

# MT310 Homework 2

## Solutions

Due Friday, February 5

**Exercise 1.** Let  $G = \langle a \rangle$  be a finite cyclic group of order  $n$ , with generator  $a$ . Prove that  $a^k$  generates  $G$  if and only if  $\gcd(k, n) = 1$ .

*Proof.* ( $\Rightarrow$ ) Suppose that  $a^k$  generates  $G$ . Then  $a$  is some power of  $a^k$ , so we have  $a = (a^k)^\ell = a^{k\ell}$  for some integer  $\ell$ . This means that  $k\ell \equiv 1 \pmod{n}$ , so that  $[k]_n$  is a unit in  $\mathbb{Z}_n$ . We have proved that this implies that  $\gcd(k, n) = 1$ .

( $\Leftarrow$ ) Suppose that  $\gcd(k, n) = 1$ . Then there are integers  $x, y$  such that  $kx + ny = 1$ . We compute

$$a = a^1 = a^{kx+ny} = (a^k)^x (a^n)^y = (a^k)^x,$$

since  $a^n = 1$ . If  $g \in G$  is an arbitrary element, there is an integer  $i$  such that  $g = a^i$ , and we have

$$g = a^i = (a^k)^{xi} \in \langle a^k \rangle.$$

Hence  $a^k$  generates  $G$ . □

**Exercise 2.** Suppose that  $n = p^k$ , where  $p$  is a prime and  $k$  is a positive integer. Find the number of generators of  $G$ .

*Solution.* From the previous problem,  $a^d$  is *not* a generator of  $G$  iff  $p \mid d$ . The set  $\{d \in \mathbb{Z} : 1 \leq d \leq p^k, p \mid d\} = \{p, 2p, \dots, p^{k-1}p\}$  has  $p^{k-1}$  elements. This is the number of non-generators of  $G$ . Hence  $G$  has  $p^k - p^{k-1} = p^{k-1}(p - 1)$  generators. □

**Exercise 3.** Use Lagrange's theorem to prove that any group of prime order is cyclic.

*Proof.* Let  $G$  be a group whose order is a prime  $p$ . Since  $p > 1$ , there is an element  $a \in G$  such that  $a \neq e$ . The group  $\langle a \rangle$  generated by  $a$  is a subgroup of  $G$ . By Lagrange's theorem, the order of  $\langle a \rangle$  divides  $|G|$ . But the only divisors of  $|G| = p$  are 1 and  $p$ . Since  $a \neq e$  we have  $|\langle a \rangle| > 1$ , so  $|\langle a \rangle| = p$ . Hence  $\langle a \rangle = G$  and  $G$  is cyclic. □

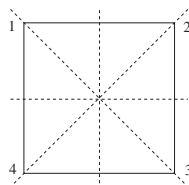
**Exercise 4.** Let  $G$  be a group and let  $a \in G$ . Show that the subset  $C_G(a) = \{b \in G : ba = ab\}$ , consisting of the elements of  $G$  which commute with  $a$ , is a subgroup of  $G$ .

*Proof.* The identity element  $e$  commutes with every element of  $G$ , so  $e \in C_G(a)$ . If  $x \in C_G(a)$  then  $xa = ax$ . Multiplying both sides of this equation on the left by  $x^{-1}$ , we get  $a = x^{-1}ax$ . Multiplying both sides of this new equation on the right by  $x^{-1}$ , we get  $ax^{-1} = x^{-1}a$ . Hence  $x^{-1} \in C_G(a)$ . Let  $x, y \in C_G(a)$ . Then  $x$  and  $y$  both commute with  $a$ , so we have

$$xya = xay = axy,$$

hence  $xy \in C_G(a)$ . Hence  $C_G(a)$  is a subgroup of  $G$ . □

**Exercise 5.** The dihedral group  $D_4$  is the symmetry group of a square. Number the vertices of a square as shown:



Each element of  $D_4$  gives a permutation of the vertices, which is an element of the group  $S_4$ . Let  $H \subset S_4$  be the set of permutations arising from symmetries of the square. Let  $\sigma = (13)(24)$  be the permutation switching  $1 \leftrightarrow 3$  and  $2 \leftrightarrow 4$ . Prove that  $H = C_{S_4}(\sigma)$  (see Exercise 4).

*Proof.* First check that every element of  $D_4$  commutes with the  $180^\circ$  rotation  $\sigma$ . It follows that every permutation coming from  $D_4$  commutes with  $(13)(24)$ . So we have a chain of subgroups

$$D_4 < C_{S_4}(\sigma) < S_4.$$

Since  $|D_4| = 8$  and  $|S_4| = 24$ , Lagrange's theorem implies that  $|C_{S_4}(\sigma)|$  is a number divisible by 8 and dividing 24. The only possible orders are 8, 24, so we have either  $C_{S_4}(\sigma) = D_4$  or  $C_{S_4}(\sigma) = S_4$ . Since there are permutations that do not commute with  $\sigma$ , eg  $(12)$ , it follows that  $C_{S_4}(\sigma) \neq S_4$ , so we must have  $C_{S_4}(\sigma) = D_4$ .  $\square$

**Exercise 6.** Let  $T$  be the group of rigid motions of a regular tetrahedron. Show that  $|T| = 12$  (Hint: imitate the proof of Prop. 4.11 in Judson) and list the orders of all the elements in  $T$ .

*Proof.* Every symmetry sends a face to one of four faces in three possible ways, so  $|T| = 12$ . There are 8 rotations of order three, two for each axis through a vertex and the midpoint of the opposite face. There are 3 rotations of order 2, about axes through pairs of opposite edges. With the identity element of order 1, we have  $8 + 3 + 1 = 12$  elements of  $T$ , which is all of  $T$ , since  $|T| = 12$ .  $\square$