Groups

Sergei Silvestrov

Spring term 2011, Lecture 8

Contents of the lecture

- Binary operations and binary structures.
- Groups - a special important type of binary structures.
- Isomorphisms of binary structures.
The essence of a “binary (=two, 2) operation” is that two things are combined to form a third thing of the same kind.

**Definition 1.** A binary operation on a set $G$ is a function

$$*: G \times G \mapsto G.$$

A binary algebraic structure is a set $S$ together with a binary operation $*$ on $S$.

Suppose that $*$ is a binary operation on a set $G$ and $H$ is a subset of $G$. If the restriction of $*$ to $H$ is a binary operation on $H$, i.e., for all $x, y \in H$, $x*y \in H$, then $H$ is said to be closed under $*$.

The binary operation on $H$ given by restricting $*$ to $H$ is the induced operation of $*$ on $H$.

**Binary substructure** is a subset $(H, *)$ with induced operation.
Examples of binary operations, binary structures, induced operations, binary substructures

Example 1. Addition is a binary operation on the set $\mathbb{Z}_+$ whose value at a pair $(x, y)$ is $x + y$.

Example 2. Subtraction is a binary operation on the set $\mathbb{Z}$ whose value at a pair $(x, y)$ is $x - y$.

Example 3. Multiplication is a binary operation on the set $\mathbb{Z}$ whose value at a pair $(x, y)$ is $xy$.

Example 4. Let $\mathcal{M} = \mathcal{F}(\mathbb{R})$ be the set of all real valued functions of a real variable, that is, all functions $f : \mathbb{R} \rightarrow \mathbb{R}$. Then composition $\circ : \mathcal{M} \times \mathcal{M} \rightarrow \mathcal{M}$ is an operation on $\mathcal{M}$ whose value at a pair $(f, g) \in \mathcal{M} \times \mathcal{M}$ is $f \circ g$.

Example 5. The subset of continuous functions $\mathcal{M} = C(\mathbb{R})$ is closed under the operation of composition. (OBS! This is one of the easy theorems from basic 1st year calculus/analysis course) So, $(C(\mathbb{R}), \circ)$ is substructure of $(\mathcal{F}(\mathbb{R}), \circ)$

Example 6. OBS! generalization of previous example
Let $\mathcal{M} = \mathcal{F}(\mathcal{X})$ be the set of all functions (mappings, transformations)

$$f : \mathcal{X} \rightarrow \mathcal{X}$$

Composition $\circ : \mathcal{M} \times \mathcal{M} \rightarrow \mathcal{M}$ is an operation on $\mathcal{M}$ whose value at a pair $(f, g) \in \mathcal{M} \times \mathcal{M}$ is the composition $f \circ g : \mathcal{X} \rightarrow \mathcal{X}$ defined by

$$f \circ g(x) = f(g(x))$$

Example 7. OBS! Linear algebra restriction of previous example
If $\mathcal{X}$ is a linear space, then the subset $\mathcal{L}(\mathcal{X})$ of all linear operators (=linear mappings/linear transformations) on $\mathcal{X}$ form a subset of $\mathcal{M} = \mathcal{F}(\mathcal{X})$ closed under composition. Hence $(\mathcal{L}(\mathcal{X}), \circ)$ is a binary substructure of $(\mathcal{F}(\mathcal{X}), \circ)$. 

– Typeset by FoilTEX –
Commutative, non-commutative and associative operations

The examples of composition and subtraction operations show why ordered pairs $x \ast y$ and $y \ast x$ may be distinct.

**Definition 2.** A binary operation $\ast$ on a set $G$ is **commutative** if for all $x, y \in G$,

$$x \ast y = y \ast x$$

**Example 8.** Addition and multiplication on $\mathbb{Z}_+$ are **commutative**.

**Example 9.** Subtraction on $\mathbb{Z}$ and composition on the set of all functions (=transformations) on a set $\mathcal{X}$ with more than one element are **non-commutative** operations.

**Example 10.** Composition of linear operators on the set of all linear operators on any linear (vector) space of the dimension more than one $\dim \mathcal{X} > 1$ over any field with more than one element is a **non-commutative** operation. The matrix multiplication on the space of matrices of size $n \times n$ with $n \geq 2$ over any field with more than one element is a **non-commutative** operation.

**Example 11.** The matrix multiplication of diagonal matrices (composition of linear operators which correspond to diagonal matrices in some and the same basis) is a commutative operation.

**Definition 3.** A binary operation $\ast$ on a set $G$ is **associative** if for all $x, y, z \in G$ we have

$$x \ast (y \ast z) = (x \ast y) \ast z.$$ 

**Example 12.** Addition and multiplication on $\mathbb{Z}_+$ are associative.

Subtraction on $\mathbb{Z}$ is not associative.

Composition of functions on $\mathcal{M}$ is associative.
The definition of a group

**Definition 4.** (Sec 7.1. p. 163)
A binary structure \((G, \ast)\) is called a **group**, if the following axioms are satisfied.

\(G_1:\) The binary operation \(\ast\) is associative, i.e., for all \(a, b, c \in G\), we have
\[
(a \ast b) \ast c = a \ast (b \ast c).
\]

\(G_2:\) There exist an **unity (identity) element** \(e \in G\) such that for all \(a \in G\),
\[
e \ast a = a \ast e = a.
\]

\(G_3:\) For each \(a \in G\), there exist an **inverse** element \(a' \in G\) such that
\[
a \ast a' = a' \ast a = e.
\]

**Usual notation:** Inverse \(a' = a^{-1}\).
Examples of groups

**Example 13.** \((\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +),\) and \((\mathbb{C}, +)\) are groups with \(e = 0\) and \(a' = -a\).

**Example 14.** \((U, \cdot)\) 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 15.** \((U_n, \cdot)\) 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 16.** 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 17.** \((\mathbb{Z}^+, +)\) is not a group, because there is no unity (identity) element. This is the reason for introducing 0.

**Example 18.** \((\mathbb{Z}^+ \cup \{0\}, +)\) 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 19.** \((\mathbb{Z} \setminus \{0\}, \cdot)\) 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 and non-abelian groups

Definition 5. A group \((G, \ast)\) is **abelian** (or commutative) if \(\ast\) is commutative and non-abelian (or non-commutative) if \(\ast\) is non-commutative (there exist \(x, y \in G\) such that \(x \ast y \neq y \ast x\)).

Until now, we met only abelian groups.

Example 20. 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.
Finite groups and group tables

Let \((G, \ast)\) 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,

\[
\begin{array}{c|cc}
\ast & 1 & -1 \\
\hline
1 & 1 & -1 \\
-1 & -1 & 1 \\
\end{array}
\]

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

\[
\begin{array}{c|cc}
+ & 0 & 1 \\
\hline
0 & 0 & 1 \\
1 & 1 & 0 \\
\end{array}
\]

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

Theorem 1. ("Theorem" 7.1, Sec 7.1. p. 168)
Any ring with its addition as operation is abelian group.

Obs! There is nothing to prove here. It is even funny to call this "theorem" since it is actually a part of a definition of a ring, isn't it?
(Compare pages 42 and 163 to get the point!

Theorem 2. (Thm 7.2, Sec 7.1. p. 169)
In any associative ring with unity (identity element) (unital ring), the set of all units (invertible elements) is a group under multiplication in the ring.

Proof. Easy exercise! The same as for invertible matrices, but now for invertible elements in any unital ring

(Let us do it quickly (2 minutes) together just for fun.

Is 1 in any ring invertible? Is \(a \times b\) invertible for invertible \(a\) and \(b\)? Is the induced product (in a subset of associative ring closed under the product) an associative operation?
Are the answers enough to conclude that invertible elements form a group according to the definition of the group?).

Theorem 3. (Cor 7.3, Sec 7.1. p. 170)
The set of non-zero elements of a field is an abelian group under multiplication.
VERY IMPORTANT EXAMPLE!

Groups of bijective mappings and in particular Permutation groups $S_n$

**Theorem 4.** For any nonempty set $T$, the set of all bijective (= one-to-one = invertible) mappings from $T$ to $T$ form a group under operation of composition.

**Definition 6.** (Compare with p. 161 and example on p. 164)

Invertible mappings of the set with $n$ elements are called **permutations** and form a group under composition, called **permutation group** and denoted $S_n$.

**Example 21.** (Compare with examples on p. 161-163)

Let $T = \{1, 2, 3\}$. Then permutation (that is a bijective map $f: T \rightarrow T$) can be represented as

$$
\begin{pmatrix}
1 & 2 & 3 \\
 f(1) & f(2) & f(3)
\end{pmatrix}
$$

Composition

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$f \circ g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$g \circ f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$ (f \circ g)(1) = f(g(1)) = f(3) = 2 $$

Inverse of permutation

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad f^{-1} = \begin{pmatrix} 3 & 1 & 2 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Check NOW in 3 minutes that

$$f \circ f^{-1} = e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$ (identity permutation)

For more examples look in Chapter 7.1!
Elementary theorems about groups

Theorem 5. (Thm 7.5, p. 174)
In any group:

1. There exist only one unity element $e$.

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

3. For any $a \in G$, there exist only one inverse $a^{-1}$.

Proof. 1) If $e_1$ and $e_2$ are two unity elements, then $e_1 = e_1e_2 = e_2$.

2)

\[
\begin{align*}
  x * a &= x * b \\
  x' * (x * a) &= x' * (x * b) \\
  (x' * x) * a &= (x' * x) * b \\
  e * a &= e * b \\
  a &= b
\end{align*}
\]

3) $aa_1^{-1} = aa_2^{-1} = e \Rightarrow a_1^{-1} = a_2^{-1}$
by the left cancelation law proved in part 2.

Theorem 6. (Exercise 15 (a), p. 179)
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 $G$.

Proof. For $a * x = b$ the solution must be $x = a^{-1}b$ as this is obtained by multiplying both sides of the equation by $a^{-1}$ from the left.
For $y * a = b$ the solution must be $y = ba^{-1}$ as this is obtained by multiplying both sides of the equation by $a^{-1}$ from the left.
Then, the uniqueness of the solution for both equations follows from uniqueness $a^{-1}$ of inverse element for any element $a \in G$. 

\[\Box\]
Theorem 7. (Cor 7.6, Sec 7.2, p. 175)

\((ab)^{-1} = b^{-1}a^{-1}\) and \((a^{-1})^{-1} = a\)

Proof. \( (ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = (ae)a^{-1} = aa^{-1} = e, \)
and \((a^{-1})^{-1} = a \iff a^{-1}a = e. \)

\(\square\)
Definition 7. (Sec 7.2, p. 176)
Order $|a|$ of an element $a \in G$ is the smallest positive integer $n$ such that $a^n = a \cdots a = e$ or $\infty$ if such positive integer does not exists.

Theorem 8. (Thm 7.8, Sec 7.2, p. 177)

1. If $a \in G$ is of infinite order, then $i \neq j \Rightarrow a^i \neq a^j$
2. If $|a| = n$, then $a^k = e \iff n | k$
3. If $|a| = n$ and $n = td$ with $d > 0$, then $|a^d| = d$

Proof. 1) $e = a^i (a^j)^{-1} = a^i a^{-j} = a^{i-j}$ which is in contradiction with infinite order of $a$.
2) $\iff: n | k \Rightarrow k = tn \Rightarrow a^k = (a^n)^k = e^k = e$.
$\Rightarrow: n \leq k$ since $n = |a|$ is the smallest positive integer such that $a^n = e$.
$k = qn + r, \quad 0 \leq r < n \Rightarrow e = a^k = a^{qn+r} = (a^n)^q a^r = e^q a^r = a^r$
But $n = |a|$ is the smallest positive integer such that $a^n = e$. Thus $r = 0$ and hence $n | k$.
3) $(a^d)^k = a^{kd} = a^n = e$.
$d$ is the smallest since $e = (a^d)^k = a^{kd} \Rightarrow n = (td)(tk) \Rightarrow d | k \Rightarrow d \leq k$

Theorem 9. (Cor 7.9, Sec 7.2, p. 178)
If every element in a group $G$ is of a finite order, then the order $|a|$ of every element $a \in G$ divides $c = \max\{|a| : a \in G\}$.
Isomorphisms of binary structures

Definition 8. Let \((S, \ast)\) and \((S', \ast')\) be the binary algebraic structures. An isomorphism of \((S, \ast)\) with \((S', \ast')\) is a one-to-one correspondence \(\varphi: S \mapsto S'\) such that for all \(x, y \in S\) the following homomorphism property holds:

\[ \varphi(x \ast y) = \varphi(x) \ast' \varphi(y). \]

If such a map \(\varphi\) exists, we say that \((S, \ast)\) and \((S', \ast')\) (or just \(S\) and \(S'\)) are isomorphic binary structures, and denote this by \(S \simeq S'\).

Guidelines for proving the isomorphism of binary structures

There exist only one way to prove that two binary structures \(S\) and \(S'\) are isomorphic: propose a map \(\varphi\) and prove that your map satisfies Definition 8. So, you need to do four steps.

1. Write a formula for \(\varphi\).
2. Prove that \(\varphi\) is one-to-one (injective).
3. Prove that \(\varphi[S] = S'\) (\(\varphi\) is surjective).
4. Prove the homomorphism property.

Example 22. Let \(n \in \mathbb{Z}^+\), and let \((S, \ast) = (\mathbb{Z}_n, +_n)\) be the binary structure of integers modulo \(n\) with the binary operation of addition modulo \(n\), and let \((S', \ast') = (U_n, \cdot)\) be the binary structure of \(n\)-th roots of 1 in complex numbers with the binary operation of usual multiplication of complex numbers.

Define \(\varphi: \mathbb{Z}_n \mapsto U_n\) as

\[ \varphi(k) = e^{2k\pi i/n}. \]

If \(\varphi(k) = \varphi(l)\), then \(e^{2k\pi i/n} = e^{2l\pi i/n}\). Taking the natural logarithm, we have \(2k\pi i/n = 2l\pi i/n\), so \(k = l\).

If \(\theta \in U_n\), then \(\theta = 2k\pi/n\) for \(k \in \mathbb{Z}_n\), and \(\varphi(k) = e^{2k\pi i/n} \in U_n\). Thus \(\varphi\) is onto \(U_n\).

For \(k, l \in \mathbb{Z}_n\) we have \(\varphi(k +_n l) = e^{2(k+l)\pi i/n} = e^{2k\pi i/n} \cdot e^{2l\pi i/n} = \varphi(k) \cdot \varphi(l)\).

Example 23. Let \(U\) be the unit circle in the complex plane. The map \(\varphi(\theta) = e^{i\theta}\) maps \(\mathbb{R}_{2\pi}\) onto \(U\) and establishes an isomorphism between binary structures \((\mathbb{R}_{2\pi}, +)\) and \((U, \cdot)\).
Example 24. Let $\mathcal{X}$ be ANY finite-dimensional linear/vector space $\dim(\mathcal{X}) = n < \infty$ over complex or real numbers (or other field $F$).
Then $(\mathcal{L}(\mathcal{X}), \circ)$ is isomorphic to the well-known specific binary structure $(M_n(F), \cdot)$ of $n \times n$ matrices over $F$ with the binary operation of usual matrix multiplication.

How to choose isomorphism map $\varphi: \mathcal{L}(\mathcal{X}) \mapsto M_n(F)$?

Guess the answer in 1 minute!

Hint: OBS! You already know it, do’nt you?
Guidelines for proving the non-isomorphism of binary structures

There exist only one way to prove that two binary structures $S$ and $S'$ are not isomorphic: find a property that must be shared by any isomorphic structures (structural property) but distinguishes $S$ and $S'$.

Example 25. Because any isomorphism $\phi$ is a one-to-one correspondence, two isomorphic binary structures must have the same cardinality. Thus, the binary structures $(\mathbb{R}, +)$ and $(\mathbb{Q}, +)$ are not isomorphic.

Example 26. We have $|\mathbb{Z}| = |\mathbb{Q}| = \aleph_0$. However, an equation $2 \cdot x = 1$ has a solution $x = 1/2$ in $\mathbb{Q}$, but no solutions in $\mathbb{Z}$. Therefore the binary structures $(\mathbb{Q}, \cdot)$ and $(\mathbb{Z}, \cdot)$ are not isomorphic.

Example 27. The binary structures, the set of all complex matrices of the size $2 \times 2$ with matrix product and the set of complex numbers with the product (OBS! the same as matrix product on $1 \times 1$ matrices), are non-isomorphic.

Guess in 1 minute:
Which important property that must be preserved by any isomorphism is different in these two algebraic structures?