II. Groups

II.A. Introduction

A **group** is a set G with a binary operation, i.e. a map[1]

$$\bullet \colon G \times G \to G\,,$$

satisfying

$$\text{(II.A.1)} \qquad \begin{cases} \text{(i) [associativity] } (x \cdot y) \cdot z = x \cdot (y \cdot z) \\ \text{(ii) [identity] } \exists \text{ “}1\text{”} \in G \text{ s.t. } 1 \cdot x = x = x \cdot 1 \\ \text{(iii) [inverses] } \exists \text{“}x^{-1}\text{”} \in G \text{ s.t. } x^{-1} \cdot x = 1 = x \cdot x^{-1} \end{cases}$$

for all $x, y, z \in G$. Associativity means that there is no need for parentheses in a product like $a \cdot b \cdot c \cdot d \cdot e$. The operator $\bullet$ is *not* in general commutative; when it is, a group is said to be **abelian**, and (only then) you will sometimes encounter the notation $+, 0, -x$ in lieu of $\bullet, 1, x^{-1}$. If we drop hypothesis (iii) above, then (i)-(ii) define a **monoid**. We will often write groups and monoids in the form “(set, binary operation, identity element)”, e.g. “$(G, \bullet, 1_G)$”.

Continuing our overview, a **homomorphism** is a map of groups (or monoids) — i.e. of the underlying sets —

$$\varphi \colon G \to H$$

respecting the binary operation

$$\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y) \qquad (\forall\, x, y \in G)$$

and with $\varphi(1_G) = 1_H$. (In the case of groups, $\varphi(x^{-1}) = \varphi(x)^{-1}$ follows at once.)

---

[1] We'll use a large dot “$\bullet$” when talking about the operation, and a small dot “$\cdot$” when using it.

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 talked about the "Gruppenpest". Here are some more interesting examples of this pest:

(1) **Galois theory.** By considering the structure of [roughly] the group of permutations of the roots of a polynomial, one arrives at:
   - the insolubility of a general quintic equation by radicals;
   - the impossibility of trisecting an angle with a straightedge and compass;
   - the impossibility of "duplicating the cube" (constructing $\sqrt[3]{2}$ using a 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.** The (nonabelian) **homotopy** and the (abelian) **homology** groups of a manifold can be utilized to determine (for example):
   - the impossibility of a continuous embedding of one manifold into another; or
   - the impossibility of giving a smooth hairstyle to a sphere.

(4) **Diophantine equations.** Integer solutions of algebraic equations (e.g. $x^2 - y^2 d = \pm 1$) sometimes have a group structure — meaning that by "taking powers" of one solution you get further solutions. (Similar phenomena arise in algebraic geometry over the complex numbers or "finite fields".)

As to what the "representation theory" mentioned in (2) is all about: suppose you have a group G *of* linear transformations of a vector space V [or permutations of a set X]. This can profitably be separated into two concepts: (i) the abstract group G; and (ii) a homomorphism from that group into $GL(V)$ [or $\mathfrak{S}_X$] — called a group representation [or group action]. There are extensive classification results for abstract groups *and* their representations; one uses these to "recognize" 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 and/or abelian) groups and of the theory of group actions $G \stackrel{\varphi}{\to} \mathfrak{S}_X$ soon, and representation theory in Algebra II.

You are no doubt familiar with the noncommutativity of matrix multiplication: for instance,

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

is a computation in the infinite[2] group $GL_2(\mathbb{Q})$. Here is an example in a finite group. Take a square sheet of paper, write "TOP" at the top; then

- rotate 90° counterclockwise ("r"),
- flip about its horizontal axis ("h"),
- rotate 90° clockwise ("r^{-1}"), and
- flip again about the horizontal ("h^{-1}"$(= h)$).

The end result of your flipping represents the element $(*) := h^{-1}r^{-1}hr$ of the symmetry group of the sheet. If this group (the *dihedral group* D_4, with elements $1, r, r^2, r^3, h, hr, hr^2, hr^3$) were abelian, then $(*)$ would equal 1. But "TOP" doesn't reappear at the top, and indeed $(*) = r^2$.

[2]When we say a group is finite or infinite, we are referring to the order of the group, which means its order as a set (i.e. the number of elements).