II. Groups

A. Introduction

A group is a set $G$ with a binary operation, i.e. a mapping $*: G \times G \to G$, satisfying

\[\begin{align*}
&A.1 \quad \left\{ 
\begin{array}{ll}
(i) & (x \cdot y) \cdot z = x \cdot (y \cdot z) \quad (\forall x, y, z \in G) \quad \text{[associativity]} \\
(ii) & \exists \ "1" \in G \quad \text{s.t.} \quad 1 \cdot x = x = x \cdot 1 \quad (\forall x \in G) \quad \text{[identity]} \\
(iii) & \forall x \in G \quad \exists \ "x^{-1}" \in G \quad \text{s.t.} \\
& \quad \quad \quad \quad \quad x^{-1} \cdot x = 1 = x \cdot x^{-1} \quad \text{[inverses]} 
\end{array}
\right. \\
\end{align*}\]

Associativity means that there is no need for parentheses in a product like $a \cdot b \cdot c \cdot d \cdot e$. The operator $*$ is not in general commutative; when it is, a group is said to be abelian, and (only then) you will sometimes encounter the notation $\{+, 0\}$ in lieu of $\{1, x^{-1}\}$.

If we drop hypothesis (iii) above, then $(A.1)(i-ii)$ defines a monoid. We will often write groups & monoids in the form (set, binary operation, identity element), e.g.

"$(G, \cdot, 1)$".
Continuing our overview, a homomorphism is a map of groups (or monoids) — i.e. of the sets —
\[ \varphi : G \rightarrow H \]
respecting the binary operation
\[ \varphi(x\cdot y) = \varphi(x) \cdot \varphi(y) \quad \forall x, y \in G \]
and with \( \varphi(1_G) = 1_H \). (In the case of groups, \( \varphi(x^{-1}) = \varphi(x)^{-1} \)
follows at once.)

Groups abound in mathematics and physics, e.g. via rotational symmetries of a polyhedron or permutations of
n particles. (Not that people in physics always liked this — Pauli: “Gruppenpest.”) Some more interesting examples:

1. **Galois theory.** Structure of group of permutations of roots of polynomials [roughly]
   \[ \Rightarrow \] insolubility of general quintic equation by radicals
   - impossibility of trisecting angle w. straightedge & compass
   - impossibility of “duplicating the cube” (constructing \( \sqrt[3]{2} \) using
     unit grid)

2. **Quantum physics.** The manner in which different atomic
   states of an electron (eigenfunctions of the Schrödinger
   operator) come packaged has to do with the irreducible
   representations of the symmetry group \( O(3) \).
(3) Topology of manifolds. homotopy (nonabelian) +
  homology (abelian) groups (of invariants) can be
  utilized to determine, say,
  • the impossibility of a continuous embedding of one
    manifold into another
  • the impossibility of giving a smooth hairstyle to a sphere.

(4) Diophantine equations. solutions (in integers) of algebraic
  equations (e.g. $x^2 - dy^2 = \pm 1$) sometimes have a group
  structure — meaning that by 'taking powers' of one
  solution you get further solutions. (Similar phenomena
  arise in complex algebraic geometry.)

What is the "representation theory" mentioned in (2) is all
about: suppose you have a group $G$ of transformations
of a vector space $V$ [or permutations of a set $X$].

This can profitably be separated into two concepts: (i) the
abstract group, and (ii) homomorphism from that group
into $\text{GL}(V)$ [or $S_X$] — called a group representation
[or group action]. There are extensive classification results
for abstract groups and their representation; one uses
These to ‘recognise’ G and to list possibilities for the representation (and hence e.g. for the decomposition of V under the original set of transformations). We’ll see some of the classification results for (finite & abelian) groups and of the theory of group actions $G \xrightarrow{\phi} S_\mathbb{E}$ soon, and representation theory in the Spring term.

You are no doubt familiar with the noncommutativity of matrix multiplication (in the group $GL_2(\mathbb{Q})$, say):

$$(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}) \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$

but here is an example in a finite group: take a sheet of paper, write “Top” at the top; then

1. rotate $90^\circ$ counter clockwise (“r”)
2. flip (“h”)
3. rotate $90^\circ$ clockwise (“r$^{-1}$”)
4. flip (“h$^{-1}$x”)

If this group of symmetries of the square (the dihedral group $D_4$, with elements 1, r, r$^2$, r$^3$, h, hr, hr$^2$, hr$^3$) were abelian, then (x) would equal 1. But “Top” doesn’t reappear at the top, and indeed (x) = r$^2$.