Course 2: 11.10.2021

1.4 Operations

Definition 1.4.1 By an *operation* (or *composition law*) on a set A we mean a function $\varphi : A \times A \to A$.

Usually, we denote operations by symbols like $\cdot$, $+$, $*$, so that $\varphi(x, y)$ is denoted by $x \cdot y$, $x + y$, $x * y$, $\forall (x, y) \in A \times A$. We denote by $(A, \cdot)$ the fact that "$\cdot$" is an operation on a set A.

Example 1.4.2 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 1.4.3 Let "$\cdot$" be an operation on an arbitrary set A. Define the following laws:
- *Associative law*: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, $\quad \forall x, y, z \in A$
- *Commutative law*: $x \cdot y = y \cdot x$, $\quad \forall x, y \in A$
- *Identity law*: $\exists e \in A$: $a \cdot e = e \cdot a = a$, $\forall a \in A$. In this case, e is called an *identity element*.
- *Inverse law*: $\forall a \in A$, $\exists a' \in A$: $a \cdot a' = a' \cdot a = e$, where e is the identity element. In this case, a' is called an *inverse element for* a.

Lemma 1.4.4 *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.

Definition 1.4.5 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

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

In this case, we may consider the operation $\varphi' : B \times B \to B$ on B defined by $\varphi'(x, y) = \varphi(x, y)$, $\forall (x, y) \in B \times B$, that is called the *operation induced by φ in the stable subset B of A*.
When using a symbol "$\cdot$" for φ, we simply say that B *is a stable subset of* $(A, \cdot)$.

Example 1.4.6 (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 1.4.7 Notice that the associative, the commutative (and later on, the distributive 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).

1.5 Groups and rings

Definition 1.5.1 Let "$\cdot$" be an operation on a set A. Then $(A, \cdot)$ is called a:
(1) *semigroup* if the associative law holds.
(2) *monoid* if it is a semigroup with identity element.
(3) *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).

Remark 1.5.2 We denote by 1 the identity element of a group $(G, \cdot)$ and by x^{-1} the inverse of an element $x \in G$. In case of an additive group $(G, +)$, the identity element is denoted by 0, while the inverse of an element $x \in G$ is called the *symmetric* of x and is denoted by $-x$.

Example 1.5.3 (a) The operation "$-$" defined on $\mathbb{Z}$ is not associative.

(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.

(e) 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.

(f) 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*.

(g) Let $n \in \mathbb{N}$, $n \geq 2$. Then $(\mathbb{Z}_n,+)$ is an abelian group, called the *group of residue classes modulo* n. The addition is defined by

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

(h) 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. Denote by $GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det(A) \neq 0\}$ 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.

(i) 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 the inverse function 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.

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

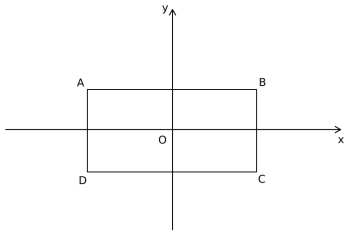
$\cdot$	**e**	**a**	**b**	**c**
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Then $(K,\cdot)$ is a commutative group, called *Klein's group*. Note that the operation table of any group has the property that every element appears exactly once on each row and each column.

It may be viewed as the group of geometrical 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.



Definition 1.5.4 Let R be a set. Then a structure with two operations $(R,+,\cdot)$ is called a:

(1) *ring* if $(R,+)$ is an abelian group, $(R,\cdot)$ is a semigroup and the distributive laws hold:

$$x \cdot (y+z) = x \cdot y + x \cdot z, \quad (y+z) \cdot x = y \cdot x + z \cdot x, \quad \forall x,y,z \in R.$$

(2) *unitary ring* if $(R,+,\cdot)$ is a ring and there exists an identity element with respect to "$\cdot$".

(3) *division ring* (or *skew field*) if $(R,+,\cdot)$ is a ring, $|R| \geq 2$ and any $x \in R^*$ has an inverse $x^{-1} \in R^*$.

(4) *field* if it is a commutative division ring.

The ring $(R,+,\cdot)$ is called *commutative* if the operation "$\cdot$" is commutative.

If $(R,+,\cdot)$ is a ring, then we denote the identity elements with respect to "$+$" and "$\cdot$" respectively by 0 and 1. We will also use the notation $R^* = R \setminus \{0\}$.

Example 1.5.5 (a) $(\mathbb{Z},+,\cdot)$ is a unitary ring, but not a field.

(b) $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ and $(\mathbb{C},+,\cdot)$ are fields.

(c) Let $\{e\}$ be a single element set and let both "$+$" and "$\cdot$" be the only operation on $\{e\}$, defined by $e+e=e$ and $e\cdot e=e$. Then $(\{e\},+,\cdot)$ is a commutative unitary ring, called the *trivial ring*.

(d) Let $n\in\mathbb{N}$, $n\geq 2$. Then $(\mathbb{Z}_n,+,\cdot)$ is a commutative unitary ring, called the *ring of residue classes modulo* n. The addition and the multiplication are defined by

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

(e) Let $(R,+,\cdot)$ be a commutative unitary ring. Then $(R[X],+,\cdot)$ is a commutative unitary ring, called the *polynomial ring over* R *in the indeterminate* X, where the operations are the usual addition and multiplication of polynomials.

(f) Let $n\in\mathbb{N}$, $n\geq 2$ and let $(R,+,\cdot)$ be a ring. Then $(M_n(R),+,\cdot)$ is a ring, called the *ring of matrices* $n\times n$ *with entries in* R, where the operations are the usual addition and multiplication of matrices.

(g) A ring $(R,+,\cdot)$ is called *Boolean* (after the name of G. Boole) if $a^2=a$ for every $a\in R$. If M is a set and $\mathcal{P}(M)$ is the power set of M (that is, the set of all subsets of M), then $(\mathcal{P}(M),\Delta,\cap)$ is a Boolean ring, where Δ is the *symmetric difference* operation defined by $A\Delta B=(A\setminus B)\cup(B\setminus A)$ for every $A,B\in\mathcal{P}(M)$.

1.6 Subgroups and subrings

Definition 1.6.1 Let $(G,\cdot)$ be a group and let $H\subseteq G$. Then H is called a *subgroup of* G if:
(i) $H\neq\emptyset$ $(1\in H)$;
(ii) $x,y\in H\Longrightarrow x\cdot y\in H$;
(iii) $x\in H\Longrightarrow x^{-1}\in H$.

We denote by $H\leq G$ the fact that H is a subgroup of a group G.

Theorem 1.6.2 *Let $(G,\cdot)$ be a group and let $H\subseteq G$. Then $H\leq G$ if and only if*
(i) $H\neq\emptyset$ $(1\in H)$;
(ii) $x,y\in H\Longrightarrow x\cdot y^{-1}\in H$.

Remark 1.6.3 (1) Note that if H is a subgroup of a group $(G,\cdot)$, then $(H,\cdot)$ is also a group.

(2) In case of an additive group $(G,+)$, the conditions (ii) and (iii) in Definition 1.6.1 become: (ii') $x,y\in H\Longrightarrow x+y\in H$; (iii') $x\in H\Longrightarrow -x\in H$, while the condition (ii) in Theorem 1.6.2 becomes: (ii') $x,y\in H\Longrightarrow x-y\in H$.

Example 1.6.4 (a) Every non-trivial group $(G,\cdot)$ has the subgroups $\{1\}$ and G.

(b) $\mathbb{Z}$ is a subgroup of $(\mathbb{Q},+)$, $(\mathbb{R},+)$ and $(\mathbb{C},+)$; $\mathbb{Q}$ is a subgroup of $(\mathbb{R},+)$ and $(\mathbb{C},+)$; $\mathbb{R}$ is a subgroup of $(\mathbb{C},+)$.

(c) The set $n\mathbb{Z}=\{nx\mid x\in\mathbb{Z}\}$ is a subgroup of $(\mathbb{Z},+)$ for every $n\in\mathbb{N}$.

Definition 1.6.5 Let $(R,+,\cdot)$ be a ring and let $A\subseteq R$. Then A is called a *subring of* R if:
(i) $A\neq\emptyset$ $(0\in A)$;
(ii) $x,y\in A\Longrightarrow x-y\in A$;
(iii) $x,y\in A\Longrightarrow x\cdot y\in A$.

Definition 1.6.6 Let $(K,+,\cdot)$ be a field and let $A\subseteq K$. Then A is called a *subfield of* K if:
(i) $|A|\geq 2$ $(0,1\in A)$;
(ii) $x,y\in A\Longrightarrow x-y\in A$;
(iii) $x,y\in A\,,y\neq 0\Longrightarrow x\cdot y^{-1}\in A$.

We denote by $A\leq R$ $(A\leq K)$ the fact that A is a subring (subfield) of a ring R (field K).

Remark 1.6.7 Note that if A is a subring (subfield) of a ring (field) $(R,+,\cdot)$, then $(A,+,\cdot)$ is also a ring (field).

Example 1.6.8 (a) Every non-trivial ring $(R,+,\cdot)$ has two subrings, namely $\{0\}$ and R, called the *trivial subrings*.

(b) $\mathbb{Z}$ is a subring of $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ and $(\mathbb{C},+,\cdot)$; $\mathbb{Q}$ is a subfield of $(\mathbb{R},+,\cdot)$ and $(\mathbb{C},+,\cdot)$; $\mathbb{R}$ is a subfield of $(\mathbb{C},+,\cdot)$.

(c) For every $n\in\mathbb{N}$, $n\mathbb{Z}=\{nx \mid x\in\mathbb{Z}\}$ is a subring of the unitary ring $(\mathbb{Z},+,\cdot)$. If $n\geq 2$, then $n\mathbb{Z}$ does not have identity.

1.7 Group and ring homomorphisms

Let us now define some special maps between groups or rings. We denote by the same symbol operations in different arbitrary structures.

Definition 1.7.1 Let $(G,\cdot)$ and $(G',\cdot)$ be groups and let $f:G\to G'$. Then f is called a *group homomorphism* if

$$f(x\cdot y)=f(x)\cdot f(y),\quad \forall x,y\in G.$$

Also, f is called a *group isomorphism* if it is a bijective group homomorphism.

We denote by $G\simeq G'$ the fact that two groups G and G' are isomorphic.
Usually, we denote by 1 and $1'$ the identity elements in G and G' respectively.

Example 1.7.2 (a) Let $(G,\cdot)$ and $(G',\cdot)$ be groups and let $f:G\to G'$ be defined by $f(x)=1'$, $\forall x\in G$. Then f is a homomorphism, called the *trivial homomorphism*.

(b) Let $(G,\cdot)$ be a group. Then the identity map $1_G:G\to G$ is an isomorphism.

(c) Let $f:\mathbb{Z}\to\mathbb{Z}$ be defined by $f(x)=2x$. Then f is a group homomorphism from the group $(\mathbb{Z},+)$ to itself.

Theorem 1.7.3 *Let $f:G\to G'$ be a group homomorphism. Then:*
(i) $f(1)=1'$;
(ii) $(f(x))^{-1}=f(x^{-1})$, $\forall x\in G$.

Definition 1.7.4 Let $(R,+,\cdot)$, $(R',+,\cdot)$ be rings. Then $f:R\to R'$ is called a *ring homomorphism* if

$$f(x+y)=f(x)+f(y),\quad f(x\cdot y)=f(x)\cdot f(y),\quad \forall x,y\in R.$$

Also, f is called a *ring isomorphism* if it is a bijective ring homomorphism.

We denote by $R\simeq R'$ the fact that two rings R and R' are isomorphic.
Usually, we denote by 0 and $0'$ the zero elements in R and R' respectively.

Remark 1.7.5 If $f:R\to R'$ is a ring homomorphism, then the first condition from its definition tells us that f is a group homomorphism between $(R,+)$ and $(R',+)$. Then f takes the identity element of $(R,+)$ to the identity element of $(R',+)$, that is, $f(0)=0'$ and we also have $f(-x)=-f(x)$, $\forall x\in R$. But in general, even if R and R' have identities, denoted by 1 and $1'$ respectively, in general it does not follow that a ring homomorphism $f:R\to R'$ has the property that $f(1)=1'$.

Example 1.7.6 (a) Let $(R,+,\cdot)$ and $(R',+,\cdot)$ be rings and let $f:R\to R'$ be defined by $f(x)=0'$, $\forall x\in R$. Then f is a homomorphism, called the *trivial homomorphism*.

(b) Let $(R,+,\cdot)$ be a ring. Then the identity map $1_R:R\to R$ is an isomorphism.

(c) The map $f:\mathbb{R}\to M_2(\mathbb{R})$ defined by $f(x)=\begin{pmatrix} x & 0\\ 0 & x\end{pmatrix}$, $\forall x\in\mathbb{R}$, is a ring homomorphim between the rings $(\mathbb{R},+,\cdot)$ and $(M_2(\mathbb{R}),+,\cdot)$.

Extra: Fast adding

Remark 1.7.7 If a and b are two natural numbers, then it makes no difference if we add them as natural numbers or as elements (that is, residue classes) of some group $\mathbb{Z}_n$ for some $n > a + b$.

Theorem 1.7.8 *If $n = p_1^{r_1} \cdots p_k^{r_k}$ for some distinct primes $p_1, \ldots, p_k$, then there is an isomorphism of additive groups:*

$$\mathbb{Z}_n \simeq \mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}}$$

given by

$$\varphi([x]_n) = ([x]_{p_1^{r_1}}, \ldots, [x]_{p_k^{r_k}}),$$

where $[x]_m$ denotes the residue class modulo $m \in \mathbb{N}$.

This allows one (the computer) to replace the addition of large natural numbers by parallel "small" simultaneous additions. This technique is used in the design of computer software in order to speed up calculations.

Example 1.7.9 Let $a = 37$, $b = 56$, and choose $n = 140 = 2^2 \cdot 5 \cdot 7$.

$$\begin{aligned} a = 37 \to [37]_{140} \to ([37]_4, [37]_5, [37]_7) &= ([1]_4, [2]_5, [2]_7) \quad + \\ b = 56 \to [56]_{140} \to ([56]_4, [56]_5, [56]_7) &= ([0]_4, [1]_5, [0]_7) \\ a + b \qquad\qquad\qquad\qquad\qquad\qquad &= ([1]_4, [3]_5, [2]_7) \end{aligned}$$

Now one solves (by an efficient method given by the *Chinese Remainder Theorem*) the system:

$$\begin{cases} x = 1 \pmod 4 \\ x = 3 \pmod 5 \\ x = 2 \pmod 7 \end{cases}$$

and gets $x = 93$ (unique solution modulo n). Hence $a + b = 93$.

Reference: R. Lidl, G. Pilz, Applied Abstract Algebra*, Springer-Verlag, 1998.*