e_1, \ldots, e_n$.

Exercise 8.20 (*). Consider l pairwise commuting linear operators. Prove that they all can be represented by upper-triangular matrices in the same basis $e_1, \ldots, e_n$.

Symmetric and skew-symmetric matrices

Definition 8.6. A matrix is called **symmetric** if it is equal to its transpose: $A = A^{\perp}$. A matrix is called **skew-symmetric**, or **antisymmetric**, if $A = -A^{\perp}$.

Definition 8.7. Consider a vector space V together with a non-degenerate bilinear symmetric form g and a linear operator $A \in \operatorname{End} V$. The operator A is called **symmetric** if for any $x, y \in V$ we have $g(Ax, y) = g(x, Ay)$; it is called **skew-symmetric**, if we have $g(Ax, y) = -g(x, Ay)$.

Definition 8.8. Let V be a vector space endowed with a non-degenerate bilinear symmetric form g. Recall that a basis $e_1, \ldots, e_n \in V$ is called **orthonormal** if e_i-s are pairwise orthogonal and $g(e_i, e_i) = 1$.

Exercise 8.21. Let V be a vector space endowed with a non-degenerate bilinear symmetric form g and $e_1, \ldots, e_n$ be an orthonormal basis. Consider a linear operator $A \in \operatorname{End} V$. Prove that A is symmetric iff its matrix is symmetric, and antisymmetric iff its matrix is antisymmetric.

Exercise 8.22. Let V be a finite-dimensional vector space endowed with a bilinear non-degenerate form g. Prove that any bilinear form can be a represented as $g(Ax, y)$ for some linear operator A and that such an operator is unique.

Remark. In the previous problem setting assume that g is symmetric. Obviously, The form $g(Ax, y)$ is symmetric iff A is symmetric, and antisymmetric iff A is antisymmetric.

Exercise 8.23. Let V be a finite-dimensional vector space. The space of bilinear forms is naturally isomorphic to $V^* \otimes V^*$ and the space $\operatorname{End} V$ is naturally isomorphic to $V \otimes V^*$. A form g induces an isomorphism between V and V^*. This gives an isomorphism between $V^* \otimes V^*$ and $V \otimes V^*$, i.e. between the bilinear forms and the linear operators. Prove that this isomorphism coincides with the one constructed in the Problem 8.22.

Exercise 8.24 (!). Let V be a finite-dimensional vector space endowed with non-degenerate bilinear symmetric form g and let A by a symmetric operator. Suppose A preserve the subspace $V' \subset V$. Prove that A preserves the orthogonal complement to V'.

Definition 8.9. Let V be a vector space over $\mathbb{R}$ and $V \otimes \mathbb{C}$ it the tensor product of the latter with $\mathbb{C}$. Since $\mathbb{C} \cong \mathbb{R} \oplus \sqrt{-1}\,\mathbb{R}$, there is an isomorphism $V \otimes \mathbb{C} \cong V \oplus \sqrt{-1}\,V$. That means that one can consider a **real** ($\operatorname{Re} v$) and **imaginary** part ($\operatorname{Im} v$) of any vector $v \in V \otimes \mathbb{C}$.

Exercise 8.25. Let V be a vector space over $\mathbb{R}$ endowed with a bilinear symmetric form g. Consider a complex vector space $V \otimes \mathbb{C}$ and continue g to $V \otimes \mathbb{C}$ using the linearity of the bilinear complex-valued form. For any vector $v \in V \otimes \mathbb{C}$ denote by $\overline{v}$ the vector $\operatorname{Re}(v) - \sqrt{-1}\operatorname{Im}(v)$ (this vector is called the **complex conjugate to** v). Prove that $g(v, \overline{v}) = g(\operatorname{Re}(v), \operatorname{Re}(v)) + g(\operatorname{Im}(v), \operatorname{Im}(v))$.

Exercise 8.26 (!). Let V by a finite-dimensional vector space over $\mathbb{R}$ of dimension n endowed with a positive definite bilinear symmetric form g (such space is called **Euclidean**), and let A be a symmetric operator and $P(t)$ be his characteristic polynomial. Prove that $P(t)$ has exactly n real roots.

Hint. Consider the action of A on $V \otimes \mathbb{C}$, and let v be the eigenvector corresponding to a non-real eigenvalue. Prove that $g(v, \overline{v}) = 0$. Use the Problem 8.25.

Exercise 8.27 (!). Let V be a Euclidean space and $A \in V$ be a symmetric operator. Prove that V has an orthogonal basis of eigenvectors of A. In other words, A is diagonalisable in an orthonormal basis.

Hint. Use the Problems 8.26 and 8.24.

Exercise 8.28 (*). Let V be a finite-dimensional vector space over $\mathbb{R}$ endowed with a non-degenerate but non necessary positive definite bilinear symmetric form. Is any symmetric operator diagonalisable?

Exercise 8.29 (*). Let V be a Euclidean space and $A \in V$ be a skew-symmetric operator. Denote by ω the skew-symmetric form $g(A\cdot, \cdot)$. Let v be an eigenvector of the operator A^2 (with a non-zero eigenvalue). Prove that ω is non-degenerate on the linear span $\langle v, A(v) \rangle$.

Exercise 8.30 (*). In the previous problem setting prove that in some orthonormal basis $e_1, \dots, e_{2m}, e_{2m+1}$ ω is of the form

$$\sum_{i=0}^{m-1} \alpha_i e^{i+1} \wedge e^{i+2}.$$

Exercise 8.31 (*). Let A be a skew-symmetric operator defined on a Euclidean space and $\det A$ be its determinant. Consider $\det A$ as a polynomial of matrix coefficients of A in some basis. Prove that in a odd-dimensional space V this determinant polynomial is identically zero. Prove that $\det A$ is a full square of some other polynomial of matrix coefficients. This polynomial is called the **Pfaffian of** A.

Hint. Let $2m = \dim V$. Consider the bilinear form ω represented in the form above. Prove that ω^m (considered as an element of the Grassmann algebra $\Lambda^*(V^*)$) is proportional to $e^1 \wedge e^2 \wedge \cdots \wedge e^{2m}$ with a polynomial coefficient Q, moreover $Q^2 = \det A$.

Algebra 9: Artinian rings and idempotents

Definition 9.1. Consider a commutative algebra R with unity over a field k. One says that R is a **finitely generated Artinian ring over the field** k if R is finite-dimensional as a vector space.

Exercise 9.1. Consider a linear operator $A \in \operatorname{End} V$. Consider a subalgebra of $\operatorname{End} V$ generated by k and A. Prove that this in an Artinian ring over k.

Definition 9.2. An element $r \in R$ of an algebra (or ring) R is called **nilpotent** if $r^k = 0$ for some $k \in \mathbb{N}$.

Exercise 9.2. Let r, r' be nilpotent elements in an Artinian ring over a field. Prove that any linear combination r, r' is nilpotent.

Exercise 9.3. Let r, r' be nilpotent elements in the algebra $\operatorname{Mat}(V)$. Is $r + r'$ always nilpotent?

Remark. A nilpotent element in the matrix algebra is called a **nilpotent operator**.

Exercise 9.4. Let $A \in \operatorname{End} V$ be a nilpotent operator. Prove that there is a chain of subspaces $V \supset V_1 \supset V_2 \supset \cdots \supset V_k = 0$ in V such that $A(V_i) = V_{i+1}$.

Exercise 9.5 (!). Consider a nilpotent operator $A \in \operatorname{End} V$. Prove that in some basis A has the form:

$$\begin{pmatrix} 0 & * & * & \dots & * & * & * \\ 0 & 0 & * & \dots & * & * & * \\ 0 & 0 & 0 & \dots & * & * & * \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & * & * \\ 0 & 0 & 0 & \dots & 0 & 0 & * \\ 0 & 0 & 0 & \dots & 0 & 0 & 0 \end{pmatrix}$$

(that is, an upper-triangular matrix with 0 on the diagonal). Prove that any matrix of this form is nilpotent.

Hint. Use the previous problem.

Exercise 9.6 (!). Let $A \in \operatorname{End} V$ be nilpotent operator. Prove that $\mathsf{tr}(A) = \det(A) = 0$ and $\mathsf{Chpoly}_A(t) = t^{\dim V}$.

Definition 9.3. Let R be a ring. A subset $\mathfrak{m} \subset R$ is called an **ideal** if the following it has the following properties:

(i) $\mathfrak{m}$ is closed under addition (that is, the sum of two elements from $\mathfrak{m}$ belongs to $\mathfrak{m}$)

(ii) For any $m \in \mathfrak{m}$, $a \in R$ the product am belongs to R.

Exercise 9.7. Consider a homomorphism of rings $R \longrightarrow R'$. Prove that the kernel of this homomorphism is an ideal.

Exercise 9.8. Consider a surjective homomorphism $f : R_1 \to R_2$ of algebras over a field k and let R_1 be a field. Prove that either $R_2 = 0$, or f is an isomorphism.

Exercise 9.9. Consider an ideal $\mathfrak{m} \subset R$. Consider the quotient $R/\mathfrak{m}$, that is the set of cosets of the form $r + \mathfrak{m}$. Define on $R/\mathfrak{m}$ the natural ring structure.

Definition 9.4. A ring $R/\mathfrak{m}$ is called a **quotient ring** of the ring R. An ideal is called **prime**, if the corresponding quotient ring is non-zero and has no zero divisors. An ideal is called maximal if, moreover, the quotient is a field.

Exercise 9.10. Prove that any prime ideal in an Artinian ring is maximal.

Exercise 9.11 (*). Describe all maximal ideals in the ring of polynomials $k[t]$.

Exercise 9.12. Consider the set of all nilpotent elements in the ring R. Prove that it is an ideal.

Definition 9.5. This ideal is called the **nilradical** of the ring R.

Exercise 9.13 (!). Consider the quotient ring $R/\mathfrak{n}$ of a ring by its nilradical. Prove that $R/\mathfrak{n}$ has no nilpotent elements.

Exercise 9.14. Consider an ideal in an Artinian ring that does not coincide with the whole ring. Prove that it is contained in a maximal one.

Exercise 9.15 (*). Consider an ideal in a ring (not necessary Artinian) that does not coincide with the whole ring. Prove that it is contained in a maximal one.

Hint. Use Zorn's lemma.

Definition 9.6. An Artinian ring R is called **semisimple**, if it does not have non-zero nilpotents.

Definition 9.7. Consider a direct sum $\oplus R_i$ with the natural (coordinate-wise) multiplication and addition. The resulting algebra is called the **direct sum of** R_i and is denoted $\oplus R_i$ too.

Exercise 9.16. Prove that the direct sum of semisimple Artinian rings in semisimple.

Exercise 9.17. Let v be an element of a finite-dimensional algebra R over k. Consider a subspace R generated by $1, v, v^2, v^3, \dots$ (for all powers of v). Supposed this space has dimension n. Prove that $P(v) = 0$ for some polynomial $P = t^{n+1} + a_n t^n + \dots$ with coefficients in k. Prove that this polynomial is unique.

Definition 9.8. This polynomial is called the **minimal polynomial** of the element v and is denoted $\mathsf{Minpoly}(v)$.

Exercise 9.18. Let $v \in R$ be an element of an Artinian ring over k, and $P(t)$ be its minimal polynomial. R_v, v k. , R_v $k[t]/P$ P.

Definition 9.9. Let $v \in R$ be an element of an algebra R such that $v^2 = v$. Then v is called an **idempotent**.

Exercise 9.19. Let $e \in R$ be an idempotent in a ring. Prove that $1 - e$ is an idempotent too. Prove that a product of idempotents is and idempotent.

Exercise 9.20. Let $e \in R$ be an idempotent in a ring. Consider the space $eR \subset R$ (the image of the multiplication by e). Prove that eR is a subalgebra in R, that e is an identity in eR, and that $R = eR \oplus (1 - e)R$.

Exercise 9.21 (!). Let $R = k(t)/P$ where P is a polynomial that decomposes into a product of pairwise co-prime polynomials $P = P_1 P_2 \dots P_n$. Prove that R has m idempotents $e_1, \dots, e_n \subset R$, and that $e_i R \cong k[t]/P_i$.

Hint. Find polynomials $Q(t)$, $Q'(t)$ such that $QP_1 + Q'P_1P_3 \dots P_n = 1$. Let $e = Q'P_1P_3 \dots P_n$. Prove that $e^2 = e(\mod P)$, $eP_1(t) = 0(\mod P)$. Deduce that $k[z]/P_1(z) \cong eR$, and the isomorphism is given by $z \mapsto et$.

Exercise 9.22. Let R be a semisimple Artinian ring without non-identity idempotents. Prove that it is a field.

Hint. Let R be a field. Consider the subalgebra $k(x) \subset R$ generated by a non-invertible element $x \in R$, and apply the previous problem.

Definition 9.10. Two idempotents $e_1, e_2 \in R$ in a commutative algebra R are called **orthogonal** if $e_1e_2 = 0$.

Exercise 9.23. Let $e_1, e_2, e_3 \in R$ be idempotents in an Artinian ring R over a field k and let $e_1 = e_2 + e_3$, let e_2 and e_3 be orthogonal. Prove that $e_2, e_3 \in e_1R$ and $e_1R = e_2R \oplus e_3R$.

Exercise 9.24. Let $\mathsf{char}\, k \neq 2$. Suppose that e_1, e_2, e_3 be idepmotents in an Artinian ring R over a ring k and $e_1 = e_2 + e_3$. Prove that e_2 and e_3 are orthogonal.

Definition 9.11. Let R be an Artinian ring over a field k. An idempotent e in R is called **indecomposable** if there are no such non-zero orthogonal idempotents e_2, e_3 such that $e_1 = e_2 + e_3$.

Exercise 9.25 (!). Let R be a semisimple Artinian ring and e be an indecomposable idempotent. Prove that eR is a ring.

Exercise 9.26 (!). Let R be a semisimple Artinian ring over a field k. Prove that 1 decomposes into a sum of indecomposable orthogonal idempotents: $1 = \sum e_i$. Prove that this decomposition is unique.

Hint. For existence take some idempotent $e \in R$ and decompose $R = eR \oplus (1 - e)R$ then use induction. For uniqueness, consider the product of two possible decompositions of 1.

Exercise 9.27 (!). Let R be a semisimple Artinian ring over a ring k. Prove that R is isomorphic to a direct sum of fields.

Hint. Use the previous problem.

Exercise 9.28 (!). Let $R_1 \xrightarrow{\psi} R_2$ be a surjective homomorphism of Artinian rings, moreover, let R_1 be semisimple and thus decomposed into a direct sum of fields over some set of indices I, $R_1 = \oplus_{i \in I} K_i$. Prove that $R_2 = \oplus_{i \in I'} K_i$, where I' is some subset of I and ψ is the natural projection (that is, ψ acts identically on K_i, $i \in I'$ and is zero on K_i, $i \notin I'$).

Hint. Decompose $1 \in R_1$ into the sum of indecomposable idempotents e_i, $i \in I$, prove that $f : e_iR \to f(e_i)R_2$ is surjective for all $i \in I$, and apply Problem 9.8.

Exercise 9.29 (*). Let $R = k[t]/P$ and the polynomial P has multiple roots over the algebraic closure $\overline{k}$. Can R be semisimple? Analyse the cases $\mathsf{char}\, k = 0$, $\mathsf{char}\, k \neq 0$.

Exercise 9.30 (*). Let R be a semisimple Artinian ring over a field k, and $1 = e_1 + \dots + e_n$ be the decomposition of 1 into the sum of indecomposable orthogonal idempotents. Prove that R has exactly n prime ideals. Describe these ideals in terms of e_i.

Exercise 9.31 (*). Let R be an Artinian ring over a field k (of any characteristic). Prove that the intersection of all simple ideals R is the nilradical of R.

Definition 9.12. Let R be an algebra over a field k, and g be a bilinear form on R. The form g is called **invariant**, if $g(x, yz) = g(xy, z)$ for any x, y, z.

Exercise 9.32. Let R be an Artinian ring endowed with a bilinear invariant form, and $\mathfrak{m}$ be an ideal in R. Prove that $\mathfrak{m}^\perp$ is an ideal too.

Exercise 9.33 (*). Find an Artinian ring that does not admit a non-degenerate invariant bilinear form.

Exercise 9.34 (!). Let R be an Artinian ring over a field k. Consider a the bilinear form $a, b \longrightarrow \mathsf{tr}(ab)$, where $\mathsf{tr}(ab)$ is the trace of the endomorphism $L_{ab} \in \operatorname{End} R$, $x \stackrel{L_{ab}}{\mapsto} abx$. Prove that if this form is non-degenerate then R is semisimple. Prove that if R is semisimple and $\mathsf{char}\, k = 0$ then the form is non-degenerate.

Hint. One direction can be proved using the Problem 9.6. For the other direction consider first the case when R is a field.

Exercise 9.35. Let V, V' be vector spaces over k endowed with bilinear forms g, g'. Define on $V \otimes V'$ the bilinear form $g \otimes g'$ that would satisfy

$$g \otimes g'(v \otimes v', w \otimes w') = g(v, w)g'(v', w')$$

Prove that the bilinear form on $V \otimes V'$ is well-defined and unique.

Exercise 9.36. Let R, R' be commutative algebras over k. Consider a tensor product $R \otimes R'$. Endow $R \otimes R'$ with a multiplicative structure such that $v \otimes v' \cdot w \otimes w = vw \otimes v'w'$. Prove that the ring structure on $R \otimes R'$ is well-defined and unique.

Exercise 9.37. Describe the algebra $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$.

Exercise 9.38. Describe the algebra $\mathbb{Q}[\sqrt{-1}\,] \otimes_{\mathbb{Q}} \mathbb{Q}[\sqrt{-1}\,]$.

and apply the problem

Exercise 9.39 (!). Let $P(t)$ and $Q(t)$ be polynomials over a field k. Denote $K_1 = k[t]/P(t)$ and $K_2 = k[t]/Q(t)$. Prove that $K_1 \otimes K_2 \cong K_1[t]/Q(t) \cong K_2[t]/P(t)$.

Exercise 9.40 (*). Let R, R' be Artinian rings over k, $\mathsf{char}\, k = 0$. Denote the natural bilinear forms $a, b \longrightarrow \mathsf{tr}(ab)$ on these rings by g, g'. Consider the tensor product $R \otimes R'$ with the natural structure of Artinian algebra. Consider the form $g \otimes g'$ on $R \otimes R'$. Prove that $g \otimes g'$ is equal to the form $a, b \longrightarrow \mathsf{tr}(ab)$.

Exercise 9.41 (*). Prove that the tensor product of semisimple Artinian rings over a field k of characteristic 0 is semisimple.

Hint. Use the Problem 9.34.

Exercise 9.42 (*). Find two fields K_1, K_2, algebraic over but not equal to $\mathbb{Q}$, such that $K_1 \otimes_{\mathbb{Q}} K_2$ is also a field.

Exercise 9.43 (*). Let $P(t) \in \mathbb{Q}[t]$ be a polynomial that does not have rational roots but has exactly r real and $2s$ complex roots (that are non-real). Prove that

$$(\mathbb{Q}[t]/P) \otimes_{\mathbb{Q}} \mathbb{R} = \bigoplus_{s} \mathbb{C} \oplus \bigoplus_{r} \mathbb{R}.$$

Exercise 9.44 (*). Let $P(t)$ be an irreducible polynomial over $\mathbb{Q}$ that does not have real roots and $v \in \mathbb{Q}[t]/P$ be an element that does not belong to $Q \subset \mathbb{Q}[t]/P$. Prove that the minimal polynomial of v does not have real roots.

ALGEBRA 10: normal subgroups and representations

10.1 Normal subgroups

Definition 10.1. Let G be a group and let x, y be its elements. Denote by x^y the element of the form yxy^{-1}. A subgroup $G_1 \subset G$ is called **normal**, if for any $x \in G_1$, $y \in G$ it holds that $x^y \in G_1$.

Exercise 10.1. The **centre** of the group G (denoted $Z(G)$) is the set of all elements $x \in G$ that commute with all elements of G. Prove that $Z(G) \subset G$ is a normal subgroup.

Exercise 10.2. Let $G_1 \subset G$ be a subgroup. **Left cosets** of the subgroup G_1 are subsets of G the form $G_1 \cdot x \subset G$, where x takes all values in G_1. **Right cosets** are subsets of G of the form $x \cdot G_1 \subset G$. Prove that right (left) cosets either intersect or coincide. Prove that right cosets are right (and vice versa) if and only if G_1 is a normal subgroup.

Exercise 10.3. Let $G_1 \subset G$ be a normal subgroup and let S_1, S_2 be its cosets. Take $x \in S_1$, $y \in S_2$. Prove that the coset of the product xy does not depend on the choice of x, y in S_1, S_2. Prove that the product thus defined makes the set G_2 of cosets of G_1 into a group.

Definition 10.2. In this case one says that G_2 is the **quotient group of** G **by** G_1 (denoted $G_2 = G/G_1$), and G is an **extension of** G_2 **by** G_1. A group extension is denoted as follows:: $1 \longrightarrow G_1 \longrightarrow G \longrightarrow G_2 \longrightarrow 1$.

Exercise 10.4. Let $G \xrightarrow{\varphi} G'$ be a homomorphism of groups. Prove that the kernel φ (i.e. the set of elements that are mapped to $1_{G'}$) is a normal group in G.

Exercise 10.5. Let $G \xrightarrow{\varphi} G'$ be a surjective homomorphism of groups. Prove that $G' \cong G/\ker\varphi$ where $\ker\varphi$ is the kernel of φ.

Exercise 10.6. Consider the set $\mathrm{Aut}(G)$ of automorphisms of a group G with the composition operation. Prove that it is a group. Prove that the correspondence $\varphi_y(x) \mapsto x^y$ defines a homomorphism $G \longrightarrow \mathrm{Aut}(G)$.

Definition 10.3. Let G, G' be groups and

$$G \longrightarrow \mathrm{Aut}(G')$$

be a homomorphism. In this case one says that G **acts on** G' **by automorphisms**. Automorphisms of the form $x \xrightarrow{\varphi_y} x^y$ are called **inner**.

Exercise 10.7. Find the group $\mathrm{Aut}(G)$ for $G = \mathbb{Z}/p\mathbb{Z}$ (p prime).

Exercise 10.8 (*). Find the group $\mathrm{Aut}(G)$ for $G = \mathbb{Z}/n\mathbb{Z}$ (n arbitrary).

Exercise 10.9. Consider a homomorphism $G_2 \xrightarrow{\varphi} \mathrm{Aut}(G_1)$. Define the following operation on the set of pairs (g_1, g_2): $(g_1, g_2) \cdot (h_1, h_2) = (g_1\varphi(g_2, h_1), g_2h_2)$. Prove that this defines a group.

Definition 10.4. This group is called a **semi-direct product of** G_1 **and** G_2 and is denoted $G_1 \rtimes G_2$.

Exercise 10.10. In the previous problem setting prove that $(G_1, 1)$ defines a normal subgroup in G and that the quotient by this subgroup is isomorphic to G_2.

Exercise 10.11. Describe the group S_3 as a semi-direct product of two non-trivial Abelian groups.

Exercise 10.12 (!). Describe the dihedral group as a semi-direct product of two non-trivial Abelian groups.

Exercise 10.13 (*). The Klein group is the group of quaternions of the form $\pm 1, \pm I, \pm J, \pm K$, with the natural product. Is it possible to get the Klein group as a semi-direct product of two Abelian groups?

Exercise 10.14 (*). Consider a group extension $1 \longrightarrow G_1 \longrightarrow G \stackrel{\varphi}{\longrightarrow} G_2 \longrightarrow 1$. Suppose that $G \stackrel{\psi}{\longrightarrow} G_1$ is a homomorphism such that $\psi \circ \varphi$ is the identity automorphism of G_2 (in this case one says that φ **admits a section** or **splits**). Prove that G is not a semi-direct product $G_1 \rtimes G_2$.

Exercise 10.15 (!). Consider a group G. Consider a subgroup $[G, G] \subset G$ generated by the elements of the form $xyx^{-1}y^{-1}$. Prove that this is a normal subgroup and the quotient by this subgroup is commutative.

Definition 10.5. $[G, G]$ is called the **commutant** of the group G.

Exercise 10.16 (*). Find the commutant of the symmetric group.

Exercise 10.17 (!). . Consider the group of even substitutions A_n, $n \geqslant 5$. Prove that it coincides with its commutant.

Hint. Compute $xyx^{-1}y^{-1}$ where x, y are cyclic permutations of order 3.

Solvable groups

Definition 10.6. A group G is called **solvable** if there exists a sequence $1 = G_n \subset G_{n-1} \subset \cdots \subset G_0 = G$ of normal subgroups such that all G_i/G_{i-1} are Abelian.

Exercise 10.18. Prove that a subgroup of a solvable group is solvable.

Exercise 10.19. Prove that the symmetric group S_3 is solvable.

Exercise 10.20. Prove that the symmetric group S_4 is solvable.

Exercise 10.21. Prove that the Klein group $\{\pm 1, \pm I, \pm J, \pm K\}$ is solvable.

Exercise 10.22 (!). Consider a group G_0 and its commutant G_1, then $G_2 = [G_1, G_1]$ – the commutant of the commutant and so on, $G_i = [G_{i-1}, G_{i-1}]$. Prove that G_0 is solvable if and only if at some stage we get $G_n = 1$.

Exercise 10.23 (!). Prove that the group of even permutations A_n, $n \geqslant 5$ is not solvable.

Exercise 10.24 (*). Prove that the group of motions of $\mathbb{R}^3$ is not solvable.

Hint. Construct an isomorphism between A_5 and the group of motions of an icosahedron and use the Problem 10.17.

Exercise 10.25. Consider a group G of order p^n. Prove that the centre of G contains more that one element.

Hint. Consider the action of G on itself by automorphisms. The order of G equals the sum of cardinalities of classes of the form x^G where x^G is the set of all elements of the form x^y, $y \in G$. First prove that if x is not in the centre then the order of x^G is divisible by p. We thus obtain that $|G| = 1 + \sum |y_i^G|$, and if G has no centre then all $|y_i^G|$ are divisible by p.

Exercise 10.26 (!). Let G be a group of order p^n. Prove that G is solvable.

Exercise 10.27 (*). Let G be a group of order p^2, where p is prime. Prove that G is Abelian.

Exercise 10.28 (*). Give an example of a non-Abelian group of order p^3 where p is any prime number.

Exercise 10.29 (*). Consider the set S of all upper-triangular matrices $n \times n$ with unity on the diagonal over the field k. Prove that these matrices form a subgroup in $GL(n, k)$. Prove that this group is solvable. Find its order for $k = \mathbb{Z}/p\mathbb{Z}$.

10.2 Representations and invariants

Definition 10.7. A **representation of a group** G **on a vector spac** V is a homomorphism $G \longrightarrow GL(V)$ from G into the group $GL(V)$ of invertible endomorphisms of V. If there is a representation of G on V one says that G **acts on** V. A **subrepresentation** V is a subspace that is preserved under the action of G.

Exercise 10.30. Let G act on vector spaces V, V'. Define the action G on $V \otimes V'$ by the formula $g(v \otimes v') = g(v) \otimes g(v')$. Prove that this definition is correct and defines a representation of G on $V \otimes V'$.

Definition 10.8. Let G be a group acting on a vector space V. A vector $v \in V$ is called **invariant under the action of** G or an **invariant of** G if $g(v) = v$ for any $g \in V$. The space of all G-invariant vectors is denoted V^G.

Exercise 10.31. Consider the action of the symmetric group S_n on $V = R^n$ defined by the permutations of coordinates. Find the space of invariants.

Exercise 10.32 (*). In the previous problem setting find the space of invariants of the action of S_n on $V \otimes V$.

Exercise 10.33. Consider the action of the cyclic group $\mathbb{Z}/n\mathbb{Z}$ on $V = R^n$ by the cyclic permutations of coordinates. Find the space of invariants.

Exercise 10.34 (*). In the previous problem setting find the space of invariants $(V \otimes V)^{\mathbb{Z}/n\mathbb{Z}}$ under the action of $\mathbb{Z}/n\mathbb{Z}$ on $V \otimes V$.

ALGEBRA 11: Galois theory

Galois extensions

Exercise 11.1 (!). Consider a polynomial $P(t) \in K[t]$ of degree n with coefficients in a field K that has n distinct roots in K. Prove that the ring $K[t]/P$ of residues modulo P is isomorphic to the direct sum of n copies of K.

Hint. There was a similar problem in ALGEBRA 9.

Definition 11.1. Let K be an algebraic extension of a field k (this fact is often denoted in writing by $[K : k]$). One says that $[K : k]$ is a **Galois extension** if $K \otimes_k K$ is isomorphic (as an algebra) to a direct sum of several copies of K.

Exercise 11.2. Let $P(t) \in k[t]$ be an irreducible polynomial of degree n that has n distinct roots in $K = k[t]/P$. Prove that $[K : k]$ is a Galois extension.

Exercise 11.3. Prove that $[\mathbb{Q}[\sqrt{-1}\,] : \mathbb{Q}]$ is a Galois extension.

Exercise 11.4. Let $[k : \mathbb{Q}]$ be an extension of degree 2 (i.e. K is two dimensianal as a vector space over $\mathbb{Q}$). Prove that it is a Galois extension.

Exercise 11.5 (!). Let p be a prime. Prove that for any root of unity ζ of degree p $[\mathbb{Q}[\zeta] : \mathbb{Q}]$ is a Galois extension.

Exercise 11.6 (*). Is $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}]$ a Galois extension?

Exercise 11.7 (*). Consider F, a field of characteristic p and $k = F(z)$, the field of rational functions over F. Prove that the polynomial $P(t) = t^p - z$ is irreducible over k. Prove that $[k[t]/P : k]$ is not a Galois extension.

Exercise 11.8. Let $K_1 \supset K_2 \supset K_3$ be a sequence of field extensions. Prove that

$$K_2 \otimes_{K_3} K_1 \cong (K_2 \otimes_{K_3} K_2) \otimes_{K_2} K_1.$$

Exercise 11.9. Let $K_1 \supset K_2 \supset K_3$ be a sequence of field extensions. Prove that

$$K_1 \otimes_{K_2} (K_2 \otimes_{K_3} K_2) \otimes_{K_2} K_1 \cong K_1 \otimes_{K_3} K_1.$$

Exercise 11.11. Prove that $\mathbb{Q}[\sqrt[3]{2}, \frac{\sqrt{-3}-1}{2}]$ is a Galois extension.

Exercise 11.12. Let $K_1 \supset K_2 \supset K_3$ be a sequence of field extensions. Prove that the natural map

$$K_1 \otimes_{K_3} K_1 \longrightarrow K_1 \otimes_{K_2} K_1$$

is a surjective homomorphism of algebras.

Exercise 11.13 (!). Let $K_1 \supset K_2 \supset K_3$ be a sequence of field extensions such that $[K_1 : K_3]$ is a Galois extension. Prove that $[K_1 : K_2]$ is also a Galois extension.

Hint. Use the Problem 9.28 from ALGEBRA 9.

Exercise 11.14. Let $P \in k[t]$ be a polynomial of degree n over the field k. Let $K_1 = k$; consider the sequence of field extensions $K_l \supset K_{l-1} \supset \cdots \supset K_1$ which is constructed as follows. Suppose K_j is constructed. Decompose P into irreducible factors $P = \prod P_i$ in K_j. If all P_i are linear then the construction is over. Otherwise, let P_0 be an irreducible factor of P of degree > 1. Consider $K_{j+1} = K_j[t]/P_0$. Prove that this process terminates in a finite number of steps and gives some field $K \supset k$.

Definition 11.2. This field is called a **splitting field** of the polynomial P.

Exercise 11.15 (!). Let K be a splitting field of a polynomial $P(t) \in k[t]$. Prove that K is isomorphic to a subfield of the algebraic closure $\overline{k}$ that is generated by all roots of P.

Exercise 11.16. Let $P(t)$ be a polynomial of degree n. Prove that the degree of its splitting field is not greater than $n!$.

Exercise 11.17. Let $P \in k[t]$ be a polynomial of degree n that has n pairwise disjoint roots in the algebraic closure k and let $[K : k]$ be its splitting field and $K_l \supset K_{l-1} \supset \cdots \supset K_1$ the corresponding sequence of field extensions. Prove that $K \otimes_{K_{i-1}} K_i$ is isomorphic to a direct sum of several copies of K.

Hint. This follows immediately from Problem 11.1.

Exercise 11.18 (!). Let $P(t) \in k[t]$ be an irreducible polynomial of degree n that has n pairwise disjoint roots in the algebraic closure k (this polynomial is said to have **no multiple roots**) and let K be its splitting field. Prove that $[K : k]$ is a Galois extension.

Hint. Use the previous problem.

Exercise 11.19 (*). Let $P(t) \in k[t]$ be an irreducible polynomial over a field k of characteristic 0. Prove that P has no multiple roots.

Hint. Prove that $P(t) = t^n + a_{n-1}t^{n-1} + \dots$ doesn't have multiple roots if and only if P has no common factors with the polynomial

$$P'(t) = nt^{n-1} + (n-1)a_{n-1}t^{n-2} + \cdots + 2a_2t + a_1.$$

In order to show this, prove that $(PQ)' = PQ' + Q'P$ and compute $P'(t)$ for $P = (t-b_1)\dots(t-b_n)$.

Remark. It follows from the previous problem that over a field of characteristic 0 the splitting field of any polynomial is a Galois extension.

Exercise 11.20 (*). Give an example of a field k (of non-zero characteristic) and an irreducible polynomial $P \in k[t]$ such that its splitting field is not a Galois extension.

Galois groups

Definition 11.3. Let $[K : k]$ be a Galois extension. The **Galois group** $[K : k]$ is the group of k-linear automorphisms of the field K. We denote the Galois group by $\mathrm{Gal}([K : k])$ or $\mathrm{Aut}_k(K)$.

In what follows we consider $K \otimes_k K$ as a K-algebra with the action of K^* given by a formula $a(v_1 \otimes v_2) = av_1 \otimes v_2$. This action of K^* is called the **left** action. It is different than the "right action" which is defined by the formula $a(v_1 \otimes v_2) = v_1 \otimes av_2$.

Exercise 11.21. Let $[K : k]$ be a Galois extension. Construct a bijection between the set of K-linear homomorphisms $K \otimes_k K \longrightarrow K$ and the set of indecomposable idempotents in $K \otimes_k K$.

Exercise 11.22. Let $\mu : K \otimes_k K \longrightarrow K$ be non-zero K-linear homomorphism and $k \otimes_k K \subset K \otimes_k K$ be a k-subalgebra naturally isomorphic to K. Prove that $\mu \mid_{k \otimes_k K}$ defines a k-linear automorphism $K \longrightarrow K$.

Exercise 11.23. Prove that every k-linear automorphism K can be obtained this way.

Hint. Let $\nu \in \mathrm{Gal}([K : k])$. Define a homomorphism $K \otimes_k K \to K$ as follows: $v_1 \otimes v_2 \longrightarrow v_1 \nu(v_2)$.

Exercise 11.24 (!). Let $[K : k]$ be a Galois extension. Construct the natural bijection between $\mathrm{Gal}([K : k])$ and the set of indecomposable idempotents in $K \otimes_k K$. Prove that the order of the Galois group is the k-vector space dimension of K.

Exercise 11.25. Let $[K : k]$ be a Galois extension, $\nu \in \mathrm{Gal}([K : k])$ be an element of the Galois group and e_ν be the corresponding idempotent in $K \otimes_k K$. Let μ_l denote the standard (left) action K^* on $K \otimes_k K$, and let μ_r denote the standard right action. Prove that $\mu_l(a)e_\nu = \mu_r(\nu(a))e_\nu$.

Exercise 11.26. Let $[K : k]$ be a Galois extension and $a \in K$ be an element invariant under the action of $\mathrm{Gal}([K : k])$. Prove that $a \otimes 1 = 1 \otimes a$ in $K \otimes_k K$.

Hint. Use the Problem 11.25.

Exercise 11.27 (!). Let $[K : k]$ be a Galois extension and let $a \in K$ be an element invariant under the action of $\mathrm{Gal}([K : k])$. Prove that $a \in k$.

Exercise 11.28. Let $[K : k]$ be a Galois extension and let K' be an intermediate extension, $K \supset K' \supset k$. Prove that $K' = K^{G'}$ where $G' \subset \mathrm{Gal}([K : k])$ is the group of K'-linear automorphisms of K and $K^{G'}$ denotes the set of elements of K invariant under G'.

Hint. Prove that $[K : K']$ is a Galois extension and use the previous problem.

Exercise 11.29 (!). Prove the **Fundamental Theorem of Galois theory**. Let $[K : k]$ be a Galois extension. Then $G' \longrightarrow K^{G'}$ defines a bijective correspondence between the set of subgroups $G' \subset \mathrm{Gal}([K : k])$ and the set of intermediate fields $K \supset K' \supset k$.

Exercise 11.30. Let $[K : k]$ be a Galois extension and let K' be an intermediate field, $K \supset K' \supset k$. Construct the natural correspondence between the set of k-linear homomorphisms $K' \to K$ and the collection $\mathrm{Gal}([K : k])/\mathrm{Gal}([K : K'])$ of cosets of $\mathrm{Gal}([K : K']) \subset \mathrm{Gal}([K : k])$ in the Galois group $\mathrm{Gal}([K : k])$.

Exercise 11.31. Find the Galois group $[\mathbb{Q}[\sqrt{a}] : \mathbb{Q}]$.

Exercise 11.32 (!). Let $[K : k]$ be a Galois extension and let a be an element of the field K generates K over k (this element is called **primitive**). Prove that if $\nu_1, \nu_2, \dots, \nu_n$ are pairwise distinct elements of $\mathrm{Gal}([K : k])$ then $\nu_1(a), \nu_2(a), \dots \nu_n(a)$ are linearly independent over k.

Exercise 11.33 (!). Let $[K : k]$ be a Galois extension and let $V \subset K$ be the union of all intermediate fields $k \subset K' \subset K$ which are proper subfields of K. Suppose that is infinite. Prove that $V \neq K$.

Hint. V is the union of a finitely many k-subsspaces of K that have a dimension (over k) lower than the dimension of K as a linear space over k. Prove that in this case $V \neq K$.

Remark. It follows that any Galois extension $[K : k]$ of any infinite field k has a primitive element.

Exercise 11.34 (!). Let $[K : k]$ be a Galois extension. Prove that for any $a \in K$ the product $P(t) = \prod_{\nu_i \in \mathrm{Gal}([K:k])}(t - \nu_i(a))$ is a polynomial with coefficients in k.

Exercise 11.35 (*). In the previous problem setting, let a be primitive. Prove that $P(t)$ is irreducible.

Exercise 11.36 (!). Recall that the n-th root of unitiy is called **primitive** if it generates the group of n-th roots of unity. Let $\xi \in \mathbb{C}$ be a primitive n-th root. Prove that the group $\mathrm{Gal}([\mathbb{Q}[\xi] : \mathbb{Q}])$ is isomorphic to the group $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ of automorphisms of the group $\mathbb{Z}/n\mathbb{Z}$. Find its order.

Exercise 11.37 (*). Consider an integer n. Let $P(t) = \prod(t - \xi_i)$ where the product is taken over all primitive n-th roots of unity ξ_i. Prove that $P(t)$ has rational coefficients and is irreducible over $\mathbb{Q}$.

Remark. This polynomial is called **cyclotomic polynomial**.

Exercise 11.38 (*). Find a decomposition of $x^n - 1$ into factors irreducible over $\mathbb{Q}$.

Exercise 11.39. Let $a_1, \ldots, a_n \in \mathbb{Z}$ be co-prime and non-square numbers. Prove that $[\mathbb{Q}[\sqrt{a_1}, \sqrt{a_2}, \ldots, \sqrt{a$
$\mathbb{Q}]$ is a Galois extension.

Exercise 11.40. Find the Galois group of this extension.

Exercise 11.41 (!). Prove that $\sqrt{a_1}, \sqrt{a_2}, \ldots, \sqrt{a_n}$ are linearly independent over $\mathbb{Q}$.

Finite fields

We know the following facts about finite fields from the previous problem sheets. The order of a finite fied is p^n where p is its characteristic. For any field k of characteristic p there exists the **Frobenius endomorphism**, $Fr : \ k \longrightarrow k$, $x \mapsto x^p$. The finite field of $\mathbb{F}_p$ naturally embeds into any field of characteristic field p.

We denote the field of order p^n by $\mathbb{F}_{p^n}$.

Exercise 11.42. Let $x \in \mathbb{F}_{p^n}$, $x \neq 0$. Prove that $x^{p^n-1} = 1$.

Hint. Use Lagrange's theorem (the order of an element divides the number of elements in the group).

Remark. It follows that the polynomial $P(t) = t^{p^n-1} - 1$ has exactly $p^n - 1$ roots in $\mathbb{F}_{p^n}$.

Exercise 11.43 (!). Prove that $\prod_{\xi \in \mathbb{F}_{p^n} \setminus 0} = t^{p^n-1} - 1$.

Exercise 11.44 (!). Prove that $[\mathbb{F}_{p^n} : \mathbb{F}_p]$ is a Galois extension.

Exercise 11.45 (!). Prove that $Fr, Fr^2, \ldots, Fr^{n-1}$ are pairwise distinct automorphisms of $\mathbb{F}_{p^n}$.

Exercise 11.46 (!). Prove that $\mathrm{Gal}([\mathbb{F}_{p^n} : \mathbb{F}_p])$ is a cyclic group of order n.

Exercise 11.47 (*). Prove that the splitting field of the polynomial $t^{p^n-1}-1$ over $\mathbb{F}_p$ has order p^n.

Exercise 11.48 (*). Prove that the field of order p^n is unique up to isomorphism.

Exercise 11.49 (!). Find all subfields of $\mathbb{F}_{p^n}$.

Exercise 11.50 (!). Let $[K:k]$ be a Galois extension. Prove that K has a primitive element.

Remark. We have already proved this for infinite fields, see the remark after the Problem 11.33.

Abel's theorem

Abel's theorem states that a generic polynomial of degree 5 is not solvable by radicals; in other words, the solution of a generic equation of degree 5 cannot be expressed using algebraic operations (multiplication, addition, division) and taking an n-th root. In this section we will give an example of an equation that is not solvable by radicals.

Exercise 11.51. Let $[K:k]$ be a Galois extension. Prove that the subgroup $G' \subset \mathrm{Gal}([K:k])$ is normal if and only if $[K^{G'}:k]$ is a Galois extension.

Exercise 11.52 (!). Let $G' \subset \mathrm{Gal}([K:k])$ be a normal subgroup. Prove that the group $\mathrm{Gal}([K^{G'}:k])$ is isomorphic to the quotient $\mathrm{Gal}([K:k])/G'$.

Definition 11.4. A Galois extension $[K:k]$ is called **cyclic**, if its Galois group is cyclic.

Exercise 11.53 (!). Let Galois group of an extension $[K:k]$ be solvable. Prove that $[K:k]$ can be broken into a sequence of Galois extensions $k = K_0 \subset K_1 \subset ... \subset K_n = K$ so that for any i, $\mathrm{Gal}([K_i:K_{i-1}])$ is a cyclic group.

Exercise 11.54 (*). Let k contain all n-th roots of unity and $[K:k]$ be a splitting field of the polynomial t^n-a which does not have roots over k. Prove that this extension is cyclic.

Hint. Let α be some root of the polynomial t^n-a. Then all roots of t^n-a are of the form $\alpha, \alpha\xi, \alpha\xi^2, \ldots, \alpha\xi^{p-1}$, where ξ is a root of unity. Prove that the automorphism that maps α to $\alpha\xi^i$, also maps $\alpha\xi^q$ to $\alpha\xi^{q+i}$.

Exercise 11.55 (*). Take $n \in \mathbb{N}$. Let for any $k > 1$ dividing n, $a \in \mathbb{Q}$ does not equal k-th power of any rational number, and $[K:\mathbb{Q}]$ be the splitting field of the polynomial t^n-a. Prove that K contains all n-th roots of unity and that $\mathrm{Gal}([K:\mathbb{Q}])$ is isomorphic to a semi-direct product $\mathbb{Z}/n\mathbb{Z} \rtimes \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$.

Exercise 11.56 (*). Let k be a field of characteristic 0, and let $[K:k]$ be a splitting field of the polynomial t^n-a. Prove that the Galois group $\mathrm{Gal}([K:k])$ is solvable.

Hint. If k contains the n-th roots of unity then there is nothing to prove. Suppose not, then prove that K contains the n-th roots. Consider an intermediate extension K' generated by these roots over k and prove that $[K:K']$ and $[K':k]$ are Galois extensios with Abelian Galois groups.

Exercise 11.57. Let $[K : k]$ be a cyclic extension of order n, and let ν be a primitive element of the group $\mathrm{Gal}[K : k]$, $\xi \in k$ be the primitive roots of unity of degree n, and $\alpha \in K$ is a primitive element of the extension. Consider the **Lagrange's resolvent**

$$L = a + \xi^{-1}\nu(a) + \xi^{-2}\nu^2(a) + \cdots + \xi^{-n+1}\nu^{n-1}(a)$$

Prove that $\nu(L) = \xi L$. Prove that $L \neq 0$.

Exercise 11.58 (*). Prove that $\prod_{i=0}^{n-1}(t - \nu^i(L)) = t^n - L^n$. Prove that L generates K over k and that $L^n \in k$.

Hint. To see that L generates K over k, use the fact that $\mathrm{Gal}[k[\sqrt[n]{L^n}], k] = \mathbb{Z}/n\mathbb{Z}$, and therefore the dimension of $k[L]$ over k is the same as dimension of K over k.

Exercise 11.59 (*). Let $[K : k]$ be a Galois extension of order n, and let k contain all the n-th roots of unity. Prove that $[K : k]$ is cyclic if and only if it is generated by an n-th root of $a \in k$.

Exercise 11.60 (*). (Galois theorem) Deduce the following theorem. A Galois extension $[K : k]$ is obtained by successive addition of solutions of equations of the form $t^n - a$ if and only if the group $\mathrm{Gal}[K : k]$ is solvable.

Remark. Let $P(t) \in k[t]$ be a polynomial. The **Galois group** of P is defined to be the Galois group its splitting field. Galois theorem states that $P(t) = 0$ is solvable by radicals if and only if the Galois group of $P(t)$ is solvable.

Definition 11.5. Let group G act on a set Σ. The action is called **transitive** if any $x \in \Sigma$ can be mapped to any $y \in \Sigma$ by an action of some $g \in G$.

Exercise 11.61. Let $G \subset S_n$ be a subgroup that contains a transposition and that acts transitively on $\{1, 2, 3, \dots, n\}$. Prove that $G = S_n$.

Exercise 11.62. Let $P \in k[t]$ be an irreducible polynomial, and let $\xi_1, \dots, \xi_n$ be its roots and let all these roots be distinct. Prove that the Galois group of P acts on $\{\xi_1, \dots, \xi_n\}$ transitively.

Hint. Consider a decomposition of $\{\xi_1, \dots, \xi_n\}$ into equivalence classes under the action of $\mathrm{Gal}(P)$. Let S be one of these equivalence classes. Prove that the polynomial $\prod_{\xi_i \in S}(t - \xi_i)$ has coefficients in k and divides P.

Exercise 11.63 (!). Let $P \in \mathbb{Q}[t]$ be an irreducible polynomial of degree n that has exactly $n - 2$ real roots. Prove that its Galois group is S_n.

Hint. Prove that $\mathrm{Gal}(P)$ acts transitively on the roots of P, and that the complex conjugation preserves the splitting field of P and acts on the set of roots as a transposition.

Exercise 11.64 (!). (Eisenstein theorem) Let $Q = t^n + t^{n-1}a_{n-1} + t^{n-2}a_{n-2} + \cdots + a_0$ be a polynomial with integer coefficients such that all a_i divide a given prime numeber p, and $a_0 \not\vdots p^2$. Prove that Q is irreducible over $\mathbb{Q}$.

Exercise 11.65 (*). Prove that $Q(t) = x^5 - 10x + 5$ is an irreducible (over $\mathbb{Q}$) polynomial which has exactly 3 real roots. Deduce that its Galois group is S_5.

Exercise 11.66 (*). Prove that the equation $x^5 - 10x + 5 = 0$ is not solvable by radical.

ALGEBRA 12: semisimple and nilponent operators

Artinian algebras over an algebraically closed field

Let R be an Artinian ring over a field k. Recall that in the exercise sheet 9 we have constructed a canonical decomposition $R \cong \oplus_i e_i R_i$ where e_i are indecomposable orthogonal idempotents and $e_i R$ is Artinian with no non-unit idemotents; moreover, this decomposition is unique.

Exercise 12.1 (!). Assume that R does not have non-unit idempotents and k is algebraically closed. Prove that if R is semisimple then $R = k$.

Exercise 12.2 (!). Assume that R does not have non-unit idempotents, and k is algebraically closed. Prove that $R = k \oplus \mathfrak{n}$ where $\mathfrak{n}$ is a nilradical.

Hint. Prove that $R/\mathfrak{n}$ is semisiple and apply the previous exercise.

Exercise 12.3 (!). Let R be an Artinian ring over an algebraically closed field k. Prove that $R = R_{ss} \oplus \mathfrak{n}$ where R_{ss} is a semisimple Artinian subring in R. Prove that $R_{ss} \subset R$ is uniquely defined.

Exercise 12.4 (*). Is this true if k is not algebraically closed?

We will further need the following statement.

Exercise 12.5 (!). Let R be a semi-simple Artinian ring over a field k, and $R \longrightarrow R'$ be a surjective homomorphism of k-algebras. Prove that R' is a semisimple Artinian ring too.

Hint. There is a similar problem in ALGEBRA 9.

Definition 12.1. Let R be an algebra over a field k. A **representation** of an algebra R is a homomorphim of algebras from R to $\operatorname{End}(V)$, where V is a vector space over k.

Exercise 12.6. Let R be an algebra over a field k. Consider a mapping $R \longrightarrow \operatorname{End}(R)$, defined by the formula $r \mapsto (v \longrightarrow rv)$. Prove that this is a representation.

Exercise 12.7. Let R be an algebra over k, isomorphic to a finite extension k, and let V be a finite dimensional representation of R. Prove that $V \cong R^n$, that is, V is isomorphic (as a representation of R) to a sum of several copies of R.

Exercise 12.8. Let V be a finite dimensional representation of the quaternion algebra $\mathbb{H}$ over $\mathbb{R}$. Prove that V is isomorphic to $\mathbb{H}^n$.

Exercise 12.9. Let G be a group, and k be a field. A **group algebra** G over k (denoted $k[G]$) is the vector space of linear combinations of the form $\sum \lambda_i g_i$ ($\lambda_i \in k$, $g_i \in G$) with multiplication defined by the formula

$$(\sum \lambda_i g_i)(\sum \lambda'_j g'_j) = \sum_{i,j} \lambda_i \lambda'_j g_i g'_j.$$

Prove that this is indeed an algebra. Prove that any representation of a group G can be uniquely extended to a representation of the group algebra.

Exercise 12.10 (!). Let G_1, G_2 be groups and $k[G_1 \times G_2]$ be the group algebra of their product. Prove that $k[G_1 \times G_2] \cong k[G_1] \otimes k[G_2]$.

Exercise 12.11 (!). Let $G = (\mathbb{Z}/2\mathbb{Z})^n$ be a product of n copies of $\mathbb{Z}/2\mathbb{Z}$. Prove that $k[G] \cong k^{\oplus 2^n}$ (direct sum of 2^n copies of k).

Hint. Prove that $k[\mathbb{Z}/2\mathbb{Z}] \cong k \oplus k$, and use the isomorphism $k[G_1 \times G_2] \cong k[G_1] \otimes k[G_2]$.

Exercise 12.12 (*). Consider the Klein group (the subgroup of order 8 in the quaternions that consists of elements $\{\pm 1, \pm I, \pm J, \pm K\}$). Prove that its group algebra over $\mathbb{R}$ is isomorphic to $\mathbb{H} \oplus \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R}$.

Exercise 12.13 (*). Let G be a finite Abelian group, and let k be an algebraically closed field of characteristic 0. Prove that $k[G]$ is a semisimple Artinian ring over k. Deduce from this that $k[G]$ is a direct sum of $|G|$ copies of k.

Hint. Use the criterion mentioned in ALGEBRA 9: an Artinian ring R over a field of characteristic 0 is semisimple if and only if the trace defines a nondegenerate form on R.

Exercise 12.14 (*). Let G be a finite Abelian group, k be an algebraically closed field characteristic 0, and $\rho: G \longrightarrow \operatorname{End}(V)$ be a representation of G over k. Prove that V decomposes into a direct sum of one-dimensional G-invariant subspaces.

Hint. Use the previous exercise and the exercise 12.5.

Exercise 12.15 (*). Let G be a finite Abelian group, and $\mathbb{R}[G]$ its group ring over $\mathbb{R}$. Prove that $\mathbb{R}[G]$ is isomorphic to a direct sum of several copies of $\mathbb{R}$ and $\mathbb{C}$.

Exercise 12.16 (*). Let G be a finite Abelian group, and $\rho: G \longrightarrow \operatorname{End}(V)$ be a representation of G over $\mathbb{R}$. Prove that V can be decomposed into a direct sum of one-dimensional and two-dimensional G-invariant subspaces.

Exercise 12.17 (!). Let G be a finite Abelian group, and let $\rho: G \longrightarrow \operatorname{End}(V)$ be its three-dimensional representation over $\mathbb{R}$. Prove that there is a G-invariant line in V.

Semi-simple operators

Let $A \in \operatorname{End}(V)$ be a linear operator over a finite-dimensional vector space. It is easy to see that the subalgebra $\langle 1, A, A^2, A^3, \dots \langle \subset \operatorname{End}(V)$ generated by A is commutative.

Definition 12.2. The operator $A \in \operatorname{End}(V)$ is called **semi-simple** if the algebra generated by it in $\operatorname{End}(V)$ is semi-simple.

Exercise 12.18. Prove that a linear operator over an algebraically closed field is semi-simple if and only if it is diagonalizable.

Exercise 12.19 (!). Let $k \subset \overline{k}$ be two fields, moreover $\overline{k}$ is algebraically closed, and let V be a finite dimensional vector space over k. Consider $V \otimes_k \overline{k}$ as a vector space over $\overline{k}$. Prove that $\operatorname{End}(V) \otimes_k \overline{k}$ is naturally isomorphic to $\operatorname{End}_{\overline{k}}(V \otimes_k \overline{k})$. This defines a natural inclusion $\operatorname{End}(V) \longrightarrow \operatorname{End}_{\overline{k}}(V \otimes_k \overline{k})$. Prove that the linear operator $A \in \operatorname{End}(V)$ is semi-simple if and only if the corresponding linear operator in $V \otimes_k \overline{k}$ is diagonalizable.

Exercise 12.20. Let V be a two-dimensional vector space over $\mathbb{R}$ endowed with a positive definite bilinear symmetric form, and let $A \in \operatorname{End}(V)$ be an orthogonal operator. Prove that it is semi-simple.

Exercise 12.21 (*). Let V be a vector space over $\mathbb{R}$ of arbitrary finite dimension endowed with a positive definite bilinear symmetric form, and let $A \in \operatorname{End}(V)$ be an orthogonal operator. Prove that it is semi-simple.

Exercise 12.22 (*). Let V be a vector space over $\mathbb{R}$ endowed with a non-degenerate bilinear symmetric form, not necessarily positive definite, and let $A \in \operatorname{End}(V)$ be an orthogonal operator. Is it always semi-simple?

Definition 12.3. An element of an Artinian ring over k is called **semi-simple** if it generates a semi-simple subalgebra in R.

Exercise 12.23. Let R be an Artinian ring over k and let $r \in R$ be a semi-simple element. Prove that in any representation of $R \longrightarrow \operatorname{End}(V)$, r is mapped to a semi-simple endomorphism of V.

Hint. Use the exercise 12.5.

Exercise 12.24 (!). Let V be a finite dimensional vector space over an algebraically closed field, and let $A \in \operatorname{End}(V)$ be a linear operator. Prove that A decomposes into a direct sum of a semi-simple and a nilpotent operator, $A = A_{ss} + A_n$, which commute. Prove that this decomposition is unique and A_{ss}, A_n can be expressed as polynomials of A.

Hint. Use exercise 12.3.

Exercise 12.25 (*). Is this true if the base field k is not algebraically closed?

Exercise 12.26 (!). Let A be a upper-triangular matrix, A_δ be its diagonal part. Prove that A and A_δ commute.

Exercise 12.27 (**). Let (V, g) be a vector space endowed with a bilinear skew-symmetric form, and let A be anti-symmetric operator and $A = A_{ss} + A_n$ be its decomposition into a semi-simple and nilpotent part. Prove that A_{ss}, A_n are anti-symmetric.

Exercise 12.28 (*). Is it possible that an antisymmetric operator over $\mathbb{C}$ be nilpotent?

Hamilton-Cayley theorem

Let k be any field and let $k(t)$ be the field of rational functions over k, and V be an n-dimensional vector space over k, and $B(t) \in \operatorname{End}(V)[t]$ a polynomial with coefficients in $\operatorname{End}(V)$. Recall that in this situation $\det(B(t))$ is a polynomial of t (see ALGEBRA 8). Let us consider $B(t)$ as a $k(t)$-linear endomorphism of $V \otimes k(t)$. Consider the endomorphism $\Lambda^{n-1}(V \otimes k(t))$ induced by $B(t)$ and let $\check{B}(t)$ be the adjoint endoorphim of $V \otimes k(t)$ with respect to the natural pairing

$$\Lambda^{n-1}(V \otimes k(t)) \otimes V \otimes k(t) \longrightarrow \det V \otimes k(t)$$

It is shown in ALGEBRA 7 that $B(t)\check{B}(t) = \check{B}(t)B(t) = \det(B(t))\,\mathsf{Id}_V$.

Exercise 12.29. In this situation show that $\check{B}(t)$ is $\operatorname{End}(V)$-valued polynomial: $\check{B}(t) \in \operatorname{End}(V)[t]$.

Hint. Express $\check{B}(t)$ via the minors of $B(t)$.

Exercise 12.30. Let $A \in \operatorname{End}(V)$. Applying the argument from the Remark to $B = t - A$ prove that $(t - A)(t \check{-} A) = \mathsf{Chpoly}_A(t)$. Prove the the coefficients of the polynomial $(t \check{-} A) \in \operatorname{End}(V)[t]$ commute with A.

Exercise 12.31. Let $R \subset \mathrm{End}(V)$ be a subset. Denote by $Z(R)$ the set of all operators $A' \in \mathrm{End}(V)$ that commute with all operators $r \in R$ (this set is called the **centralizer** of R). Prove that $Z(R)$ is a subalgebra of $\mathrm{End}(V)$.

Exercise 12.32. Let $R \in \mathrm{End}(V)$ be a subalgebra and let $A_1 \in Z(A)$ be an element of the centralizer R, $R[t]$ be the algebra of R-valued polynomials, and $R[t] \xrightarrow{\varphi} R'$ be a homomorphism of algebras. Denote by $R[A_1]$ the subalgebra $\mathrm{End}(V)$, generated by R and A_1. Prove that there exists a homomorphism $\varphi_0 : R[A_1] \longrightarrow R'$ such that $\varphi_0\big|_R = \varphi\big|_R$ and $\varphi_0(A_1) = \varphi(t)$. Prove that these conditions determine φ_0 uniquely.

Exercise 12.33. Let $A \in \mathrm{End}(V)$ be a linear operator, apply the previous exercise and construct a homomorphism $Z(A)[t] \xrightarrow{\Psi} Z(A)$ that maps t to A, and which is identity on $Z(A)$.

Exercise 12.34 (!). (Cayley-Hamilton theorem) Consider the equality $(t-A)(t \check{-} A) = \mathsf{Chpoly}_A(t)$ in $Z(A)[t]$. Apply the homomorphism Ψ constructed above to both left and right parts of the equality. Prove that this results in the following equality in the algebra $\mathrm{End}(V)$:

$$\mathsf{Chpoly}_A(A) = 0.$$

Exercise 12.35 (*). Let $A, B \in \mathrm{End}\, V$ be linear operators. Consider a function of two variables $Q(t_1, t_2) = \det(t_1 A + t_2 B)$, where $t_1 A + t_2 B$ is considered as a linear operator on $V \otimes_k k(t_1, t_2)$, and $k(t_1, t_2) = k(t_1)(t_2)$ is the field of rational functions over $k(t_1)$. Prove that $Q(t_1, t_2)$ is a polynomial with coefficients in k. Prove that in the ring $\mathrm{End}\, V$ the equality $Q(-B, A) = 0$ holds.

Exercise 12.36 (!). Let $A \in \mathrm{End}(V)$ be a linear operator that acts on a finite dimensional vector space over an algebraically closed field k. Let $\{\lambda_1, \dots, \lambda_n\}$ be the roots of the characteristic polynomial of the operator A. Consider the space V_{λ_i} of all $v \in V$ such that $(A - \lambda_i)^{m_i}(v) = 0$ where m_i is the multiplicity of the root λ_i of the polynomial $\mathsf{Chpoly}_A(t)$. Prove that $V = \oplus V_{\lambda_i}$, where summation is over all roots λ_i of the characteristic polynomial A.

Hint. Use the Cayley-Hamilton theorem.

Remark. The space V_{λ_i} is called an **generalized eigenspace** of operator A.

Minimal polynomial and characteristic polynomial

Definition 12.4. Let $A \in \mathrm{End}(V)$ be a linear operator that acts on a vector space of finite dimension over k. a sequence of endomorphisms $1, A, A^2, \dots \in \mathrm{End}(V)$. Since the space $\langle 1, A, A^2, \dots \rangle$ is finite dimensional, then starting from some - i all A^i can be expressed as a sum of the form: $A^N = \sum_{i=0}^{l-1} \lambda_i A^i$, $\lambda_i \in k$, $l = \dim\langle 1, A, A^2, \dots \rangle$. Let us write down such an equation for A^l: $A^l + \sum_{i=0}^{l-1} \lambda_i A^i = 0$. Recall that the polynomial $P(t) = t^l + \lambda_{l-1} t^{l-1} + \dots + \lambda_0$ is called the **minimal polynomial** of A and is denoted $\mathsf{Minpoly}_A(t)$.

Exercise 12.37 (!). Prove that the following identity holds in the algebra $\mathrm{End}(V)$:

$$\mathsf{Minpoly}_A(A) = 0.$$

Prove that any polynomial $Q(t) = t^m + \mu_{m-1} t^{l-1} + \dots + \mu_0$, such that $Q(A) = 0$, is divided by $\mathsf{Minpoly}_A(t)$.

Exercise 12.38. Prove that the characteristic polynomial of the operator is divided by its minimal polynomial.

Exercise 12.39. Let $A \in \mathrm{End}(V)$ be a linear operator.

a. Prove that A is nilpotent if and only if $\mathsf{Minpoly}_A(t) = t^n$.

b. Prove that A is a non-identity idempotent if and only if $\mathsf{Minpoly}_A(t) = t^2 - t$.

Exercise 12.40. Let $A \in \mathrm{End}(V)$ be a linear operator that acts on a finite dimensional vector space over an algebraically closed field k and let $V = \oplus V_{\lambda_i}$ be a decomposition of V into a direct sum of generalized eigenspaces. Let $P(t)$ be a minimal polynomial of A and let $P_i(t)$ be minimal polynomials of restrictions of A to V_{λ_i}. Prove that $P(t) = P_1(t)P_2(t)\dots$. Prove that $P_i(t) = (t-\lambda_i)^k$ where $k \leqslant \dim V_{\lambda_i}$.

Hint. It is clear that $P_i(t) = (t - \lambda_i)^k$, since the operator $A - \lambda_i$ on V_{λ_i} is nilpotent. That $P(t) = P_1(t)P_2(t)\dots$ follows easily from the fact that all $P_j(A)$ $(j \neq i)$ are invertible on V_{λ_i}.

Remark. The characteristic polynomial also has this muliplicativity property, as can be easily observed.

Exercise 12.41. Let $A \in \mathrm{End}(V)$ be a linear operator in a n-dimensional vector space. Prove that $\mathsf{Minpoly}_A(t) = (t - \lambda)^n$ if and only if in some basis A has the form

$$\begin{pmatrix} \lambda & 1 & 0 & \dots & \dots & 0 \\ 0 & \lambda & 1 & 0 & \dots & 0 \\ 0 & 0 & \lambda & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & \dots & \lambda & 1 & 0 \\ 0 & 0 & \dots & \dots & \dots & \lambda & 1 \\ 0 & 0 & \dots & \dots & \dots & \dots & \lambda \end{pmatrix} \tag{12.1}$$

Hint. Replacing A by $A - \lambda\,\mathsf{Id}_V$ one may assume that $\mathsf{Minpoly}_A(t) = t^n$. Take a vector $v \in V$ such that $(A - \lambda)^{n-1}(v) \neq 0$. Prove that $v, A(v), A^2(v), \dots, A^{n-1}(v)$ constitute a basis in V, and in this basis A hase the form (12.1).

Remark. Such a matrix is called a **Jordan block**. We will denote it by $J(n, \lambda)$.

Definition 12.5. Let $e_1, \dots, e_n$ be a basis in a vector space and let A_i^j be a matrix of a linear operator A in this basis. Assume that $e_1, \dots, e_n$ are divided into groups (blocks) $[e_1, \dots, e_{k_1}][e_{k_1+1}, \dots, e_{k_2}] \dots$, in such a way that A maps every e_i into a linear combination of vectors that belong to the same block. In this case A consists of square pieces of size $k_i - k_{i-1}$, and is zero outside of these square pieces:

$$\begin{pmatrix} * & \dots & * & 0 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ * & \dots & * & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & \dots & 0 & * & \dots & * & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & * & \dots & * & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 & \dots & 0 & * & \dots & * \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & 0 & \dots & 0 & * & \dots & * \end{pmatrix}$$

A matrix of this form is called **block diagonal**.

Exercise 12.42. Let $A \in \mathrm{End}(V)$ be a linear operator that acts on a finite dimensional vector space over an algebraically closed field k. Assume that the minimal polynomial $\mathsf{Minpoly}_A(t)$ equals characteristic polynomial $\mathsf{Chpoly}_A(t)$. Prove that in some basis A can be represented as a block diagonal matrix that consists of Jordan blocks $J(n_i, \lambda_i)$ where all λ_i are distinct.

Hint. Use the multiplicativity of Minpoly and Chpoly with respect to decomposition of V into a direct sum of generalized eigenspaces, and reduce the problem to the case $V = V_{\lambda_i}$. Now apply exercise 12.41.

Definition 12.6. Assume that operator A can be represented in some basis as a block diagonal matrix that consists of Jordan blocks. The operator A is said then to be in a **Jordan normal form**.

We will now show the unicity of the Jordan normal form, and then we will show its existence. We work assuming the base field to be algebraically closed.

Exercise 12.43. Let $A \in \mathrm{End}(V)$ be a nilpotent operator with the Jordan normal form that consists of Jordan blocks $J(0, n_1), \dots, J(0, n_k)$. Prove that the number of blocks in the Jordan normal form of A equals the dimension of the space V/AV. Prove that $A^jV/A^{j+1}V$ is the number of blocks $J(0, n_i)$ with $n_j \geqslant j$. Deduce that Jordan normal form of a nilpotent operator is determined uniquely, up to permutation of the blocks.

Exercise 12.44 (!). Prove that Jordan normal form of any operator is unique, up to permutation of the blocks.

Hint. Decompose V into a direct sum of generalized eigenspaces, and reduce the problem to the case $V = V_{\lambda_i}$. Replacing A by $A - \lambda_i$, one can content oneself with nilpotent operators. Now the statement follows from the previous exercise.

Definition 12.7. Let $A \in \mathrm{End}(V)$ be a linear operator. We say that A **acts cyclically** on V if there exists an element v such that $v, Av, A^2v, A^3v, \dots$ generates V.

Exercise 12.45. Let $A \in \mathrm{End}(V)$ be a linear operator that acts cyclically on V. Prove that $\mathsf{Minpoly}_A(t) = \mathsf{Chpoly}_A(t)$.

Hint. If A act cyclically then the degree of $\mathsf{Minpoly}_A(t)$ equals $\dim V$ equals the degree of $\mathsf{Chpoly}_A(t)$.

Exercise 12.46. Let $A \in \mathrm{End}(V)$ be a linear operator such that V decomposes as a sum of A-invariant subspaces on which A acts cyclically. Prove that A can be represented in some basis in a Jordan normal form.

Hint. Use the exercise 12.42.

Modules over a ring and Jordan normal form

Definition 12.8. Let R be a ring. A **module** over R is an Abelian group endowed with an operation $R \times M \longrightarrow M$ that is compatible with the addition in the following sense

(i) For any $\lambda \in R$, $u, v \in M$ we have $\lambda(u + v) = \lambda u + \lambda v$. For any $\lambda_1, \lambda_2 \in R$, $u \in M$ we have $(\lambda_1 + \lambda_2)u = \lambda_1 u + \lambda_2 u$ (distributivity of multiplication over addition).

(ii) For any $\lambda_1, \lambda_2 \in R$, $u \in M$ we have $\lambda_1(\lambda_2 u) = (\lambda_1\lambda_2)u$ (associativity of multiplication).

(iii) For any $v \in M$ we have $1v = v$ where 1 denotes the identity in R.

Remark. This definition repeats almost verbatim the definition of a vector space over a field. Many notions that were defined for vector spaces (for example, homomorphism, monomorphism, epimorphism, kernel, image, quotient space) can be redefined without modification for modules over a ring.

Exercise 12.47. Let R be an algebra over a field k. For any module M over R consider M as a vector space over $k \subset R$. Consider each the operation of multiplication by an elements of R as an endomorphism of M. Prove that this defines a homomorphism $R \longrightarrow \mathrm{End}_k(M)$. Prove that all representations can be obtained in this way.

Exercise 12.48. Prove that any Abelian group has a unique structure of a module over $\mathbb{Z}$.

Definition 12.9. Consider the group R^n as a module over R, with the action given by $r\cdot(x_1, \dots, x_n) = (rx_1, \dots, rx_n)$. This module is called **free**. The quotient of R^n by a submodule is called **finitely generated**. If M can be represented as a quotient of a free module by a finitely generated submodule then M is called **finitely presented**.

Definition 12.10. Let $\varphi : M \to M'$ be a homomorphism of modules over an algebra R. The **cokernel** φ (denoted by $\mathrm{Coker}\,\varphi$) is the quotient of M' by the image of φ.

Exercise 12.49. Let M be a module over R. Prove that M is finitely generated if and only if it has a collection of elements $m_1, \dots, m_N$ such that any element of M can be represented as a linear combination , $m = r_1m_1 + \dots + r_Nm_N$, $r_1, \dots, r_N \in R$.

Exercise 12.50. Let M be a module over R. Prove that M is finitely presented if and only if it is isomorphic to a cokernel of a homomorphism $\varphi : R^N \to R^M$ of free R-modules.

Exercise 12.51 (!). Let k be a field and M be a module over $k[t]$ that has a finite dimension over k. Prove that M is finitely generated and finitely presented over $k[t]$.

Hint. Consider M as a vector space over k, pick a basis $m_1, \dots, m_M \in M$, and consider these elements as generators. Then prove that the kernel of the map $\varphi : M \otimes_k k[t] \to M$ is generated by elements of the form $m_i \otimes t - tm_i \otimes 1$.

Exercise 12.52 (!). Let M be a finite Abelian group. Prove that M is finitely generated and finitely presented as a module over $\mathbb{Z}$.

Hint. Take all elements of M as the set of generators $m_1, \dots, m_N \in M$.

Exercise 12.53. Let R be a ring and V a module over R represented as the cokernel of the homomorphism $(R)^n \xrightarrow{\varphi} (R)^m$. Write down φ as a matrix A^i_j with coefficients in R. Let B^i_j be a matrix obtained from R using elementary (Gaussian) row and column transformations (see ALGEBRA 7). Prove that V is isomorphic to a cokernel of a homomorphism that corresponds to B^i_j.

Definition 12.11. Let R be a ring and $a \in R$ be an element. Consider aR as a module over R. A **cyclic module** over R is a quotient module R/aR.

Exercise 12.54. Let M be a Z-module. Prove that M is cyclic if and only if the corresponding Abelian group is cyclic.

Exercise 12.55. Let M be a $k[t]$-module. Prove that M is cyclic if and only if for some $v \in M$, $v, tv, t^2v, t^3v, \dots$ generated M.

Exercise 12.56 (!). Let R be a ring such that any $n \times m$ matrix with coefficients in R can be brought into a diagonal form using elementary row and column operations. Prove that any finitely generated and finitely presented module over R is isomorphic to a direct sum of cyclic ones.

Hint. If $(R)^n \xrightarrow{\varphi} (R)^n$ is represented by a diagonal matrix with a_i^i on the diagonal then the cokernel of this homomorphism has the form $\oplus_i R/a_i^i R$.

Exercise 12.57 (!). Let R be a Euclidean ring (see ALGEBRA 2). Prove that any matrix of size $n \times m$ with coefficients in R can be brought to a diagonal form using elementary row and column operations. Deduce that any finitely generated and finitely presented module over R is a direct sum of cyclic ones.

Hint. A similar problem is in ALGEBRA 7.

Exercise 12.58 (!). Let G be a finite Abelian group. Prove that G is a finite sum of cyclic groups.

Exercise 12.59 (!). Let V be a module over $k[t]$ which is finite dimensional over k. Prove that V is a direct sum of cyclic modules.

Hint. The ring $k[t]$ is Euclidean and V is finitely generated and finitely presented as fallows from exercise 12.51.

Exercise 12.60 (!). Let $A \in \mathrm{End}(V)$ be a linear operator. Prove that V can be decomposed into a direct sum of A-invariant subspaces so that on each of them A acts cyclically. Deduce that if the field k is algebraically closed then A can be brought into Jordan normal form.

Hint. Consider the action of $k[t]$ on V given by $P(t)(v) = P(A)v$. Prove that V is a $k[t]$-module. Decompose V into a direct sum of cyclic submodules: $V = \oplus V_i$. Prove that all V_i are A-invariant, and A acts on them cyclically.

Exercise 12.61 (*). Find a commutative ring and a module over it that does not decompose into a direct sum of cyclic ones.