Groups

Abdennour Kitouni, Anatoliy Malyarenko, Sergei Silvestrov

November 17, 2015

Abstract

Contents of the lecture.

- ☞ Definition of a group
- ☞ Subgroups.
- ☞ Cyclic groups.
- ☞ Generating sets and Cayley digraphs.

The definition of a group

Definition 1. A binary structure $(G,*)$ is called a **group**, if the following axioms are satisfied.

$\mathscr{G}_1$: The binary operation $*$ is associative, i.e., for all a, b, $c \in G$, we have

$$(a*b)*c = a*(b*c).$$

$\mathscr{G}_2$: There exist an **identity element** $e \in G$ such that for all $a \in G$,

$$e*a = a*e = a.$$

$\mathscr{G}_3$: For each $a \in G$, there exist an **inverse** element $a' \in G$ such that

$$a \cdot a' = a' \cdot a = e.$$

Examples of groups

Example 1. $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, and $(\mathbb{C},+)$ are groups with $e = 0$ and $a' = -a$.

Example 2. $(U,\cdot)$ is a group with $e = 1$ and $a' = a^{-1}$. Because $(U,\cdot)$ and $(\mathbb{R}_{2\pi},+_{2\pi})$ are isomorphic binary structures, $(\mathbb{R}_{2\pi},+_{2\pi})$ is also a group with $e = 0$ and $a' = 2\pi - a$.

Example 3. $(U_n, \cdot)$ is a group with $e = 1$ and $a' = a^{-1}$. Because $(U_n, \cdot)$ and $(\mathbb{Z}_n, +_n)$ are isomorphic binary structures, $(\mathbb{Z}_n, +_n)$ is also a group with $e = 0$ and $a' = n - a$.

Example 4. Let $M_{m\times n}(\mathbb{Z})$ be the set of all $m \times n$ matrix with integer elements. $(M_{m\times n}(\mathbb{Z}), +)$ is a group. The obviously defined sets $M_{m\times n}(\mathbb{Z}_n)$, $M_{m\times n}(\mathbb{Q})$, $M_{m\times n}(\mathbb{R})$, and $M_{m\times n}(\mathbb{C})$ are groups under matrix addition.

Examples of binary structures that are not groups

Example 5. $(\mathbb{Z}^+, +)$ is not a group, because there is no identity element. This is the reason for introducing 0.

Example 6. $(\mathbb{Z}^+ \cup \{0\}, +)$ is not a group, because the element 1 has no inverse. This is the reason to introduce negative integers. $(\mathbb{Z}, +)$ *is* a group.

Example 7. $(\mathbb{Z} \setminus \{0\}, \cdot)$ is not a group, because the element 2 has no inverse. This is the reason to introduce rational numbers. Check that $(\mathbb{Q} \setminus \{0\}, \cdot)$ *is* a group.

Abelian groups

Definition 2. A group $(G, *)$ is **abelian** if $*$ is commutative.

Until now, we met only abelian groups.

Example 8. Let $GL(n, \mathbb{R})$ be a subset of $M_{n\times n}(\mathbb{R})$ consisting of invertible matrices. $GL(n, \mathbb{R})$ together with matrix multiplication is a non-abelian group. The obviously defined sets $GL(n, \mathbb{Q})$ and $GL(n, \mathbb{C})$ are non-abelian groups under matrix multiplication.

Elementary theorems about groups

Theorem 1. *If $x * a = x * b$, then $a = b$ (left cancellation law). If $a * x = b * x$, then $a = b$ (right cancellation law).*

Proof of the left cancellation law.

$x * a = x * b$	Theorem's condition
$x' * (x * a) = x' * (x * b)$	Left multiplication by x'
$(x' * x) * a = (x' * x) * b$	$\mathscr{G}_1$, associativity
$e * a = e * b$	$\mathscr{G}_3$, inverse
$a = b$	$\mathscr{G}_2$, identity.

□

Theorem 2. *Let $(G, *)$ be a group and let a, $b \in G$. The linear equations $a * x = b$ and $y * a = b$ have unique solutions x and y in G.*
Theorem 3. *Let $(G, *)$ be a group. There exist only one identity element e. For any $a \in G$, there exist only one inverse a'.*

Left definition of a group

Definition 3. A binary structure $(G, *)$ is called a **group**, if the following axioms are satisfied.

$\mathscr{G}_1$: The binary operation $*$ is associative.

$\mathscr{G}_2^l$: There exist a **left identity element** $e \in G$ such that for all $a \in G$,

$$e * a = a.$$

$\mathscr{G}_3^l$: For each $a \in G$, there exist a **left inverse** element $a' \in G$ such that

$$a' \cdot a = e.$$

Theorem 4. *The system of* two-sided *axioms $(\mathscr{G}_1, \mathscr{G}_2, \mathscr{G}_3)$ and the system of* left *axioms $(\mathscr{G}_1, \mathscr{G}_2^l, \mathscr{G}_3^l)$ determine the same binary algebraic structures (called* groups*). Likewise, the obviously defined system $(\mathscr{G}_1, \mathscr{G}_2^r, \mathscr{G}_3^r)$ of* right *axioms determine the same binary algebraic structures.*

Finite groups and group tables

Let $(G,*)$ be a group and let G be a *finite* set. The structure of the group G can be completely described by the *group table*. For example,

$\cdot$	1	-1
1	1	-1
-1	-1	1

is the group table of the group $(U_2,\cdot)$. The table

$+_2$	0	1
0	0	1
1	1	0

is the group table of the group $(\mathbb{Z}_2,+_2)$. It is very easy to see that the groups are indeed isomorphic.

Notation

Along with notation from Lecture 2, algebraists use another notation:

Notation of Lecture 2	Additive notation	Multiplicative notation
$a*b$	$a+b$	ab
e	0	1
a'	$-a$	a^{-1}
$a*a*\cdots*a$ (n times)	na	a^n

Additive notation is used only for abelian groups.

Definition 4. The **order** $|G|$ of a group G is the cardinality of the set G.

Subgroups

A *subgroup* H of a group G is a group contained in G so that if h, $h'\in H$, then the product hh' in H is the same as the product hh' in G. The formal definition of subgroup, however, is more convenient to use.

Definition 5. A subset H of a group G is a **subgroup** if

① $1\in H$;

② If a, $b \in H$, then $ab \in H$;

③ if $a \in H$, then $a^{-1} \in H$.

If H is a subgroup of G, we write $H \leq G$; if H is a **proper** subgroup of G, that is, $H \neq G$, then we write $H < G$. G is the **improper** subgroup of G. The subgroup $\{1\}$ is the **trivial subgroup** of G. All other subgroups are **nontrivial**.

Examples of subgroups

Example 9. We have $(\mathbb{Z},+) < (\mathbb{Q},+) < (\mathbb{R},+) < (\mathbb{C},+)$.

Example 10. Let $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$. Then, for any $n \in \mathbb{Z}^+$, we have $(U_n,\cdot) < (U,\cdot) < (\mathbb{C}^*,\cdot)$.

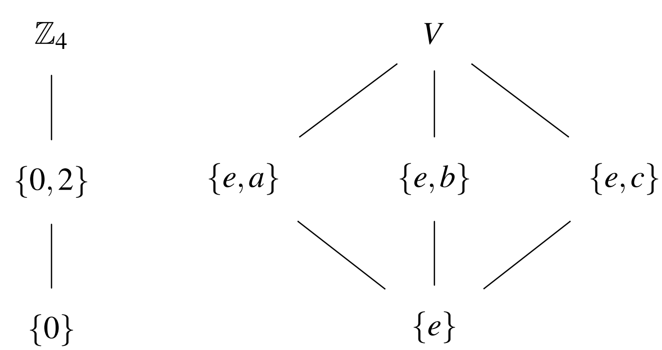
Example 11. The set of cardinality 4 may carry exactly two different group structures. The first is $(\mathbb{Z}_4,+)$,

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

while the second is the **Klein 4-group** V (V abbreviates the original German term *Vierergruppe*):

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$\mathbb{Z}_4$ has only one nontrivial proper subgroup $\{0,2\}$, while V has three nontrivial proper subgroups, $\{e,a\}$, $\{e,b\}$, and $\{e,c\}$. This is shown at the following *subgroup diagrams*.



Cyclic subgroups

Definition 6. If G is a group and $a \in G$, write

$$\langle a \rangle = \{ a^n : n \in \mathbb{Z} \}.$$

$\langle a \rangle$ is called the **cyclic subgroup** of G **generated** by a. A group G is called **cyclic** if there exists $a \in G$ with $G = \langle a \rangle$, in which case a is called a **generator** for G.

Example 12. For any $n \in \mathbb{Z}^+$, U_n is a cyclic group with $\zeta = e^{2\pi i/n}$ as a generator, i.e., $U_n = \langle \zeta \rangle$. Because $\mathbb{Z}_n$ is isomorphic to U_n, $\mathbb{Z}_n$ is also a cyclic group with 1 as a generator, i.e., $\mathbb{Z}_n = \langle 1 \rangle$. Check that $\mathbb{Z}_4 = \langle 3 \rangle$.

Example 13. V is *not* cyclic, because $\langle a \rangle$, $\langle b \rangle$, and $\langle c \rangle$ are proper subgroups.

Example 14. $(\mathbb{Z}, +) = \langle 1 \rangle$. For any $n \in \mathbb{Z}$, the cyclic subgroup generated by n, $\langle n \rangle$, consists of all multiples of n, and is denoted by $n\mathbb{Z}$. We have $n\mathbb{Z} = -n\mathbb{Z}$.

Properties of cyclic groups

Definition 7. Let G be a group, and let $a \in G$. If $\langle a \rangle$ is finite, then the **order** of a is the order $|\langle a \rangle|$ of this cyclic subgroup. Otherwise, we say that a is of **infinite order**.

Theorem 5. *Every cyclic group is abelian.*

Theorem 6 (Division algorithm for $\mathbb{Z}$)**.** *Let $m \in \mathbb{Z}^+$ and $n \in \mathbb{Z}$. Then there exist unique $q \in \mathbb{Z}$ (the **quotient**) and $r \in \mathbb{Z}$ (the **remainder**) such that*

$$n = mq + r \qquad \text{and} \qquad 0 \leq r < m.$$

Proof. Consider all nonnegative integers of the form $n - am$, where $a \in \mathbb{Z}$. Define r to be the smallest nonnegative integer of the form $n - am$, and define q to be the integer a occurring in the expression $r = n - am$.

If $mq + r = mq' + r'$, where $0 \leq r' < m$, then $|(q - q')m| = |r' - r|$. Now $0 \leq |r - r'| < m$ and, if $|q - q'| \neq 0$, then $|(q - q')m| \geq m$. We conclude that both sides are 0, that is, $q' = q$ and $r' = r$. □

Theorem 7. *A subgroup of a cyclic group is cyclic.*

Corollary 1. *The subgroups of* $(\mathbb{Z},+)$ *are* $(n\mathbb{Z},+)$ *for* $n\in\mathbb{Z}$*.*

Let $r\in\mathbb{Z}^+$ and $s\in\mathbb{Z}^+$. Let $H=\langle r,s\rangle$ denotes the smallest subgroup in $(\mathbb{Z},+)$ containing both r and s. H is a subgroup of $(\mathbb{Z},+)$. One can prove that $H=\{nr+ms\colon\, n,m\in\mathbb{Z}^+\}$. By Corollary 1, H has a generator $d\in\mathbb{Z}\setminus\{0\}$, that can be chosen to be positive.

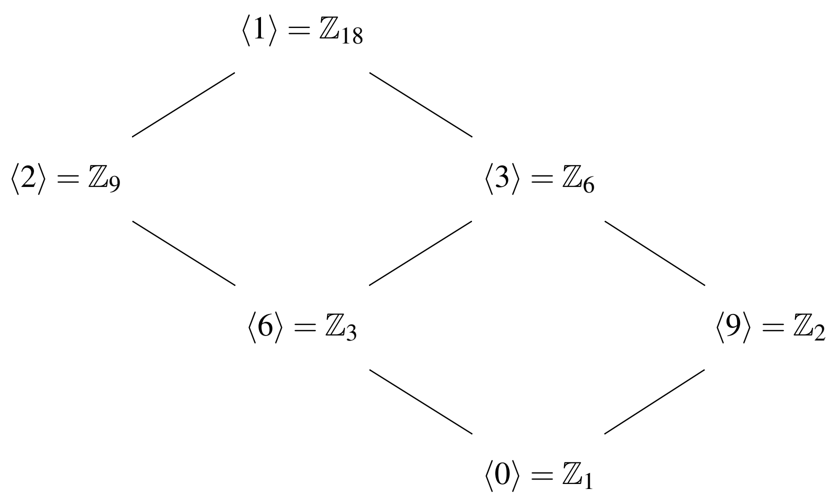
Definition 8. The positive generator d of the cyclic group $H=\{nr+ms\colon\, n,m\in\mathbb{Z}^+\}$ is called the **greatest common divisor** of r and s.

Definition 9. Two positive integers r and s are **relatively prime** if their greatest common divisor is 1.

Theorem 8 (The structure of cyclic groups)**.** *Every infinite cyclic group is isomorphic to the group* $(\mathbb{Z},+)$ *and every finite cyclic group of order* m *is isomorphic to the group* $(\mathbb{Z}_m,+_m)$*.*

Theorem 9. *Let* $G=\langle a\rangle$ *and* $|G|=n$*. Let* $b=a^s\in G$*. Let* d *be the greatest common divisor of* n *and* s*, and let* $H=\langle b\rangle$*. Then* $|H|=n/d$*. In particular,* b *generates all of* G *if and only if* r *is relatively prime with* n*.*

Example 15. The following subgroup diagram is obtained from Theorem 9 by direct calculations.



Generating sets

Let $(G,\cdot)$ be a group, and let S be a subset of G.

Theorem 10. *Let $\langle S \rangle$ be the set of elements of G consisting of all products $x_1 \ldots x_n$ such that x_i or x_i^{-1} is an element of S for each i, and also containing the unit element. It is the smallest subgroup of G containing S.*

Definition 10. The elements of S are called the **generators** of $\langle S \rangle$. If $\langle S \rangle = G$, we say that S **generates** G. If there exists a finite set S that generates G, then G is **finitely generated**.

Example 16. $(\mathbb{Z}, +) = \langle 1 \rangle$ is a finitely generated group. Its subgroup $\langle r, s \rangle$ is also generated by one element d, which is the greatest common divisor of r and s.

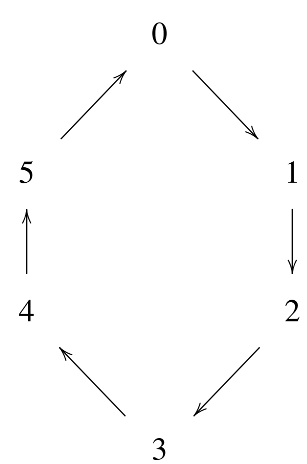
Directed graphs: definition

Definition 11. A **directed graph** (or just digraph) is a finite set of points called **vertices** and some **arcs** (with a direction denoted by an arrowhead or without a direction) joining vertices.

For each generating set S of a *finite* group G, we can construct the following **Cayley digraph** $\mathscr{D}$. The number of vertices in $\mathscr{D}$ is $|G|$. For any $a \in S$, there exist arcs of type a. An arc of type a points from $x \in G$ to $y \in G$ if and only if $y = xa$. If $a \in S$ and $a^2 = e$, it is customary to omit the arrowhead from the arc of type a.

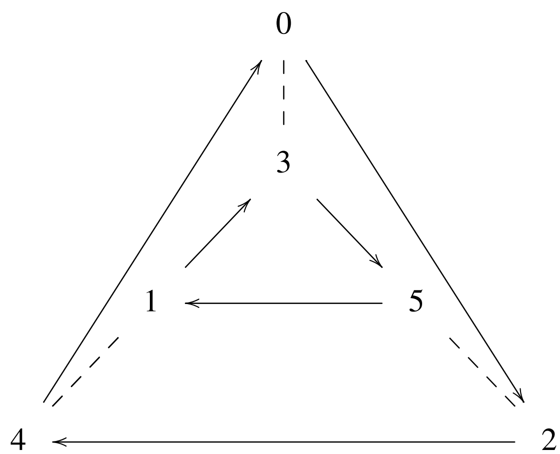
Example: Cayley digraph for $G = \mathbb{Z}_6$ and $S = \{1\}$

Example 17. Let $G = \mathbb{Z}_6$ and $S = \{1\}$. The Cayley digraph has the form



Example: Cayley digraph for $G = \mathbb{Z}_6$ and $S = \{2,3\}$

Example 18. Let $G = \mathbb{Z}_6$ and $S = \{2,3\}$. Let $\longrightarrow$ be an arrow of type 2. Because $3^2 = 0$ in $\mathbb{Z}_6$, the arrow of type 3 must be - - - . The Cayley digraph has the form



A characterisation of Cayley digraphs

Theorem 11. *A digraph $\mathscr{G}$ is a Cayley digraph of some generating set H of a finite group G if and only if the following four properties are satisfied.*

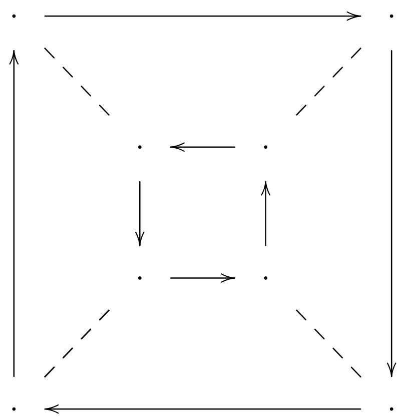
① *$\mathscr{G}$ is connected.*

② *At most one arc goes from vertex g to a vertex h.*

③ *Each vertex g has exactly one arc of each type starting at g, and one of each type ending at g.*

④ *If two different sequences of arc types starting from vertex g lead to the same vertex h, then those same sequences of arc types starting from any vertex u will lead to the same vertex v.*

Cayley used this theorem to construct new groups. For example, the following digraph satisfies all conditions of Theorem 11.



If we label $\longrightarrow$ by a and $- - -$ by b, we obtain a Cayley digraph of a new group of order 8: