

## 8 Groups

**Definition 8.1.** A *group* is a set  $G$  together with a binary operation  $*$  :  $G \times G \rightarrow G$  so that

1.  $\exists e \in G$  so that  $e * x = x * e = x$  for all  $x \in G$ .
2. For each  $g \in G$  there is an  $h \in G$  so that  $g * h = h * g = e$ .
3.  $*$  is associative, i.e.,  $(x * y) * z = x * (y * z)$  for all  $x, y, z \in G$ .

The operation  $*$  is usually written as multiplication ( $gh$  instead of  $g * h$ ) and the neutral element is often written  $e = 1$ . However, it doesn't have to be.

Some examples of groups are:

1.  $(G, *) = (\mathbb{Z}, +)$  with  $e = 0$
2.  $(G, *) = (\mathbb{R}_+, \cdot)$  with  $e = 1$
3.  $G = GL_n(\mathbb{R})$  with matrix multiplication and  $e = I_n$
4.  $(G, *) = (S_n, \circ)$

**Proposition 8.2.** 1. (*left cancellation*)  $gx = gy \Rightarrow x = y$ .

2. (*right cancellation*)  $xg = yg \Rightarrow x = y$ .

**Definition 8.3.** The *order*  $o(g)$  of an element  $g \in G$  is the smallest positive integer  $k$  so that  $g^k = e$ .  $o(g) = \infty$  if there is no such number.

I pointed out that, if  $k = o(g)$  then the elements

$$e, g, g^2, \dots, g^{k-1}$$

are all distinct. This implies that, for any  $x \in G$ , the elements

$$x, gx, g^2x, \dots, g^{k-1}x$$

are also distinct. (Otherwise  $g^i x = g^j x$  would imply  $g^i = g^j$  by right cancellation.)

**Theorem 8.4.** If  $G$  is a finite group and  $g \in G$  then  $o(g)$  divides  $|G|$ .

*Proof.* Let  $n = |G|$  and  $k = o(g)$ . Then we will show that the set  $G$  is partitioned into disjoint parts each of size  $k$ . This will show that  $n = pk$  where  $p$  is the number of parts of the partition.

The parts of the partition are sets

$$\{g^i x \mid i \in \mathbb{Z}\}$$

for each  $x \in G$  as we discussed above. We need to show the following.

1. These sets are disjoint (or equal).
2. Their union is all of  $G$ .
3. Each of these sets has exactly  $k$  elements.

We already proved that last statement using right cancellation. (2) is obvious since each  $x$  is contained in the set  $\{g^i x\}$ . To prove (1) suppose that two of these sets overlap:

$$\{g^i x\} \cap \{g^j y\} \neq \emptyset$$

Then they have a common element

$$g^p x = g^q y$$

Multiplying  $g^{-p}$  we get  $x = g^{q-p} y$  so, for any integer  $i$  we have  $g^i x = g^{i+q-p} y$  so  $\{g^i x\} \subseteq \{g^j y\}$ . Similarly,  $\{g^j y\} \subseteq \{g^i x\}$  so the two sets are equal as claimed in (1). Therefore we have a partition of  $G$  into equal parts of size  $k = o(g)$  proving that  $o(g)$  divides  $|G|$ .  $\square$