

# Dummit & Foote Ch. 3.2: More on Cosets and Lagrange's Theorem

Scott Donaldson

Oct. 2023

Let  $G$  be a group.

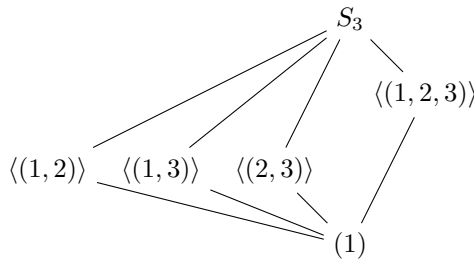
## 1. (10/1/23)

Which of the following are permissible orders of subgroups of a group of order 120: 1, 2, 5, 7, 9, 15, 60, 240? For each permissible order give the corresponding index.

*Proof.* From Lagrange's theorem, the order of a subgroup of a group of order 120 must divide 120. Then the permissible orders for subgroups are  $1 = \frac{120}{120}$ ,  $2 = \frac{120}{60}$ ,  $5 = \frac{120}{24}$ ,  $15 = \frac{120}{8}$ , and  $60 = \frac{120}{2}$ . For each of these orders the index is given by the corresponding denominator.  $\square$

## 2. (10/2/23)

Prove that the lattice of subgroups of  $S_3$  below is correct (i.e., prove that it contains all subgroups of  $S_3$  and that their pairwise joins and intersections are correctly drawn).



*Proof.* The symmetric group  $S_3$  contains 6 elements. By Lagrange's theorem, its proper subgroups must have order 2 or 3. Each of the subgroups in the lattice above have order 2 or 3, so there are no smaller or larger subgroups not depicted above.

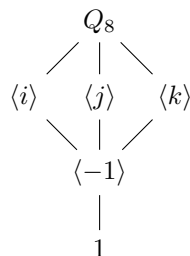
From Corollary 10, a subgroup of order 2 must be isomorphic to  $Z_2$ , that is, cyclic and generated by a single element of order 2. The three subgroups generated by the three elements of order 2 (the 2-cycles of  $S_3$ ) are depicted above. Similarly, a subgroup of order 3 must be isomorphic to  $Z_3$  and generated by a single element of order 3. The subgroup generated by  $(1, 2, 3)$  contains  $(1, 3, 2)$ , so there is only a single subgroup of order 3.

Next, again by Lagrange's Theorem, a subgroup of two different containing groups must have an order that divides the order of both of the containing groups. First consider a subgroup of order 2 and a subgroup of order 3. Only 1 divides 2 and 3, so the intersection must be the identity. Similarly, if a subgroup of order 2 and a subgroup of order 3 are contained in a larger group, then that group's order must have both 2 and 3 as divisors. The smallest integer for which this is possible is 6, which is the order of all of  $S_3$ .

Finally, consider a pair of subgroups of order 2. Their intersection is either the identity or else they are the same subgroup. Their join must have even order, but 4 does not divide 6 and any larger even number exceeds the order of  $S_3$ . Thus their join is all of  $S_3$ . This concludes the proof that the lattice of subgroups of  $S_3$  is correct.  $\square$

### 3. (10/2/23)

Prove that the lattice of subgroups of  $Q_8$  below is correct.



*Proof.* The group  $Q_8$  has order  $8 = 2^3$ , so by Lagrange's theorem its proper subgroups must have order 2 or 4. We will start from the bottom and work toward the top: There is only one element of order 2 in  $Q_8$ ,  $-1$ , and the cyclic subgroup generated by it is in the lattice.

For each of  $i, j$ , and  $k$ ,  $\langle -1 \rangle$  is contained in the subgroup generated by them (ex.  $\langle i \rangle = \{\pm 1, \pm i\}$ ) and there are no intermediate subgroups, since there is no divisor of 4 that is strictly greater than 2. At this point, every element of  $Q_8$  is represented, so there are no cyclic subgroups missing. We might ask if there is a subgroup of order 4 missing. If so, it cannot be cyclic, and from Ch. 1.1, Exercise 36, it must be isomorphic to  $V_4$ . However,  $V_4$  contains three elements of order 2, and  $Q_8$  only has one, so there is no subgroup of  $Q_8$  isomorphic to  $V_4$ .

Finally, the join of any of the subgroups generated by  $i, j$ , or  $k$  must contain strictly more than 4 elements and its order must divide 8. Then any of their joins must have order 8, that is, be all of  $Q_8$ .  $\square$

#### 4. (10/3/23)

Show that if  $|G| = pq$  for some primes  $p$  and  $q$  (not necessarily distinct) then either  $G$  is abelian or  $Z(G) = 1$ .

*Proof.* We will show, equivalently, that if  $|Z(G)| > 1$ , then  $G$  is abelian.

Let  $x \in Z(G)$ . From Corollary 9, the order of  $x$  divides  $|G| = pq$ . If  $|x| = pq$ , then  $G = \langle x \rangle$  and so is abelian. Suppose without loss of generality that  $|x| = p$ . Now since the center of a group is a subgroup, we must have  $\langle x \rangle \leq Z(G)$ . If there exists a  $y \in Z(G), y \notin \langle x \rangle$ , then the order of  $Z(G)$  exceeds  $p$  and must divide  $pq$ , then it must be all of  $G$  and hence  $G$  is abelian. So suppose  $Z(G) = \langle x \rangle$ .

The center of a group is normal in that group, so  $G/Z(G)$  is well-defined. Since  $|Z(G)| = p$ , it has  $q$  cosets in  $G$ ; that is, the quotient group  $G/Z(G)$  has prime order  $q$  and is thus isomorphic to  $Z_q$ , hence cyclic. From Ch. 3.1, Exercise 36.,  $G$  is thus abelian.  $\square$

#### 5. (10/4/23)

Let  $H$  be a subgroup of  $G$  and fix some element  $g \in G$ .

- (a) Prove that  $gHg^{-1}$  is a subgroup of  $G$  of the same order as  $H$ .

*Proof.* By definition elements of  $gHg^{-1}$  can be written in the form  $ghg^{-1}$  for some  $h \in H$ , so let  $gh_1g^{-1}, gh_2g^{-1} \in gHg^{-1}$ . Then we have:

$$(gh_1g^{-1})(gh_2g^{-1})^{-1} = gh_1g^{-1}gh_2^{-1}g = gh_1h_2^{-1}g^{-1} \in gHg^{-1},$$

so  $gHg^{-1}$  fulfills the subgroup criterion and is thus a subgroup of  $G$ .

Next, let  $\varphi_g : H \rightarrow gHg^{-1}$  be defined by  $\varphi_g(h) = ghg^{-1}$  for all  $h \in H$ . This map is injective by the cancellation laws:  $gh_1g^{-1} = gh_2g^{-1}$  implies that  $h_1 = h_2$ . It is also surjective: Let  $x \in gHg^{-1}$ . By definition  $x = ghg^{-1}$  for some  $h \in H$ , so  $\varphi_g(h) = x$ . Therefore  $\varphi_g$  is a bijection, and so  $H$  and  $gHg^{-1}$  have the same order.  $\square$

- (b) Deduce that if  $n \in \mathbb{Z}^+$  and  $H$  is the unique subgroup of  $G$  of order  $n$  then  $H \trianglelefteq G$ .

Suppose that  $H$  is the unique subgroup of order  $n$  in  $G$ . Then for all  $g \in G$ , we must have  $gHg^{-1} = H$  (it cannot be any other subgroup, because  $|gHg^{-1}| = |H| = n$  and there is no other subgroup of order  $n$  in  $G$ ). It follows that  $H$  is normal in  $G$ .

## 6. (10/4/23)

Let  $H \leq G$  and let  $g \in G$ . Prove that if the right coset of  $Hg$  equals *some* left coset of  $H$  in  $G$  then it equals the left coset  $gH$  and  $g$  must be in  $N_G(H)$ .

*Proof.* Suppose  $Hg = xH$  for some  $x \in G$ . Now  $g \in Hg$ , so we must also have  $g \in xH$ . Then  $g = xh$  for some  $h \in H$ . It follows that  $x = gh^{-1}$ . So  $Hg = xH = (gh^{-1})H = gH$ , which in turns implies that  $gHg^{-1} = H$ . Therefore  $g \in N_G(H)$ .  $\square$

## 7. (10/5/23)

Let  $H \leq G$  and define a relation  $\sim$  on  $G$  by  $a \sim b$  if and only if  $b^{-1}a \in H$ . Prove that  $\sim$  is an equivalence relation and describe the equivalence class of each  $a \in G$ . Use this to prove Proposition 4.

*Proof.* Let  $a, b, c \in G$ . We have  $a \sim a$ , because  $a^{-1}a = 1 \in H$ . If  $a \sim b$ , then we have  $b^{-1}a \in H$ . Now  $b \sim a = a^{-1}b = (b^{-1}a)^{-1} \in H$ , since  $H$  is closed under inverses, so  $a \sim b$  implies that  $b \sim a$  (and the logic holds in reverse). Finally, if  $a \sim b$  and  $b \sim c$ , then  $b^{-1}a, c^{-1}b \in H$ . Then their product,  $c^{-1}bb^{-1}a = c^{-1}a$ , is an element of  $H$ , which implies  $a \sim c$ . The relation  $\sim$  is reflexive, symmetric, and transitive, therefore it is an equivalence relation.

Let  $a \in G$  and let  $b$  lie in the left coset  $aH$ , so  $b = ah$  for some  $h \in H$ . Then  $b^{-1}a = (ah)^{-1}a = h^{-1}a^{-1}a = h^{-1} \in H$ , so  $a \sim b$ . This implies that  $aH$  is a subset of the equivalence class of  $a$ . And, if we have  $a \sim b$ , then  $b^{-1}a \in H$ , so  $b^{-1}a = h$  for some  $h \in H$ . It follows that  $b = ah^{-1} \in aH$ , so the equivalence class of  $a$  is a subset of  $aH$ . Since each is contained in the other, the equivalence class of  $a$  under  $\sim$  is the left coset  $aH$ .

Now Proposition 4 states that:

- The set of left cosets of  $H$  in  $G$  form a partition of  $G$ .
- For all  $a, b \in G$ ,  $aH = bH$  if and only if  $b^{-1}a \in H$ .
- In particular,  $aH = bH$  if and only if  $a$  and  $b$  are representatives of the same coset.

Since the equivalence class of  $a$  under  $\sim$  is exactly the left coset  $aH$  and equivalence classes partition a set, the left cosets of  $H$  in  $G$  partition  $G$ . The proof for the remaining items follows directly from the proof above that  $a \sim b \iff b^{-1}a \in H \iff b \in aH$ .  $\square$

## 8. (10/6/23)

Prove that if  $H$  and  $K$  are finite subgroups of  $G$  whose orders are relatively prime then  $H \cap K = 1$ .

*Proof.* Let  $H, K \leq G$  be finite subgroups whose orders are relatively prime. Let  $x \in H \cap K$ , so  $x \in H$  and  $x \in K$ . From Corollary 9, the order of  $x$  divides the orders of both  $H$  and  $K$ . Since  $|H|$  and  $|K|$  are relatively prime, the order of  $x$  must be 1, therefore  $x = 1$ . It follows that  $H \cap K = 1$ .  $\square$

## 9. (10/12/23)

This exercise outlines a proof of Cauchy's Theorem due to James McKay (*Another proof of Cauchy's group theorem*, Amer. Math. Monthly, 66(1959), p. 119). Let  $G$  be a finite group and let  $p$  be a prime dividing  $|G|$ . Let  $\mathcal{S}$  denote the set of  $p$ -tuples of elements of  $G$  the product of whose coordinates is 1:

$$\mathcal{S} = \{(x_1, x_2, \dots, x_p) \mid x_1 x_2 \dots x_p = 1\}.$$

- (a) Show that  $\mathcal{S}$  has  $|G|^{p-1}$  elements, hence has order divisible by  $p$ .

*Proof.* Construct an element of  $\mathcal{S}$  coordinate by coordinate. There are  $|G|$  choices for the first element  $x_1$ . There are again  $|G|$  choices for the second element  $x_2$ . We proceed similarly until the final element, which must satisfy the constraint that the product of all coordinates is 1. Therefore the final element must be equal to  $(x_1 x_2 \dots x_{p-1})^{-1}$ . We have freely chosen  $p-1$  coordinates from among  $|G|$  possibilities; therefore  $|\mathcal{S}| = |G|^{p-1}$ .  $\square$

Define the relation  $\sim$  on  $\mathcal{S}$  by letting  $\alpha \sim \beta$  if  $\beta$  is a cyclic permutation of  $\alpha$ .

- (b) Show that a cyclic permutation of  $\mathcal{S}$  is again an element of  $\mathcal{S}$ .

*Proof.* Since  $\alpha \sim \beta$  implies that  $\beta$  is a cyclic permutation of  $\alpha$ , we have

$$\alpha = (x_1, x_2, \dots, x_p) \Rightarrow \beta = (x_{1+n}, x_{2+n}, \dots, x_{p+n}),$$

where the subscripts of elements of  $\beta$  are taken mod  $p$  (although wrapping from 1 to  $p$ , rather than 0 to  $p-1$ ).

The product of the coordinates of  $\alpha$  is:

$$\begin{aligned} 1 &= \prod \alpha = x_1 x_2 \dots x_p \\ &= (x_1 \dots x_n)(x_{n+1} \dots x_p) \\ &= (x_{n+1} \dots x_p)(x_1 \dots x_n) \text{ (if } ab = 1, \text{ then } ab = ba) \\ &= (x_{1+n} \dots x_{p-n+n})(x_{(p-n+1)+n} \dots x_{p+n}) \\ &= x_{1+n} \dots x_{p+n} = \prod \beta, \end{aligned}$$

and so the product of  $\beta$ 's coordinates is 1, making it an element of  $\mathcal{S}$ .  $\square$

- (c) Prove that  $\sim$  is an equivalence relation on  $\mathcal{S}$ .

*Proof.* Let  $\alpha, \beta, \gamma \in \mathcal{S}$ . The relation  $\sim$  is:

- Reflexive: Let  $\alpha = (x_1, x_2, \dots, x_p)$ . Then  $x_i = x_{i+0}$  for all coordinates  $x_i$ , so  $\alpha$  is a cyclic permutation of itself, and therefore  $\alpha \sim \alpha$ .
- Symmetric: Let  $\alpha \sim \beta$ ,  $\alpha, \beta$  indexed by  $x, y$  respectively. Since  $\beta$  is a cyclic permutation of  $\alpha$ , we have  $y_i = x_{i+n}$  for all  $i \in \{1, \dots, p\}$  for some  $n \in \mathbb{Z}$ . It follows that  $x_i = y_{i+(p-n)}$  (subscripts mod  $p$  wrapping from 1 to  $p$ ), so  $\alpha$  is also a cyclic permutation of  $\beta$ , and therefore  $\beta \sim \alpha$ .
- Transitive: Let  $\alpha \sim \beta$  and  $\beta \sim \gamma$ , with  $\alpha, \beta$  as above and  $\gamma$  indexed by  $z$ . We have  $y_i = x_{i+n}$  and  $z_i = y_{i+k}$  for some  $k, n \in \mathbb{Z}$ . It follows that  $z_i = x_{i+k+n}$ , which implies that  $\gamma$  is a cyclic permutation of  $\alpha$ , so  $\alpha \sim \gamma$ .

Therefore  $\sim$  is an equivalence relation on  $\mathcal{S}$ .  $\square$

- (d) Prove that an equivalence class contains a single element if and only if it is of the form  $(x, x, \dots, x)$  with  $x^p = 1$ .

*Proof.* First, let  $\alpha = (x, \dots, x)$  and let  $\alpha \sim \beta$ . Then  $\beta$  is a cyclic permutation of  $\alpha$ . Since  $\alpha$  consists of a single, repeated coordinate value, we must have  $\beta = (x, \dots, x) = \alpha$ . Therefore the equivalence class of  $\alpha$  consists only of itself.

Next, let  $\alpha \in \mathcal{S}$  and suppose that the equivalence class of  $\alpha$  under  $\sim$  consists only of  $\alpha$ . Suppose  $\alpha = (x_1, x_2, \dots, x_p)$ . Let  $\beta$  be a cyclic permutation of  $\alpha$  shifted by 1:  $\beta = (x_2, x_3, \dots, x_p, x_1)$ . Now  $\beta$  is in the equivalence class of  $\alpha$ , but we must have  $\beta = \alpha$ , so  $x_{i+1} = x_i$  for all  $x_i$ . It follows that  $x_2 = x_1, x_3 = x_2 = x_1$ , and so every value is equal to  $x_1$ . Then we have  $\alpha = (x_1, \dots, x_1)$ , which is of the form  $(x, \dots, x)$ , and by definition we must have  $x^p = 1$ .  $\square$

- (e) Prove that every equivalence class has order 1 or  $p$  (this uses the fact that  $p$  is a *prime*). Deduce that  $|G|^{p-1} = k + pd$ , where  $k$  is the number of classes of size 1 and  $d$  is the number of classes of size  $p$ .

*Proof.* From (d), if  $\alpha = (x, \dots, x)$  for some  $x \in G$ , its equivalence class has order 1.

Let  $\alpha = (x_1, x_2, \dots, x_p)$ . Then there are exactly  $p$  members in the equivalence class of  $\alpha$ , and they are the cyclic permutations of  $\alpha$  shifted by  $0, 1, 2, \dots, p-1$ , respectively. For example, the  $n$ -th member of the equivalence class is  $(x_{1+n}, x_{2+n}, \dots, x_{p+n})$ .

The equivalence classes of the elements of  $\mathcal{S}$  partition  $\mathcal{S}$ . Suppose there are  $k$  equivalence classes of order 1, and  $d$  equivalence classes of order  $p$ . From (a), the order of  $\mathcal{S}$  is  $|G|^{p-1}$ . Then we have  $|G|^{p-1} = k + pd$ .  $\square$

- (f) Since  $\{(1, 1, \dots, 1)\}$  is an equivalence class of size 1, conclude from (e) that there must be a nonidentity element  $x$  in  $G$  with  $x^p = 1$ , i.e.,  $G$  contains an element of order  $p$ .

*Proof.* From (e), we have  $|G|^{p-1} = k + pd$  for some  $k, d \geq 0$ . From (a),  $p$  divides the order of  $\mathcal{S} = |G|^{p-1}$ , so we can write  $ps = k + pd$  for some  $s > 0$ . Then  $k = ps - pd = p(s - d)$ , and so  $p$  divides  $k$ . Because  $p$  is prime, this implies that  $k > 1$ , so there are at least two elements whose equivalence classes have size 1. We already know that one is the identity; therefore there must be some element  $\alpha \in \mathcal{S}, \alpha \neq (1, \dots, 1)$  whose equivalence class under  $\sim$  has size 1. From (d),  $\alpha = (x, \dots, x)$  for some  $x \in G$ , and we thus have  $x^p = 1$ , which implies that  $|x| = p$ .  $\square$

## 12. (10/16/23)

Let  $H \leq G$ . Prove that the map  $x \mapsto x^{-1}$  sends each left coset of  $H$  in  $G$  onto a right coset of  $H$  and gives a bijection between the set of left cosets and the set of right cosets of  $H$  in  $G$  (hence the number of left cosets of  $H$  in  $G$  equals the number of right cosets).

*Proof.* Let  $\varphi : G \rightarrow G$  be defined by  $\varphi(x) = x^{-1}$  for all  $x \in G$ . Consider:

$$\varphi(xH) = \{\varphi(xh) \mid h \in H\} = \{(xh)^{-1} \mid h \in H\} = \{h^{-1}x^{-1} \mid h \in H\} = Hx^{-1},$$

so  $\varphi$  maps left cosets of  $H$  onto right cosets of  $H$ .

Further, considering  $\varphi$  as a map from left cosets of  $H$  to right cosets of  $H$ , it is a bijection.

Toward injectivity, suppose that  $\varphi(xH) = \varphi(yH)$  for some  $x, y \in G$ , and let  $z \in xH$ . Then  $\varphi(z) = z^{-1} = hy^{-1}$ , because  $z \in xH$  and  $\varphi(xH) = \varphi(yH)$ . Inverting both sides, we obtain  $z = (hy^{-1})^{-1} = yh^{-1} \in yH$ , and so  $xH \subseteq yH$ . The same logic shows that  $yH \subseteq xH$ , so we must have  $xH = yH$ , and therefore  $\varphi$  is injective.

It is also surjective: Letting  $Hx$  be a right coset of  $H$ , by definition we have  $\varphi(x^{-1}H) = Hx$ . It is therefore a bijection, and so there are an equal number of left cosets and right cosets of  $H$  in  $G$ .  $\square$

## 13. (10/16/23)

Fix any labelling of the vertices of a square and use this to identify  $D_8$  as a subgroup of  $S_4$ . Prove that the elements of  $D_8$  and  $\langle(1, 2, 3)\rangle$  do not commute in  $S_4$ .

*Proof.* Label the vertices of a square starting at the upper-left corner and going clockwise 1, 2, 3, 4. We can assign to the generators  $r, s$  of  $D_8$  the permutations  $(1, 2, 3, 4), (2, 4) \in S_4$ , respectively.

To show that the elements of  $D_8$  and  $\langle(1, 2, 3)\rangle$  do not commute, we note that:

$$(1, 2, 3) \cdot s = (1, 2, 3)(2, 4) = (1, 2, 4, 3), \text{ and} \\ s \cdot (1, 2, 3) = (2, 4)(1, 2, 3) = (1, 4, 2, 3),$$

so  $s$  does not commute with  $(1, 2, 3) \in S_4$ . Therefore  $D_8$  and  $\langle(1, 2, 3)\rangle$  are not commuting subgroups of  $S_4$ .  $\square$

## 14. (10/17/23)

Prove that  $S_4$  does not have a normal subgroup of order 8 or a normal subgroup of order 3.

*Proof.* From Corollary 10, a subgroup of order 3 is isomorphic to  $Z_3$ , hence cyclic. So, without loss of generality, consider  $\langle(1, 2, 3)\rangle \leq S_4$ . Consider the conjugate of  $(1, 2, 3)$  by  $(1, 2)(3, 4)$ :

$$(1, 2)(3, 4) \cdot (1, 2, 3) \cdot (1, 2)(3, 4) = (1, 4, 2),$$

which is not an element of  $\langle(1, 2, 3)\rangle$ . Therefore there is an element of  $S_4$  that does not normalize  $\langle(1, 2, 3)\rangle$  and, by isomorphism, any subgroup of order 3, so  $S_4$  does not contain any normal subgroups of order 3.

Next, let  $X \leq S_4$  with  $|X| = 8$  and suppose that  $X \trianglelefteq S_4$ . From Cauchy's Theorem,  $X$  contains an element of order 2, which may be either a single 2-cycle or a pair of disjoint 2-cycles. We will consider each case individually:

- Without loss of generality, suppose that  $(1, 2) \in X$ . Because  $X$  is normal in  $S_4$ , the conjugate element  $(1, 2, 3) \cdot (1, 2) \cdot (1, 3, 2) = (2, 3)$  must lie in  $X$ . Because  $X$  is closed, the product  $(1, 2) \cdot (2, 3) = (1, 2, 3)$  must lie in  $X$ , a contradiction since (from Corollary 9) a subgroup of order 8 contains no elements of order 3. Thus  $X$  is not normal in  $S_4$ .
- Similarly, suppose that  $(1, 2)(3, 4) \in X$ . Again, the conjugate  $(1, 2, 3) \cdot (1, 2)(3, 4) \cdot (1, 3, 2) = (1, 4, 3, 2)$  must lie in  $X$ . So the product  $(1, 2)(3, 4) \cdot (1, 4, 3, 2) = (1, 3)$  must lie in  $X$ . Then, since  $X$  contains a 2-cycle, it must contain an element of order 3, a contradiction. Thus  $X$  is again not normal in  $S_4$ .

This concludes the proof that  $S_4$  contains no normal subgroups of order 8 or order 3.  $\square$

## 15. (10/19/23)

Let  $G = S_n$  and for fixed  $i \in \{1, 2, \dots, n\}$  let  $G_i$  be the stabilizer of  $i$ . Prove that  $G \cong S_{n-1}$ .



*Proof.* From Ch. 2.2, Exercise 8., we have defined a bijection  $\varphi : G_i \rightarrow S_{n-1}$  defined on a permutation  $\sigma \in G_i$  and an element  $m \in \{1, 2, \dots, n\}$  it permutes:

$$\varphi(\sigma)(m) = \begin{cases} \sigma(m) & \text{if } \sigma(m) \leq i \\ \sigma(m) - 1 & \text{if } \sigma(m) > i \end{cases}.$$

For  $\sigma_1, \sigma_2 \in G_i$  and  $m \in \{1, \dots, n\}$ , let  $\sigma_2(m) = k$  and  $\sigma_1(k) = p$ . Let us consider the different cases for  $k$  and  $p$ .

1.  $k \leq i, p \leq i$ . Then:

$$\begin{aligned} (\sigma_1 \circ \sigma_2)(m) &= \sigma_1(\sigma_2(m)) = \sigma_1(k) = p \leq i, \text{ which implies that} \\ \varphi(\sigma_1 \circ \sigma_2)(m) &= (\sigma_1 \circ \sigma_2)(m) = p. \end{aligned}$$

Also:

$$\begin{aligned} \sigma_2(m) = k \leq i &\Rightarrow \varphi(\sigma_2(m)) = \sigma_2(m) = k, \text{ and} \\ \sigma_1(k) = p \leq i &\Rightarrow \varphi(\sigma_1(k)) = \sigma_1(k) = p, \text{ so} \\ (\varphi(\sigma_1) \circ \varphi(\sigma_2))(m) &= \varphi(\sigma_1)(\varphi(\sigma_2)(m)) \\ &= \varphi(\sigma_1)(\sigma_2(m)) \\ &= \varphi(\sigma_1)(k) = \sigma_1(k) = p, \end{aligned}$$

thus  $\varphi(\sigma_1 \circ \sigma_2) = \varphi(\sigma_1) \circ \varphi(\sigma_2)$ .

2.  $k > i, p \leq i$ . As above, we have  $(\sigma_1 \circ \sigma_2)(m) = p \leq i$ , which implies that  $\varphi(\sigma_1 \circ \sigma_2)(m) = p$ . Also:

$$\sigma_2(m) = k > i \Rightarrow \varphi(\sigma_2)(m) = \sigma_2(m) - 1 = k - 1.$$

Now note that, in the permutation  $\varphi(\sigma_1)$ , all values greater than or equal to  $i$  have been decremented by 1, so we have  $\varphi(\sigma_1)(k - 1) = \sigma_1(k) = p$ . It follows that:

$$\begin{aligned} (\varphi(\sigma_1) \circ \varphi(\sigma_2))(m) &= \varphi(\sigma_1)(\varphi(\sigma_2)(m)) \\ &= \varphi(\sigma_1)(k - 1) \\ &= \sigma_1(k) = p, \end{aligned}$$

thus  $\varphi(\sigma_1 \circ \sigma_2) = \varphi(\sigma_1) \circ \varphi(\sigma_2)$ .

3.  $k \leq i, p > i$ . Then  $(\sigma_1 \circ \sigma_2)(m) = p > i$ , which implies that  $\varphi(\sigma_1 \circ \sigma_2)(m) = (\sigma_1 \circ \sigma_2)(m) = p - 1$ . As in the first case,  $\varphi(\sigma_2)(m) = \sigma_2(m) = k$ . So:

$$\begin{aligned} (\varphi(\sigma_1) \circ \varphi(\sigma_2))(m) &= \varphi(\sigma_1)(\varphi(\sigma_2)(m)) \\ &= \varphi(\sigma_1)(k) \\ &= \sigma_1(k) - 1 = p - 1, \end{aligned}$$

thus  $\varphi(\sigma_1 \circ \sigma_2) = \varphi(\sigma_1) \circ \varphi(\sigma_2)$ .

4.  $k > i, p > i$ . As above, we have  $\varphi(\sigma_1 \circ \sigma_2)(m) = p - 1$ . As in the second case, we have  $\varphi(\sigma_2)(m) = k - 1$ ; however,  $\sigma_1(k) = p > i$ , so  $\varphi(\sigma_1(k - 1)) = \sigma_1(k) - 1 = p - 1$ . Then:

$$\begin{aligned} (\varphi(\sigma_1) \circ \varphi(\sigma_2))(m) &= \varphi(\sigma_1)(\varphi(\sigma_2)(m)) \\ &= \varphi(\sigma_1)(k - 1) \\ &= \sigma_1(k - 1) - 1 = p - 1, \end{aligned}$$

thus  $\varphi(\sigma_1 \circ \sigma_2) = \varphi(\sigma_1) \circ \varphi(\sigma_2)$ .

This exhaustively shows that for all  $\sigma_1, \sigma_2 \in G_i$ , the equation  $\varphi(\sigma_1 \circ \sigma_2) = \varphi(\sigma_1) \circ \varphi(\sigma_2)$  holds in  $S_{n-1}$ . Thus  $\varphi$  is an isomorphism, and so  $G_i \cong S_{n-1}$ .  $\square$

## 16. (10/19/23)

Use Lagrange's Theorem in the multiplicative group  $(\mathbb{Z}/p\mathbb{Z})^\times$  to prove *Fermat's Little Theorem*: if  $p$  is a prime then  $a^p \equiv a \pmod{p}$  for all  $a \in \mathbb{Z}$ .

*Proof.* Recall that the order of the multiplicative group  $(\mathbb{Z}/p\mathbb{Z})^\times$  is equal to the number of positive integers  $n$  for which  $n < p$  and  $n$  is relatively prime to  $p$ . Since  $p$  is prime, this is  $p - 1$ .

For any  $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$ , the order of  $\bar{a}$  must divide  $p - 1$ , and in particular, we have  $\bar{a}^{p-1} = 1$ . It follows that  $\bar{a}^p = \bar{a}$ . If  $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$  is a representative of some  $a \in \mathbb{Z}$ , we then conclude that  $a^p \equiv a \pmod{p}$ .  $\square$