Course 1: 21.02.2021

0.0 Coordinates

- **Structure:**

  Chapter 1: Groups.

  Chapter 2: Rings.

- **Selective bibliography:**

1. S. Crivei, *Basic Abstract Algebra*, Ed. Casa Cărţii de Ştiinţă, Cluj-Napoca, 2002, 2003.
2. W.J. Gilbert, W.K. Nicholson, *Modern algebra with applications*, John Wiley, 2004.
3. I.D. Ion, N. Radu, *Algebră* (ed. 4), Ed. Didactică şi Pedagogică, Bucureşti, 1991.
4. I. Purdea, C. Pelea, *Probleme de algebră*, Ed. EIKON, Cluj-Napoca, 2008.
5. I. Purdea, I. Pop, *Algebră*, Ed. GIL, Zalău, 2003.

- **Seminar:**

  Minimum attendance: 75% for seminar classes in order to be allowed to participate in the exam.

  Problems for the next week will be posted after the course in the Files section of the team Algebra 2 - English from MS Teams.

  Students may get up to 0.5 extra points to the final grade: 5 problems solved during different seminars, each for 0.1 points (details about the system will be given during seminar classes).

- **Course:**

  Courses willbe posted in the Files section of the team Algebra 2 - English from MS Teams.

  Students may solve some Bonus projects, each for 0.2 extra points.

- **Exam:**

  There will be an oral exam.

  The final grade F is computed as follows:

$$\mathbf{F = 1 + T(3p) + G(3p) + R(3p) + E},$$

  where T is the grade for the theoretical subject, G is the grade for the problems from Group Theory, R is the grade for the problems from Ring Theory and E consists of the extra points from seminar and course.

Chapter 1 GROUPS

1.1 Operations

Definition 1.1.1 By an *operation* (or *composition law*) on a set A we understand a function

$$\varphi : A \times A \to A,$$

where $A \times A = \{(a_1, a_2) \mid a_1, a_2 \in A\}$.

Usually, we denote operations by symbols like $\cdot$, $+$, $*$, so that $\varphi(x, y)$ is denoted by $x \cdot y$, $x + y$, $x * y$, $\forall (x, y) \in A \times A$.

Example 1.1.2 The usual addition and multiplication are operations on $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and the usual subtraction is an operation on $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, but not on $\mathbb{N}$. The usual division is not an operation on either of the five numerical sets, because of the element zero.

Definition 1.1.3 Let " $\cdot$ " be an operation on an arbitrary set A. Define the following laws:
(1) *Associative law*: $(x \cdot y) \cdot z = x \cdot (y \cdot z)\,, \quad \forall x, y, z \in A$
(2) *Commutative law*: $x \cdot y = y \cdot x\,, \quad \forall x, y \in A$
(3) *Identity law*: $\exists e \in A$: $a \cdot e = e \cdot a = a$, $\forall a \in A$ (e is called an *identity element*)
(4) *Inverses law*: $\forall a \in A$, $\exists a' \in A$: $a \cdot a' = a' \cdot a = e$ (e is the identity element, a' is called an *inverse element for* a)

Lemma 1.1.4 *Let " $\cdot$ " be an operation on a set A.*
(i) If there exists an identity element in A, then it is unique.
(ii) Assume further that the operation " $\cdot$ " is associative and has identity element e and let $a \in A$. If an inverse element for a does exist, then it is unique.

Proof. (i) Assume that $e_1, e_2 \in A$ are identity elements in A. Then by computing their product in two ways, we have $e_1 \cdot e_2 = e_1 = e_2$.
(ii) Suppose that a has $a_1, a_2 \in A$ as inverses. Then by the associative law, we may compute the product $a_1 \cdot a \cdot a_2$ in two ways as

$$a_1 \cdot (a \cdot a_2) = a_1 \cdot e = a_1, \quad \text{and} \quad (a_1 \cdot a) \cdot a_2 = e \cdot a_2 = a_2$$

and we obtain $a_1 = a_2$. □

Let us now discuss some special subsets of sets endowed with an operation.

Definition 1.1.5 Consider an operation $\varphi : A \times A \to A$ on a set A and let $B \subseteq A$. Then B is called a *stable subset of A with respect to φ* if

$$\forall x, y \in B\,, \quad \varphi(x, y) \in B\,.$$

In this case, we may consider the operation $\varphi' : B \times B \to B$ on B defined by

$$\varphi'(x, y) = \varphi(x, y)\,, \quad \forall (x, y) \in B \times B\,,$$

that is called the *operation induced by φ in the stable subset B of A*.
When using a symbol "$\cdot$" for the operation φ, we will simply say that *B is a stable subset of* $(A, \cdot)$.

Example 1.1.6 (a) The set $2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\}$ of even integers is stable in $(\mathbb{Z}, +)$, but the set of odd integers is not stable in $(\mathbb{Z}, +)$.

(b) The interval $[0, 1]$ is stable in $(\mathbb{R}, \cdot)$, but the interval $[-1, 0]$ is not stable in $(\mathbb{R}, \cdot)$.

Remark 1.1.7 Notice that the associative and the commutative laws still hold in a stable subset (endowed with the induced operation), since they are true for every element in the initial set (only the universal quantifier $\forall$ appears in their definition). But the identity element and the inverse element do not transfer (their definition uses the existential quantifier $\exists$ as well).

1.2 Groups

Definition 1.2.1 Let A be a set. Then $(A, \cdot)$ is called a:
(1) *groupoid* if " $\cdot$ " is an operation on A.
(2) *semigroup* if " $\cdot$ " is an operation on A and the associative law holds.
(3) *monoid* if it is a semigroup with identity element.
(4) *group* if it is a monoid in which every element has an inverse.

If the operation is commutative as well, then the structure is called *commutative*. A commutative group is also called an *abelian group* (after the name of N.H. Abel).

Example 1.2.2 (a) $(\mathbb{Z}, -)$ is a grupoid, but not a semigroup.

(b) $(\mathbb{N}^*, +)$ is a semigroup, but not a monoid.

(c) $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$ are monoids, but not groups.

(d) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$ and $(\mathbb{C}^*, \cdot)$ are groups.

Remark 1.2.3 We denote by 1 the identity element of a group $(G, \cdot)$ and by x^{-1} the inverse of an $x \in G$. We denote by 0 the identity element of a group $(G, +)$ and by $-x$ the symmetric of an $x \in G$.

Definition 1.2.4 Let $(G, \cdot)$ be a semigroup, let $x \in G$ and let $n \in \mathbb{N}^*$. Then we may use the associative law and define

$$x^n = \underbrace{x \cdot x \cdot \ldots \cdot x}_{n \text{ times}}.$$

If $(G, \cdot)$ is a monoid, then we may also define $x^0 = 1$. If $(G, \cdot)$ is a group, then we may also define $x^{-n} = (x^{-1})^n$.

Remark 1.2.5 If the operation is denoted by "+", then we replace the notation x^n by nx.

Lemma 1.2.6 *Let $(G, \cdot)$ be a group, let $x \in G$ and let $m, n \in \mathbb{Z}$. Then:*
(i) $x^m \cdot x^n = x^{m+n}$;
(ii) $(x^m)^n = x^{mn}$.

Proof. By induction on n for positive values, and then by using the definition. Homework. □

Lemma 1.2.7 *Let $(G, \cdot)$ be a group and let $a, x, y \in G$. Then:*
(i) $a \cdot x = a \cdot y \Longrightarrow x = y$,
$x \cdot a = y \cdot a \Longrightarrow x = y$ *(cancellation laws);*
(ii) $(x^{-1})^{-1} = x$;
(iii) $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$.

Proof. Homework. □

Remark 1.2.8 A finite group may be defined by its operation table, that specifies the result of any multiplication of two elements of the group. The operation table of a group has the property that every element appears exactly once on each row and each column.

Let us now see some other important examples.

Example 1.2.9 (a) Let X be a non-empty set. By a *word on X* of length n we understand a string of n elements from X for some $n \in \mathbb{N}$. The word of length 0 is called the *void word* and is denoted by e. On the set X^* of words on X consider the operation "$\cdot$" given by concatenation. Then $(X^*, \cdot)$ is a monoid with identity element e, called the *free monoid* on the set X.

(b) Let $\{e\}$ be a single element set and let " $\cdot$ " be the only operation on $\{e\}$, defined by $e \cdot e = e$. Then $(\{e\}, \cdot)$ is an abelian group, called the *trivial group*.

(c) Let $n \in \mathbb{N}$ with $n \geq 2$. Denote by $M_{m,n}(\mathbb{R})$ the set of $m \times n$-matrices with entries in $\mathbb{R}$ and by $M_n(\mathbb{R})$ the set of $n \times n$-matrices with entries in $\mathbb{R}$. Then $(M_{m,n}(\mathbb{R}), +)$ is an abelian group and $(M_n(\mathbb{R}), \cdot)$ is a monoid.

(d) Let $GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det A \neq 0\}$ ($n \in \mathbb{N}$, $n \geq 2$) be the set of invertible $n \times n$-matrices with real entries. Then $(GL_n(\mathbb{R}), \cdot)$ is a group, called the *general linear group of rank n*.

(e) Let M be a set and let $S_M = \{f : M \to M \mid f \text{ is bijective}\}$. Then $(S_M, \circ)$ is a group, called the *symmetric group of M*. The identity element is the identity map 1_M and the inverse of an element f (which is a bijection) is f^{-1}.

If $|M| = n$, then S_M is denoted by S_n and the group $(S_n, \circ)$ is in fact the *permutation group* of n elements.

(f) Let $U_n = \{z \in \mathbb{C} \mid z^n = 1\}$ $(n \in \mathbb{N}^*)$. Then $(U_n, \cdot)$ is an abelian group, called the *group of n-th roots of unity*.

(g) Let $n \in \mathbb{N}$ and define on $\mathbb{Z}$ the relation ρ_n by

$$x \, \rho_n \, y \Longleftrightarrow n|(x-y).$$

If $n \neq 0$, then $x \, \rho_n \, y \Longleftrightarrow x$ and y give the same remainder when divided by n. Then ρ_n is an equivalence relation on $\mathbb{Z}$ and we denote its corresponding partition by

$$\mathbb{Z}_n = \mathbb{Z}/\rho_n = \{x + n\mathbb{Z} \mid x \in \mathbb{Z}\} = \{\widehat{x} \mid x \in \mathbb{Z}\}.$$

For $n = 0$ and $n = 1$, we have $\mathbb{Z}_0 = \{\{x\} \mid x \in \mathbb{Z}\}$ and $\mathbb{Z}_1 = \{\mathbb{Z}\}$.

For $n \geq 2$, we have $\mathbb{Z}_n = \{\widehat{0}, \ldots, \widehat{n-1}\}$.

We define an addition by

$$\widehat{x} + \widehat{y} = \widehat{x+y}, \quad \forall \widehat{x}, \widehat{y} \in \mathbb{Z}_n .$$

Then $(\mathbb{Z}_n, +)$ is an abelian group, called the *group of residue classes modulo n*.

(h) Let $K = \{e, a, b, c\}$ and define an operation " $\cdot$ " on K by the following table:

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

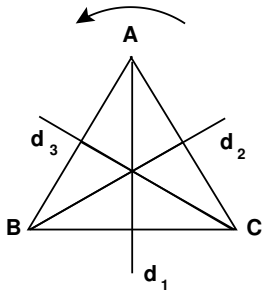
Then $(K, \cdot)$ is an abelian group, called *Klein's group*. It comes from Geometry, and it may be viewed as the group of geometric transformations of a rectangle:

- e is the identical transformation,
- a is the symmetry with respect to the horizontal symmetry axis of the rectangle,
- b is the symmetry with respect to the vertical symmetry axis of the rectangle,
- c is the symmetry with respect to the center of the circumscribed circle of the rectangle.

The product $x \cdot y$ of two transformations x and y of K is defined by performing first y and then x.

(i) Let ABC be an equilateral triangle and consider the following geometric transformations, that transform the vertices A, B and C into themselves:

- e is the identical transformation (or the rotation counterclockwise of 360^0),
- α is the rotation counterclockwise of 120^0,
- β is the rotation counterclockwise through 240^0,
- a is the symmetry with respect to the axis d_1, passing through A and perpendicular to BC,
- b is the symmetry with respect to the axis d_2, passing through B and perpendicular to AC,
- c is the symmetry with respect to the axis d_3, passing through C and perpendicular to AB.



Denote $D_3 = \{e, \alpha, \beta, a, b, c\}$. Define the product $x \cdot y$ of two transformations x and y of D_3 by performing first y and then x. Then$(D_3, \cdot)$ is a group, called the 3^{rd} *dihedral group.*

Generalizing, for every $n \in \mathbb{N}$, $n \geq 3$, we can define the n^{th} *dihedral group* D_n of rotations and symmetries of a regular n-gon, consisting of n rotations and n symmetries.

(j) Consider a set $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ and define an operation " $\cdot$ " on Q by the following rules:

- 1 is the identity element,
- $i^2 = j^2 = k^2 = -1$,
- $i \cdot j = k$, $j \cdot k = i$, $k \cdot i = j$,
- $j \cdot i = -k$, $k \cdot j = -i$, $i \cdot k = -j$,
- The signs rule holds.

Then $(Q, \cdot)$ is a non-commutative group, called the *quaternion group.*

Theorem 1.2.10 *Let $(A, \cdot)$ be a monoid. Denote*

$$U(A, \cdot) = \{x \in A \mid \exists x^{-1} : x \cdot x^{-1} = x^{-1} \cdot x = 1\},$$

that is, the set of invertible elements of A. Then $U(A, \cdot)$ is a stable subset of $(A, \cdot)$ and $U(A, \cdot)$ is a group with respect to the induced operation.

Proof. Let $x, y \in U(A, \cdot)$. Then $\exists x^{-1}, y^{-1} \in A$. Since there exists $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1} \in A$, it follows that $x \cdot y \in U(A, \cdot)$. Hence $U(A, \cdot)$ is a stable subset of $(A, \cdot)$.

Then clearly " $\cdot$ " satisfies the associative law. Since $1 \in U(A, \cdot)$, 1 is the identity element in $(U(A, \cdot), \cdot)$.

Now let $x \in U(A, \cdot)$. Then $\exists x^{-1} \in A$. Since there exists $(x^{-1})^{-1} = x \in A$, it follows that $x^{-1} \in U(A, \cdot)$. Hence every element in $(U(A, \cdot), \cdot)$ has an inverse.

Consequently, $(U(A, \cdot), \cdot)$ is a group. □

Theorem 1.2.11 *Let $(G, \cdot)$ be a non-empty semigroup. Then $(G, \cdot)$ is a group if and only if the equations*

$$a \cdot x = b \quad \text{and} \quad y \cdot a = b$$

have unique solutions in G for every $a, b \in G$.

Proof. Suppose that $(G, \cdot)$ is a group and let $a \in G$. Since $\exists a^{-1} \in G$, it follows that $x_1 = a^{-1} \cdot b$ and $y_1 = b \cdot a^{-1}$ are solutions of the above equations.

Assume now that $x_2 \in G$ is also a solution of the equation $a \cdot x = b$. Then $a \cdot x_1 = a \cdot x_2$, whence $x_1 = x_2$ by the cancellation law. Similarly, one can prove that the second equation has a unique solution.

Conversely, let $a \in G$. The equation $ax = a$ has a solution in G, say e_r. For every $b \in G$, the equation $ya = b$ has a solution in G, say c. Then

$$be_r = cae_r = ca = b.$$

Analogously, we get $e_l \in G$ such that for every $b \in G$, $e_l b = b$. Computing the product $e_l \cdot e_r$ in two ways, it follows that $e_r = e_l$ is the identity element in G. Let us denote it simply by e.

The equations $ya = e$ and $ax = e$ have solutions in G, say a' and a'' respectively. Computing the product $a'aa''$ in two ways, it follows that $a' = a''$ is the inverse of a. Hence every element of G is invertible.

Therefore, $(G, \cdot)$ is a group. □

Remark 1.2.12 The uniqueness of solutions is not needed for the converse part of Theorem 1.2.11.