

## MATH 551 HOMEWORK 2

### SOLUTIONS

(1) **The symmetric group**

(a) **Show that the adjacent transpositions  $\{(ii + 1) : 1 \leq i \leq n - 1\}$  generate  $S_n$  (that is, every element of  $S_n$  can be written as a product of finitely many adjacent transpositions).** Since every element of  $S_n$  can be written as the product of cycles, we just need to show that every cycle can be written as the product of adjacent transpositions. We first note that the cycle  $(a_1 a_2 \dots a_k) = (a_1 a_k)(a_1 a_{k-1}) \dots (a_1 a_3)(a_1 a_2)$ , so every cycle can be written as the product of transpositions. Finally, we note that if  $i < j$ , then  $(ij) = (ii + 1)(i + 1i + 2) \dots (j - 2j - 1)(j - 1j)(j - 2j - 1) \dots (ii + 1)$ .

(b) **If  $\sigma \in S_n$  can be written  $\sigma = \tau_1 \tau_2 \tau_3$ , where the  $\tau_i$  are adjacent transpositions, we say this expression for  $\sigma$  has length three. The length of  $\sigma \in S_n$  is the length of the shortest expression for  $\sigma$ . Which element(s) of  $S_n$  has/have the longest length?**

The element with the longest length is the permutation  $\sigma$  that switches 1 and  $n$ , 2 and  $n - 1$ , 3 and  $n - 2$ , and so on. This has length  $\binom{n}{2}$ . To see this, define the *inversion number* of a permutation  $\pi$  to be the number of pairs  $i < j$  with  $\pi(i) > \pi(j)$ . The inversion number of  $\sigma$  is  $\binom{n}{2}$ , and is less than this for all other permutations. We claim that the inversion number is the length of the permutation. Indeed, if  $\pi$  is a permutation with  $\pi(i) > \pi(j)$  for some  $i < j$ , then there is  $i \leq k < k + 1 \leq l$  with  $\pi(k) > \pi(k + 1)$ . Then  $\pi' = \pi(kk + 1)$  has exactly one fewer inversion (as if  $m > k + 1$  with  $\pi(k) > \pi(m)$ , then  $\pi'(k + 1) > \pi'(m)$ , and similarly for  $m < k$ ). Since the only permutation with no inversions is the identity, and the inverse of an adjacent transposition is an adjacent transposition, this shows that the number of inversions is an upper bound on the length of any permutation. Since multiplying by  $(kk + 1)$  can only

remove at most one inversion from a permutation, we see that it is also a lower bound, so we have equality.

(c) **A trivial way to get different expressions for the same element of  $S_n$  is to add  $\tau\tau$  to an expression. For example,  $(12) = (13)(13)(12)$ . If we require that there are no adjacent repeated adjacent transpositions in an expression for  $\sigma$ , is the expression unique?**

(d) **Show that the transposition  $(12)$  and the  $n$ -cycle  $(123 \dots n-1n)$  generate  $S_n$ .** From the first part, it suffices to show that we can generate all adjacent transpositions. Writing  $\sigma = (123 \dots n-1n)$ , the result now follows from the fact that for  $2 \leq i \leq n-1$ , we have  $\sigma^i(12)\sigma^{-i} = (ii+1)$  (which can be proved, for example, by induction).

(2) **Hungerford I.2.15.**

(a) Function composition is associative, and the identity automorphism  $1_G: G \rightarrow G$  defined by  $1_G(g) = g$  for all  $g \in G$  is an identity element. Inverses exist by Theorem 2.3.

(b) If  $f$  is an automorphism of  $\mathbb{Z}$ , it takes  $1$  to  $n \in \mathbb{Z}$ , and thus  $f(m) = nm$ . Since there exists  $m$  with  $f(m) = 1$ , we have  $1 = nm$  for some  $m$ , so  $n = \pm 1$ . Since the function defined by  $f(1) = -1$  is an automorphism, we have  $\text{Aut}(\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$ , via the map that sends the identity to 0, and  $f$  to 1.

For a cyclic group  $\mathbb{Z}/n\mathbb{Z}$ , if  $f$  is an automorphism, then the order of  $f(1)$  must be  $n$ , so  $f(1)$  is coprime to  $n$ . Since any  $a$  with  $(a, n) = 1$  generates  $\mathbb{Z}/n\mathbb{Z}$ , any choice of such  $a$  determines an automorphism. Thus there are two automorphisms of  $\mathbb{Z}/6\mathbb{Z}$ , corresponding to  $a = 1$  and  $a = 5$ , so  $\text{Aut}(\mathbb{Z}/6\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$ . For  $n = 8$ , the choices are  $f_1(1) = 1$ ,  $f_3(1) = 3$ ,  $f_5(1) = 5$ , and  $f_7(1) = 7$ . Since the squares of each of these is  $f_1$ , and  $f_3 \circ f_5 = f_7$ , we have  $\text{Aut}(\mathbb{Z}/8\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ . For  $\mathbb{Z}/p\mathbb{Z}$ , there are  $p-1$  choices for  $a$ , so  $|\text{Aut}(\mathbb{Z}/p\mathbb{Z})| = p-1$ . We defer the proof that it is cyclic until we discuss fields.

(c) As above, there is an automorphism  $f_a$  given by  $f_a(1) = a$  for all  $a$  coprime to  $n$ . Now  $f_a \circ f_b = f_{ab}$ , so the homomorphism  $f_a \mapsto a$  is an isomorphism from  $\text{Aut}(\mathbb{Z}/n\mathbb{Z})$  to the group of invertible elements of  $\mathbb{Z}/n\mathbb{Z}$  under multiplication.

(3) **bf Hungerford I.2.19.**

(a) Let  $H$  be a subgroup of  $G$  that is contained in  $H_i$  for all  $i \in I$ . Then  $H \subseteq \bigcap_{i \in I} H_i$ , so  $\bigcap_{i \in I} H_i$  is the unique greatest

lower bound of the  $H_i$ . By definition the subgroup  $\langle \cup_{i \in I} H_i \rangle$  is the smallest subgroup containing all of the  $H_i$ , so if  $H$  is a subgroup of  $G$  that contains all of the  $H_i$ ,  $\langle \cup_{i \in I} H_i \rangle \subseteq H$ , so  $\langle \cup_{i \in I} H_i \rangle$  is the unique lowest upper bound. Thus the partially ordered set of subsets of  $G$ , ordered by inclusion, is a lattice.

(b) I've been having trouble with the pictures. Ask me if you'd like to see a copy.

(4) **Hungerford I.3.3.** Consider the element  $ab \in G$ . Suppose  $(ab)^r = a^r b^r = e$ , with  $r \not\equiv 0 \pmod{p}$ , or  $r \not\equiv 0 \pmod{q}$ . Then there are  $i, j$  not both zero with  $0 \leq i < p$ ,  $0 \leq j < q$  with  $a^i b^j = e$ , so  $a^i = b^{q-j}$ . However the order of  $a^i$  must divide  $p$ , while the order of  $b^{q-j}$  must divide  $q$ , so since  $(p, q) = 1$  they are coprime and thus  $i = 0 = j$ , and so if  $(ab)^r = e$ , we must have  $r \equiv 0 \pmod{p}$  and  $r \equiv 0 \pmod{q}$ , so  $r \equiv 0 \pmod{pq}$ . Thus the order of  $ab$  is  $pq$ , so  $ab$  generates  $G$ .

(5) **Hungerford I.1.7** If  $0 < a < p$ , then  $(a, p) = 1$ , so there are  $r, s \in \mathbb{Z}$  with  $ar - sp = 1$ . We may assume that  $s < a, r < p$ . Thus  $ar \equiv 1 \pmod{p}$ , so every nonzero element of  $\mathbb{Z}/p\mathbb{Z}$  has a multiplicative inverse. The element 1 is clearly a multiplicative identity, and multiplication is associative because multiplication in  $\mathbb{Z}$  is, so the  $p - 1$  nonzero elements of  $\mathbb{Z}/p\mathbb{Z}$  form a group under multiplication. If  $p$  is not prime, some elements will fail to have an inverse. For example, if  $p = 6$ , the element 1 is still the only candidate for a multiplicative identity. However there is no  $a$  with  $2a \equiv 1 \pmod{6}$ .

**Hungerford I.4.4** By the previous part we know that the nonzero elements of  $\mathbb{Z}/p\mathbb{Z}$  form a group under multiplication of order  $p - 1$ . Thus the order of any element  $0 < a < p$  divides  $p - 1$ , so  $a^{p-1} \equiv 1 \pmod{p}$ . Multiplying both sides by  $a$ , we get  $a^p \equiv a \pmod{p}$ .

(6) **Hungerford I.5.10.** Let  $H$  be the subgroup generated by  $\sigma^2$  and  $\tau$ , so  $H = \{1, \sigma^2, \tau, \sigma^2\tau\}$ . Note that  $H \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ . Since  $H$  is index two it is normal. Let  $K$  be the subgroup  $\{1, \tau\}$  of  $H$ . Since  $K$  is a subgroup of the abelian group  $H$ , it is normal in  $H$ . However  $\sigma\tau\sigma^{-1} = \sigma^2\tau \notin K$ , so  $K$  is not a normal subgroup of  $G$ .

(7) **Hungerford I.5.15.** Since  $N \vee K = G$ , and  $N$  and  $K$  are normal in  $G$ , we have  $G = N \vee K = NK$ , by Theorem 5.3, so  $G/N = NK/N \cong K/(N \cap K)$  by the second isomorphism theorem. Since  $N \cap K = e$ ,  $K/(N \cap K) \cong K$  as required.

- (8) **Show that if  $H$  and  $K$  are subgroups of a group  $G$ , then every element of  $H \vee K$  can be written in the form  $h_1 k_1 h_2 k_2 \dots h_r k_r$  for some  $h_i \in H, k_i \in K$ .** Let  $P = \{h_1 k_1 \dots h_r k_r : r \in \mathbb{N}, h_i \in H, k_i \in K\}$ . Then  $H, K \subseteq P$ , and  $e = ee \in P$ . If  $a = h_1 k_1 \dots h_r k_r \in P$ , then  $a^{-1} = e k_r^{-1} h_r^{-1} \dots k_1^{-1} h_1^{-1} e \in P$ . The multiplication of elements of  $P$  lies in  $P$ , so we see that  $P$  is a subgroup of  $G$  containing  $H$  and  $K$ . Thus  $H \vee K \subseteq P$ , so each element of  $H \vee K$  can be written in the desired form. (Actually  $H \vee K = P$  !)