Things About Groups

Contents

1 Groups

We begin with a completely unmotivated definition.

Def'n 1.1 (Group)**.** A *group* is a set, G, equipped with a binary operation $*$ and a special element $1 \in G$ which satisfy the following properties.

G1. For all $a, b, c \in G$, $(a * b) * c = a * (b * c)$.

G2. For all $a \in G$, $a * 1 = 1 * a = a$.

G3. For each $a \in G$, there is an element $b \in G$ such that $a * b = b * a = 1$.

A group is a kind of *abstract arithmetic*. If you've studied rings or vector spaces before, the basic rules will look familiar. The definition of "group" is a list of axioms, and any particular object which satisfies the axioms is a concrete group. Any theorems we can prove using only the axioms are immediately true in *all* groups. For example, we can show that the special elements in axiom G3 are unique in a precise sense.

Prop'n 1.2. Let G be a group and $a \in G$. Then there is a *unique* element $b \in G$ such that $a * b = b * a = 1$. We refer to this unique element as the *inverse* of a, and denote it by a^{-1}.

Proof. Suppose b and c are elements such that $b * a = a * b = 1$ and $c * a = a * c = 1$. Now

$$b = b * 1 = b * (a * c) = (b * a) * c = 1 * c = c$$

so that $b = c$. □

We can sit around defining abstract arithmetics by writing lists of axioms all day long. But what makes a structure interesting is when it has a **diverse** array of **models** – preferably, models which are themselves known to be interesting. And so, when defining a kind of structure, it is incumbent upon us to also give some useful models. The primary model for groups is sets of *bijective functions*.

Def'n 1.3 (Bijection)**.** Let X be a set. Recall that a mapping $f : X \to X$ is called *bijective* if it is both injective (a.k.a. "one-to-one") and surjective (a.k.a. "onto"). That is,

(i) If $a, b \in X$ such that $f(a) = f(b)$, then $a = b$, and

(ii) If $b \in X$, then there is an $a \in X$ such that $f(a) = b$.

Now the bijective functions $X \to X$ are interesting enough, as we'll see. But (looking ahead) they become *really* interesting if X is not just a set but

has some additional structure of its own – a vector space, a ring, another group, and so on. For example, the bijective structure-preserving maps on a vector space of finite dimension can be represented by invertible matrices.

Prop'n 1.4. Let X be a nonempty set. Then the set

$$\mathsf{Sym}(X) = \{\varphi \mid \varphi \text{ is a bijection } X \to X\}$$

is a group under function composition and the identity map. We refer to $\mathsf{Sym}(X)$ as the *symmetric group* on X.

Symmetric groups are an extremely important family of examples of groups. In fact, it turns out that symmetric groups are essentially *all* of the groups in a very precise sense which we will discuss later. The name "symmetric" is meant to be suggestive of what these mappings are: ways to transform an object so that it looks the same.

Two more useful models of groups are found in modular arithmetic.

Prop'n 1.5. Let n be a positive integer.

(i) The set $\mathbb{Z}/(n)$ is a group under modular addition.

(ii) The set

$$\mathcal{U}_n = \{k \in \mathbb{Z}/(n) \mid \mathsf{gcd}(k, n) = 1\}$$

is a group under modular multiplication.

2 Permutations

A bijective map from a set to itself is called a *permutation*; henceforth the elements of a symmetric group $\mathsf{Sym}(X)$ will be called "permutations". Anytime you hear words like "rearrangement" or "relabeling", there is probably a permutation lurking around. We saw in the last section that the set of all permutations of X is a group under function composition. Now let's get our hands dirty, so to speak, and see some examples of exactly what that means. We can visualize a permutation σ of X using a kind of arrow diagram: we draw all the elements of X (twice) and draw an arrow from a to $\sigma(a)$ for each $a \in X$. Figure 2.1 is an example of such a drawing. In this case we have $X = \{1, 2, 3, 4, 5\}$ with $\sigma(1) = 1$, $\sigma(2) = 3$, $\sigma(3) = 4$, and so on.

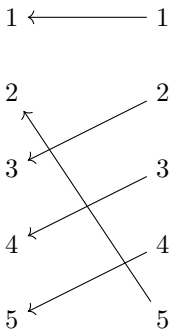

Figure 2.1: A permutation on $\{1, 2, 3, 4, 5\}$.

Viewing permutations this way gives the identity and inverse permutations a nice interpretation. The identity map sends each element "straight across", and to find the inverse of σ simply reverse all the arrows. We can also pronounce the *composition* of functions as "after". So, for instance, if σ and τ are permutations of X, then $\tau \circ \sigma$ is pronounced "tau after sigma" – meaning that to apply this map to a particular element of X, we first apply sigma and then apply tau to the result. Visually, this corresponds to plugging the output of σ to the input of τ as in Figure 2.2.

These arrow diagrams make it easy enough to visualize permutations, but they are a huge pain to compute with. And so, we use an alternative notation instead, called *cycle notation*. Before we introduce cycle notation lets reconsider our arrow diagram in Figure 2.1. There, we wrote down each element of X twice – a bit redundant. We can instead have only one copy of X as in Figure 2.3.

Using this diagram it is less straightforward to see how to compose two permutations (though it can be done, say, by using different colors for the arrows of different permutations). But it is easier to see what this permutation does when we apply it over and over. 2 goes to 3, 3 goes to 4, 4 goes to 5, and 5 goes to 2, while 1 goes to itself. Cycle notation is just a compact way

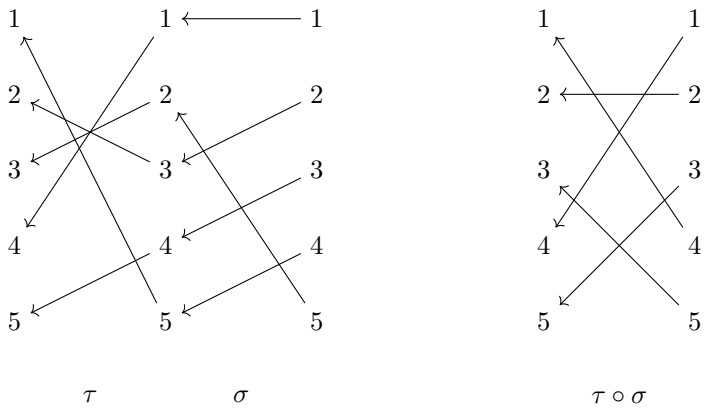

Figure 2.2: Composition of permutations.

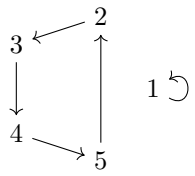

Figure 2.3: A permutation on $\{1, 2, 3, 4, 5\}$.

to express this diagram. For instance, the permutation of Figure 2.3 would be written in cycle notation as

$$(1)(2\ 3\ 4\ 5)$$

or, more compactly, simply as

$$(2\ 3\ 4\ 5).$$

Lists of objects written inside parentheses are called *cycles*.