Math 521A

7.1 – Definition and Examples of Groups

Definition

A group $(G, *)$ is a nonempty set G, closed under a binary operation $*$, such that the following axioms are satisfied:

1. Associativity: $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$.
2. Existence of an identity element: There exists $e \in G$ such that $a * e = e * a = a$ for all $a \in G$.
3. Existence of inverses: For each $a \in G$, there exists $d \in G$ such that $a * d = d * a = e$.

G is said to be Abelian or commutative if $a * b = b * a$ for all $a, b \in G$.

Example

Let $+$ denote usual addition. Then $(\mathbb{Z}, +), (\mathbb{Q}, +)$, and $(\mathbb{R}, +)$ are all groups, but $(\mathbb{N}, +)$ is *not* a group.

Example

Let $\cdot$ denote usual multiplication. Then $(\mathbb{Z}, \cdot), (\mathbb{Q}, \cdot)$, and $(\mathbb{R}, \cdot)$ are *not* groups.

Applications of groups:

1. **Algebra**: The criterion for deciding whether a polynomial equation is solvable by radicals involves group theory.
2. **Number theory**: Remainders when a^m is divided by n: One can use group theory to show that the last two digits of a^{40} are always 01 provided $2 \not| a$ and $5 \not| a$. Representation of integers by quadratic forms like $ax^2 + 2bxy + cy^2$.
3. **Combinatorics**, in particular counting (e.g., in how many distinguishable ways can we construct a die?).
4. **Cryptography**: Transmission of secret messages.
5. **Topology**: Homotopy and homology groups are associated with topological spaces. Two topological spaces are homeomorphic if there is a bijection f between them such that both f and f^{-1} are continous. Homeomorphic spaces have associated groups that are isomorphic.
6. **Physics and Chemistry**: Quantum mechanics, crystal chemistry.
7. **Computer graphics**: Symmetries of objects.

- We will start our study of group theory by analyzing the symmetries of an equilateral triangle.
- A symmetry is any rigid motion of the triangle which can be effected by taking a copy of the triangle, moving the copy in any fashion in 3-dimensional space, and then placing the copy back on the original triangle so it exactly covers it. Several examples are shown on the board:

r : rotation counterclockwise about the origin through $120^\circ = \frac{2\pi}{3}$ radians.
s : reflection about the line of symmetry through vertex 1 and the origin.

- By "combining" (i.e. composing) r and s we obtain other symmetries. The total number of symmetries of an equilateral triangle equals six. They are given by:

$$D_3 = \{\mathrm{id}, r, r^2, s, rs, r^2 s\}.$$

- D_3 is a group whose operation is composition of symmetries.

- Below is the (operation) table for D_3. The symbol $\circ$ denotes composition of symmetries.

$\circ$	id	r	r^2	s	rs	r^2s
id	id	r	r^2	s	rs	r^2s
r	r	r^2	id	rs	r^2s	s
r^2	r^2	id	r	r^2s	s	rs
s	s	r^2s	rs	id	r^2	r
rs	rs	s	r^2s	r	id	r^2
r^2s	r^2s	rs	s	r^2	r	id

- The motivation for the letter D comes from "dihedral." For any integer $n \geq 3$, D_n denotes the group of symmetries of a regular n-gon. D_n is called the dihedral group of degree n.

Example

The symmetry group of a square (D_4) is worked out on the board. More specifically,

$$D_4 = \{\mathrm{id}, r, r^2, r^3, s, rs, r^2s, r^3s\}$$

where r denotes rotation clockwise about the origin through 90° and s the reflection about the line of symmetry through vertex 1 and the origin.

One can extend the previous ideas and consider the symmetry group of a regular solids, such as the cube, tetrahedron, etc.

* * *

Permutation Groups:

Let $T = \{1, 2, 3\}$ and S_3 the symmetric group on 3 symbols, that is, the group formed by all permutations of T. By a permutation of T, we mean a bijection from T to T. Examples:

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

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \; \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \; \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Meaning of notation: Each permutation of T – represented above by a two-line array – maps an integer in the first row to the integer lying directly below it. For example, $f(1) = 1, f(2) = 3, f(3) = 2$.

The composition of two bijective functions is itself bijective. Thus, composing any two of the six mappings as above will result in one of the six mappings. For example, let

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \text{ and } g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Then:

$$\begin{array}{rcccccc} (f \circ g)(1) & = & f(g(1)) & = & f(2) & = & 3 \\ (f \circ g)(2) & = & f(g(2)) & = & f(1) & = & 1 \\ (f \circ g)(3) & = & f(g(3)) & = & f(3) & = & 2. \end{array}$$

Alternatively, $f \circ g$ can be obtained as follows:

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

Inverses: The inverse of $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ equals $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$. [You may check the result by composing the two mappings and seeing that the result equals I, the identity mapping.]

- The set of six permutations presented on slide #6 forms a group known as the symmetric group on 3 letters or the symmetric group of degree 3.
- Of course we can generalize it to n letters, $n \geq 2$, obtaining the symmetric group on n letters. Notation: S_n. Note that S_n is a group whose operation $\circ$ is *composition of mappings*.
- The number of elements of S_n (i.e., the cardinality of S_n) equals $n!$ (n factorial).

Definition

A group G is said to be finite if it has a finite number of elements, called the order of G. A group with infinitely many elements is said to have infinite order.

Notation: $|G|$ = order of G.

Example

For $n \geq 2$, $|S_n| = n!$. For $n \geq 3$, $|D_n| = 2n$.

Connections Between Groups and Rings:

Theorem

Every ring is an Abelian group under addition.

Remark: A nonzero ring is never a group under multiplication.

Theorem

If R is a ring with identity, then the set U of all units in R is a group under multiplication.

Corollary

Let F be a field. Its set of nonzero elements, denoted by F^*, is an Abelian group under multiplication.

Example

Let $n \geq 2$. The units of the ring $\mathbb{Z}_n$ are denoted by U_n. So, $U_4 = \{1, 3\}$, $U_5 = \{1, 2, 3, 4\}$, $U_6 = \{1, 5\}$. If p is prime, then $U_p = \{1, 2, \ldots, p-1\}$.

Example

$M_2(\mathbb{R})$ (all 2×2 matrices with entries in $\mathbb{R}$) is a ring under the usual operations of $+$ and $\times$ for matrices. The set of units of this ring forms the group

$$\mathrm{GL}(2, \mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \text{ and } ad - bc \neq 0 \right\},$$

which is called the general linear group of degree 2 over $\mathbb{R}$. $\mathrm{GL}(2, \mathbb{R})$ is a non-Abelian group having infinitely many elements.

New Groups from Old:

Theorem

Let G (with operation $*$) and H (with operation $\circ$) be groups. Define an operation $\bullet$ on $G \times H$ by

$$(g, h) \bullet (g', h') = (g * g', h \circ h').$$

Then $G \times H$ is a group. If G and H are Abelian, then so is $G \times H$. If G and H are finite, then so is $G \times H$ and $|G \times H| = |G||H|$.