Lecture Notes in Algebra

Cem Tezer

Ankara, 2008

Ortadoğu Teknik Üniversitesi
Matematik Bölümü
Groups

A binary operation on a set $M$ is a function from $M \times M$ into $M$.

Examples:

1. The addition on $\mathbb{Z}$ is the binary operation $+ : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ that sends each $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ into $x + y \in \mathbb{Z}$. (Only a pedant would dream of writing $+ ((x, y))$ instead of $x + y$!) Analogously: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{I}$.

Indeed, in connection with a binary operation $\mu$ on $M$, one writes $a \mu b$ instead of $\mu ((a, b))$. This, too, is abbreviated into $ab$, unless confusion is likely.

2. Multiplication on the "classical number systems" $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{I}$.

3. On any set $M$, let $\odot : M \times M \rightarrow M$ be defined by $x \odot y = x$. This is a (rather futile!) binary operation on $M$.

4. Matrix addition and multiplication on $\mathbb{R}^{n \times n}$ (the set of $n \times n$ matrices with real entries.) Similarly for matrices with rational, real, complex, quaternion
entries.

(5) Let \( A \) be an arbitrary set, \( M \) be the set of functions from \( A \) into \( A \). The "functional composition" that sends \( (f, g) \in M \times M \) into \( f \circ g \) is a binary operation.

Terminology:

Talking about a generic binary operation \( x, y \rightarrow xy \): The binary operation is said to be **associative** if \( x(yz) = (xy)z \) for all \( x, y, z \). In connection with an associative binary operation, it is possible to dispense with brackets entirely: Write \( xyz \) instead of \( x(yz) \) or \( (xy)z \) ! "Powers" make sense: Write \( x^n \) for \( \underbrace{xx \cdots xx}_{n \text{-times}} \).

In connection with a binary operation on a set \( M \), an element \( \alpha \in M \) is referred to as a **right identity** if \( x\alpha = x \) for all \( x \in M \). **Left identity** is defined similarly. With respect to the binary operation \( \circ \) defined in page 1, all \( x \in M \) are right identities. An element is called an **identity** (or *neutral element*) if it is a right identity and a left identity at the same time.

Notice that with respect to an associative binary operation there exists at most one identity. (That is, if an identity exists, then it is unique.) Indeed if \( \alpha, \alpha' \in M \) are identities with respect to \( \circ \)
binary operation on $M$, then 
\[ e' = e'e = e. \]

Given a binary operation $\mu$ on $M$, a subset $K \subseteq M$ is said to be closed with respect to $\mu$, if $\mu(a, b) \in K$ for every $a, b \in K$. Equivalently, $K \subseteq M$ is closed with respect to $\mu$ if $\mu(K \times K) \subseteq K$.

If $K$ is closed with respect to $\mu$, then clearly $\mu|_{K \times K}$ is a binary operation in $K$.

**Definition:** A group is a system $(G, \mu)$ where $G$ is a set and $\mu$ is a binary operation on $G$ such that (writing $xy$ instead of $\mu((x,y))$ !)

1) $x(yz) = (xy)z$ for all $x, y, z \in G$.

(The binary operation is associative !)

2) There exists $e \in G$ such that $xe = ex = x$ for all $x \in G$. (In $G$, there is an identity element. It is, of course, unique. It is the identity in $G$.)

3) For each $x \in G$, there exists $y \in G$ such that $xy = yx = e$.

**Remarks:**

(a) The $y$ associated with $x$ in 3) is unique: If $\exists y, z \in G$ such that $xy = yx = xz = zx = e$, then $z = ze = z(xy) = (zx)y = ey = y$.

The unique $y$ associated with $x$ in this fashion is called the inverse of $x$. It is denoted by $x^{-1}$.
(b) In a group $G$, the cancellation law holds:

$$ax = bx \iff a = b \iff xa = xb$$

for all $a, b, x \in G$. (Proof: Multiply by inverses on the right and on the left!)

(c) The axioms 2), 3) above can be replaced (in the presence of 1), of course!) with the following:

2$^R$) There exists $e \in G$ such that $xe = x$

for all $x \in G$.

3$^R$) For each $x \in G$, there exists $y \in G$ such that $xy = e$.

Indeed, $2^R \& 3^R$ hold: given $x \in G$, $\exists y \in G$ with $xy = e$ and $\exists z \in G$ with $yz = e$. Consequently,

$$x = xe = (xy)z = (xy)z = e z$$

and $y x = y (ez) = (ye)z = yz = e$.

Therefore $\Box$ is valid. Now, given $x \in G$, $\exists y \in G$ with $xy = yx = e$,

and $\exists z \in G$ such that $xy = x(yx) = xe = x$.

which shows that $\Box$ is valid.

One can similarly formulate $2^L, 3^L$ and show that they together imply 2), 3). However, the operation $\odot$ in page 1 shows that $2^R \& 3^L$ won't do!
**Examples:**

(0) The **trivial group** is a singleton \( \{a\} \) with the binary operation \( aa = a \).

(1) \( \mathbb{Z}, \mathbb{Q}, \mathbb{IR}, \mathbb{C}, \mathbb{N} \) are groups with respect to addition. \( \mathbb{Q}\setminus \{0\}, \mathbb{IR}\setminus \{0\}, \mathbb{C}\setminus \{0\}, \mathbb{N}\setminus \{0\} \) are groups with respect to multiplication.

(2) \( \mathbb{Z}_n \), integers modulo \( n \) constitute a group with respect to addition.

(3) Given any set \( A \), a bijection of \( A \) onto itself is referred to as a **permutation** of \( A \). Clearly all permutations of \( A \) constitute a group, which \( S_A \) denote by \( S_A \). If \( A \) is finite, to be quite definite, if \( A = \{1, 2, \ldots, n\} \), let's write \( S_n \) for \( S_A \). \( S_n \) is called the group of **permutations** of \( n \) objects. An element \( \sigma \in S_n \) is described explicitly by a table of the form

\[
\begin{bmatrix}
1 & 2 & \ldots & n \\
\sigma(1) & \sigma(2) & \ldots & \sigma(n)
\end{bmatrix}
\]

(2') The subset \( U(n) \) of \( \mathbb{Z}_n \) consisting of residue classes of \( n \) which are relatively prime to \( n \) constitute a group under multiplication. I intend to revisit the general case later. Let's consider the instance \( U(10) = \{\overline{1}, \overline{3}, \overline{7}, \overline{9}\} \).
and describe it fully by its "multiplication table":

<table>
<thead>
<tr>
<th>$\mathbb{U}(10)$</th>
<th>$\bar{1}$</th>
<th>$\bar{3}$</th>
<th>$\bar{7}$</th>
<th>$\bar{9}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\bar{1}$</td>
<td>$\bar{1}$</td>
<td>$\bar{3}$</td>
<td>$\bar{7}$</td>
<td>$\bar{9}$</td>
</tr>
<tr>
<td>$\bar{3}$</td>
<td>$\bar{3}$</td>
<td>$\bar{9}$</td>
<td>$\bar{1}$</td>
<td>$\bar{7}$</td>
</tr>
<tr>
<td>$\bar{7}$</td>
<td>$\bar{7}$</td>
<td>$\bar{1}$</td>
<td>$\bar{9}$</td>
<td>$\bar{3}$</td>
</tr>
<tr>
<td>$\bar{9}$</td>
<td>$\bar{9}$</td>
<td>$\bar{7}$</td>
<td>$\bar{3}$</td>
<td>$\bar{1}$</td>
</tr>
</tbody>
</table>

In group theory such a table is called the **Cayley Table** of a group.

$(3') \quad S_3 = D_6$ in detail. The group of permutations of 3 objects is also the dihedral group of order 6.

$\begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}$, $\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}$, $\begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix}$

These permutations may be regarded as "Euclidean motions" of an equilateral triangle:

![Diagram of S_3 = D_6](image)
The Cayley table of $S_3 = D_6$:

<table>
<thead>
<tr>
<th></th>
<th>$p_0$</th>
<th>$p_1$</th>
<th>$p_2$</th>
<th>$m_1$</th>
<th>$m_2$</th>
<th>$m_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$p_0$</td>
<td>$p_0$</td>
<td>$p_1$</td>
<td>$p_2$</td>
<td>$m_1$</td>
<td>$m_2$</td>
<td>$m_3$</td>
</tr>
<tr>
<td>$p_1$</td>
<td>$p_1$</td>
<td>$p_2$</td>
<td>$p_0$</td>
<td>$m_1$</td>
<td>$m_2$</td>
<td>$m_3$</td>
</tr>
<tr>
<td>$p_2$</td>
<td>$p_2$</td>
<td>$p_0$</td>
<td>$p_1$</td>
<td>$m_2$</td>
<td>$m_3$</td>
<td>$m_1$</td>
</tr>
<tr>
<td>$m_1$</td>
<td>$m_1$</td>
<td>$m_2$</td>
<td>$m_3$</td>
<td>$p_0$</td>
<td>$p_1$</td>
<td>$p_2$</td>
</tr>
<tr>
<td>$m_2$</td>
<td>$m_2$</td>
<td>$m_3$</td>
<td>$m_1$</td>
<td>$p_2$</td>
<td>$p_0$</td>
<td>$p_1$</td>
</tr>
<tr>
<td>$m_3$</td>
<td>$m_3$</td>
<td>$m_1$</td>
<td>$m_2$</td>
<td>$p_1$</td>
<td>$p_2$</td>
<td>$p_0$</td>
</tr>
</tbody>
</table>

that is, distance preserving bijections of the plane.

(4) The dihedral group of order $2n$, denoted by $D_{2n}$, is the set of "Euclidean motions" which send a regular $n$-gon into itself, of course with respect to the functional composition of the "motions".

(4') $D_8$ in detail:

![Diagrams of $D_8$](image-url)
\[ e = \rho_0 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{bmatrix} \quad M_1 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix} \]

\[ \rho_1 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix} \quad M_2 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{bmatrix} \]

\[ \rho_1^2 = \rho_2 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{bmatrix} \quad \delta_1 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{bmatrix} \]

\[ \rho_1 = \rho_1^{-1} = \rho_3 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{bmatrix} \quad \delta_2 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{bmatrix} \]

**Left to the student:** Construct the Cayley table of \( D_8 \)!

(5) \( GL(n, \mathbb{R}) \), the general linear group (of degree \( n \)) over \( \mathbb{R} \) is the set of non-singular \( n \times n \) matrices. It constitutes a group with respect to the matrix multiplication.

(6) \( A_4 \), the alternating group of \( n = 4 \) objects will be presented here as the group of Euclidean motions of a regular tetrahedron:
\[
\begin{align*}
\rho_0 &= \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{bmatrix}, & \quad M_1 &= \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \\ 4 & 2 & 1 & 3 \\ 3 & 2 & 4 & 1 \\ 2 & 3 & 1 & 4 \end{bmatrix}, & \quad \omega_1 &= \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{bmatrix}, \\
\rho_1 &= \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{bmatrix}, & \quad M_2^{-1} &= \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{bmatrix}, & \quad \omega_2 &= \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{bmatrix}, \\
\rho_2 &= \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 3 & 1 & 4 \end{bmatrix}, & \quad M_3 &= \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{bmatrix}, & \quad \omega_3 &= \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{bmatrix}, \\
\rho_3 &= \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ 3 & 1 & 2 & 4 \\ 2 & 3 & 1 & 4 \end{bmatrix}, & \quad M_4 &= \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{bmatrix}, & \quad \omega_4 &= \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 4 \end{bmatrix}.
\end{align*}
\]

Given a group \( G \), the cardinality of the set \( G \) is referred to as the **order** of \( G \), denoted by \( |G| \). A group is said to be **finite** if \( |G| < \infty \). A group is said to be **commutative** (or **Abelian**) if \( xy = yx \) for all \( x, y \in G \).

Clearly, \( |\mathbb{Z}_n| = n \), \( |S_n| = n! \), \( |A_4| = 12 \), \( |D_8| = 8 \). \( |U(n)| \) is denoted by \( \varphi(n) \), called the Euler totient function. It is of fundamental importance in number theory. \( \mathbb{Z}_n \) and \( U(n) \) are commutative.

**Definition**: Given a group \( G \), a nonempty subset \( H \subseteq G \) is said to be a **subgroup** of \( G \) if \( H \) is closed under the binary operation of \( G \) and constitutes a group under the binary operation of \( G \).