

# Math 122, Solution Set No. 2

As a general note, all elements of  $S_n$  will be written in disjoint cycle notation unless otherwise specified. Also, as a notational convention,  $H \leq G$  means  $H$  is a subgroup of  $G$ .

## 1 2.3.14

(a) Note that, if  $\varphi : \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$  is an automorphism,  $\varphi$  is completely determined by  $\varphi(1)$ . This is because, if  $n \geq 0 \in \mathbb{Z}$ ,  $\varphi(n) = \varphi(1) + \dots + \varphi(1)$  ( $n$  times) and  $\varphi(-n) = -\varphi(n)$ . Thus, for arbitrary  $n \in \mathbb{Z}$ ,  $\varphi(n) = n\varphi(1)$ .

In particular, this implies  $\text{Im } \varphi = \varphi(1)\mathbb{Z}$ . Note  $m\mathbb{Z} = \mathbb{Z}$  iff  $m = 1$  or  $-1$ . Thus  $\varphi(1) = -1$  or  $1$ , and the group of automorphisms is  $C_2$ , the only group of order 2.

(b) An automorphism on a cyclic group  $G = \langle a \rangle$  is completely determined by its action on a generator  $a$  (this is by the same reasoning as in a). If  $\varphi(a) = b$ , where  $b$  is not a generator of the cyclic group, then  $\text{Im } \varphi = \langle b \rangle \neq G$ . If  $\varphi(a) = c$ , where  $c$  is a generator, then  $\text{Im } \varphi = \langle c \rangle = G$ . The fact that this map is a homomorphism is problem 2.4.5.

In this particular situation, we note that all cyclic groups of finite order 10 are isomorphic, so it suffices to examine the case  $G = \mathbb{Z}/10$ . It is an easy check to see that  $1, 3, 7, 9 \in \mathbb{Z}/10$  are the only generators. In general, the generators for a  $\mathbb{Z}/n$  are those integers viewed modulo  $n$  that are relatively prime to  $n$ . Let 1 be a generator for  $\mathbb{Z}/10$ . We can define  $\varphi(1) = 1, 3, 7$  or  $9$ . Thus  $|\text{Aut}(G)| = 4$ . One can check that  $\text{Aut}(G)$  is cyclic, so we have that  $G$  is isomorphic to  $C_4$ .

(c) Note that if  $H$  is a subgroup of  $G$  (denoted  $H \leq G$ ), and  $\varphi \in \text{Aut}(G)$ , then  $|\text{Im}(\varphi|_H)| = |H|$ . That is, since  $\varphi$  restricted to  $H$  is an isomorphism with domain  $H$ , its image must have the same order as  $H$ .

I claim  $\langle (12), (123) \rangle = \langle H, K \rangle = S_3$ . To see this, note that  $|H| = 2$ ,  $|K| = 3$ , so 2 and 3 divide the order of  $\langle (12), (123) \rangle$ , that is,  $6 \leq |\langle (12), (123) \rangle| \leq S_3$ . But  $|S_3| = 6$ , so we have our result.

By an easy extension of the argument in (a), the image of these two generators under  $\varphi$  determines the automorphism. From order considerations, we have  $\varphi((12)) = (12), (13)$  or  $(23)$ , and  $\varphi((123)) = (123), (132)$ . Using the argument above, we note that any combination of a two-cycle and a three-cycle generates the group. Thus, since any element of  $\sigma \in S_3$  can be written as some product  $\sigma = (12)\dots(123)\dots(12)\dots$  we simply define  $\varphi(\sigma) = \varphi(12)\dots\varphi(123)\dots\varphi(12)\dots$ . It is easy to see that such a map is an isomorphism. There are 6 such maps, and thus  $|\text{Aut}(S_3)| = 6$ .

Thus, by problem 2.6.11 below,  $\text{Aut}(S_3)$  is isomorphic to  $S_3$  or  $C_6$ . I claim  $\text{Aut}(S_3)$  is isomorphic to  $S_3$ . Clearly, if we show  $\text{Aut}(S_3)$  is nonabelian, then we're done. Conjugation by an arbitrary element  $\sigma \in S_3$  is always an automorphism (this is easy to check; it actually works for any group). To prove  $S_3$  is nonabelian, therefore, it is sufficient to demonstrate  $\sigma_1, \sigma_2$  such that switching the order of conjugation by these elements does not yield the same automorphism. That is, we must find  $\sigma_1, \sigma_2, \sigma_3$  such

that  $\sigma_1\sigma_2\sigma_3\sigma_2^{-1}\sigma_3^{-1} \neq \sigma_2\sigma_1\sigma_3\sigma_1^{-1}\sigma_2^{-1}$ . One example (which you can check) is

$$(123)(12)(23)(12)^{-1}(123)^{-1} = (12)$$

$$(12)(123)(23)(123)^{-1}(12)^{-1} = (23).$$

## 2 2.4.5

Let  $x, y \in G$ . We have  $\varphi(xy) = (xy)^n = xyxyxy\dots xy$  ( $n$  times)  $= x^n y^n$  (because  $G$  is abelian)  $= \varphi(x)\varphi(y)$ .

## 3 2.4.8

(a) A subgroup of  $S_3$  must have 1, 2, 3, or 6 elements by Lagrange's Theorem. The subgroup with 1 element is clearly the trivial subgroup, and the subgroup with 6 elements is clearly  $S_3$ . If any subgroup contains a 2-cycle and a 3-cycle, it must contain the disjoint subgroups of orders 2 and 3 contained generated by these cycles, so it must be of order at least 6, that is, it must be all of  $S_3$ . Thus the only other subgroups are the cyclic subgroups generated by the three 2-cycles, (3 of order 2), and the cyclic subgroup generated by the 3-cycles, (one of order 3). By problem 2.6.10(a), the subgroup generated by the three cycles is normal. None of the 2-cycle subgroups are normal (as you can check by looking at the group table from the last assignment).

(b) Since the quaternion group, call it  $G$ , has 8 elements, it can have subgroups of order 1, 2, 4, 8. Again, the subgroups of order 1 and 8 are the trivial subgroup and  $G$  itself. Denoting the elements as on p48, we have the subgroups generated by  $i, j, k$ , each of order 4 (as one can check by simply multiplying out the matrices). Since each of these subgroups have index 2, they're normal by problem 2.6.10(a). We note that  $\langle -i \rangle = \langle i \rangle$ ,  $\langle -j \rangle = \langle j \rangle$ ,  $\langle -k \rangle = \langle k \rangle$  and  $-1$  is an element of each of these subgroups.

We also have the subgroup generated by  $-1$ , which is of order 2. Let  $g \in G - \{1, -1\}$ . Then, as stated above,  $g$  has order 4, which implies  $g^{-1}(-1)g = g^3(-1)g = (-1)(g^4) = -1$ , so this subgroup is normal as well. Any combination of two of  $i, j, k$  generates the group, as you can check from the relations given on p48. Thus, this is it.

## 4 2.4.16

Consider restricting the homomorphism  $\varphi$  to  $H = \langle x \rangle$ .  $Im(\varphi|_H) = \langle \varphi(x) \rangle$  in  $G'$ , and thus  $|Im(\varphi|_H)| = |\varphi(x)|$ . Since  $|H| = |Ker\varphi||Im\varphi|$ , we have that  $|\varphi(x)|$  divides  $r$ .

## 5 2.4.23

Suppose  $g' \in G'$ . Because  $\varphi$  is surjective, we can write  $g' = \varphi(g)$  for some  $g \in G$ . We have  $g'\varphi(N)g'^{-1} = \varphi(g)\varphi(N)\varphi(g)^{-1} = \varphi(g)\varphi(N)\varphi(g^{-1}) = \varphi(gNg^{-1}) = \varphi(N)$ .

## 6 2.6.4

Let  $\gamma = \begin{bmatrix} i & 0 \\ 0 & 1 \end{bmatrix}$ . We have

$$\gamma GL_2(\mathbb{R}) = \left\{ \begin{bmatrix} ai & bi \\ c & d \end{bmatrix} \mid ab - cd \neq 0, a, b, c, d \in \mathbb{R} \right\}$$

and

$$GL_2(\mathbb{R})\gamma = \left\{ \begin{bmatrix} ai & b \\ ci & d \end{bmatrix} \mid ab - cd \neq 0, a, b, c, d \in \mathbb{R} \right\}.$$

Clearly these two cosets are unequal.

## 7 2.6.10

(a) Let  $H \leq G$  such that  $[G : H] = 2$ . Clearly  $hHh^{-1} = H$  for  $h \in H$ . Suppose  $a \in G - H$  and  $aha^{-1} \notin H$  for some  $h \in H$ . Since  $[G : H] = 2$ , we have  $aha^{-1} \in aH$ , which implies  $(a^{-1}a)ha^{-1} = ha^{-1} \in (a^{-1}a)H = H$ . Thus  $ha^{-1} = h'$  for some  $h' \in H$ , and we have  $a^{-1} = h^{-1}h' \in H$ , which implies  $a \in H$ , a contradiction. Thus  $aha^{-1} \in H$  for all  $h \in H$ ; that is,  $H$  is normal.

(b) Consider the subgroup of  $S_3$  generated by (12). This subgroup is of order 2 in a group of order 6. Thus it has index 3. By looking at the multiplication table for  $S_3$  drawn up on the last homework, it is clear that this subgroup is not normal.

## 8 2.6.11

(a) If  $G$  is a group with an element of order 6, say  $x$ , and  $|G| = 6$ , then clearly  $G = \langle x \rangle$ , which is isomorphic to  $C_6$ .

(b) Before beginning this proof, I would like to note that very few of you actually proved this result. This is understandable; it's tricky to provide a classification of groups of a particular order. I'll try to point out the places where most had trouble.

Claim: If  $|G| = 6$ ,  $G$  has an element of order 3, and none of order 3, then  $G$  is isomorphic to  $S_3$ .

Proof: Let  $x$  be an element of order 3 in  $G$ . We thus have the subgroup  $\{e, x, x^2\} \leq G$ . Let  $y \in G$ ,  $y \notin \langle x \rangle$ . Then  $y, xy, x^2y \in G$ . This is the right coset  $\langle x \rangle y$ . Noting that cosets partition the group, and that these two cosets provide 6 elements, we have  $G = \{e, x, x^2, y, xy, x^2y\}$ .

We CANNOT automatically assume  $|y| = 2$ ; we must prove it. By Lagrange's theorem,  $|y| = 1, 2, 3$ , or 6. Clearly  $y \neq 1, 6$ . Suppose  $|y| = 3$ . Then  $y^2 \in$

$\{x, x^2, y, xy, x^2y, \}$ . Using the cancellation law, we can construct contradictions for any of these values. For example, suppose  $y^2 = x^2y$ . Then we would have  $y^2y^{-1} = x^2yy^{-1}$  which implies  $y = x^2$ , a contradiction. Thus, assuming we've done all of these checks,  $|y| = 2$ .

There is one more relation we must prove:

$$yx = x^2y.$$

Assuming this result, we may simply reference p44 of Artin and its characterization of  $S_3$ . The proof of this relation was another problem area for most people.

The cancellation law makes it clear that  $yx \notin \{e, x, x^2, y\}$ . Therefore, suppose for a contradiction that  $yx = xy$ . Then  $x$  commutes with  $y$ , and we have  $(xy)^n = x^n y^n$ , which implies  $|xy| = lcm(|x|, |y|) = 6$ . But we assumed that  $G$  contains no elements of order 6, so this is a contradiction, and we have  $yx = x^2y$ . Note that this is the only portion of the proof in which we use the fact that  $G$  contains no elements of order 6.

(Note: Thanks to William Meyerson; I stole a lot of this proof from him).

(c). Claim: If all elements of  $G$  are of order 1 or 2, then  $G$  is abelian.

Proof: Suppose  $a, b \in G$ . We have  $1 = (ab)^2 = (ab)(ab) = aba^{-1}b^{-1}$  which implies  $ba = ab$ .

By order considerations, we must have  $e, x, y \in G$ , and  $xy \in G$  and is distinct from the first three elements, by closure and the cancellation law. By commutativity and the fact that each element has order 2, this we must have at least one more element, call it  $z$ . Now we have  $e, x, y, z, xy, yz, xz, xyz \in G$  by closure. By the cancellation law, all of these elements are distinct. Thus  $|G| \geq 8$ , a contradiction. There are no groups of this form.

## 9 2.8.2

No. Suppose it was nontrivially decomposable, say into a direct product of  $G_1$  and  $G_2$ . This assumption is made without loss of generality, for we can always collapse direct products involving more groups into the product of two groups. Then, by nontriviality and Lagrange's theorem, without loss of generality  $|G_1| = 2, |G_2| = 3$ . Thus  $G_1$  is isomorphic to  $C_2$  and  $G_2$  is isomorphic to  $C_3$ , because these are the only possible isomorphism classes of groups of order 2, 3. Thus we have  $S_3$  is isomorphic to the direct product of  $C_2$  and  $C_3$ , which in turn is isomorphic to  $C_6$  (via Proposition 8.4). But this is a contradiction, see 2.6.11 above.

## 10 2.8.10

Let  $l = lcm(m, n)$ . Then  $(x, y)^l = (x^l, y^l) = (e, e)$ , for  $m, n|l$ . Further, by definition, this is the least integer that  $m, n$  both divide, so it is the order of  $(x, y)$ .

## 11 2.10.1

(a) Let  $A = (a_{ij}) \in G$ , and let  $\varphi : G \rightarrow \mathbb{R}^*$  be the map defined by  $\varphi(A) = a_{11}$ . We have

$$\varphi\left(\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \begin{bmatrix} e & f \\ 0 & h \end{bmatrix}\right) = \varphi\left(\begin{bmatrix} ab & * \\ 0 & * \end{bmatrix}\right) = ab = \varphi\left(\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}\right)\varphi\left(\begin{bmatrix} e & f \\ 0 & h \end{bmatrix}\right).$$

Thus  $\varphi$  is a homomorphism. Because its kernel is exactly the set  $H$ ,  $H \leq G$  and  $H$  is normal. This map is clearly surjective, so we have  $G/H$  is isomorphic to  $\mathbb{R}^*$ .

(b).  $H$  is not normal. For example, note

$$\begin{bmatrix} 2 & 3 \\ 0 & 4 \end{bmatrix} \begin{bmatrix} 3 & 0 \\ 0 & 5 \end{bmatrix} \begin{bmatrix} 2 & 3 \\ 0 & 4 \end{bmatrix}^{-1} = \begin{bmatrix} 3 & 3/2 \\ 0 & 5 \end{bmatrix}.$$

(c). Let  $\varphi : G \rightarrow \mathbb{R}^*$  be the map defined by  $\varphi(A) = a_{11}/a_{22}$ . We have

$$\varphi\left(\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \begin{bmatrix} e & f \\ 0 & h \end{bmatrix}\right) = \varphi\left(\begin{bmatrix} ae & * \\ 0 & dh \end{bmatrix}\right) = ae/dh = \varphi\left(\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}\right)\varphi\left(\begin{bmatrix} e & f \\ 0 & h \end{bmatrix}\right).$$

So  $\varphi$  is a homomorphism. Because its kernel is exactly the set  $H$ ,  $H \leq G$  and  $H$  is normal. This map is clearly surjective, so we have  $G/H$  is isomorphic to  $\mathbb{R}^*$ .

(d). Let  $\varphi : G \rightarrow (\mathbb{R}^*)^2$  be the map defined by  $\varphi(A) = (a_{11}, a_{22})$ . We have

$$\varphi\left(\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \begin{bmatrix} e & f \\ 0 & h \end{bmatrix}\right) = \varphi\left(\begin{bmatrix} ae & * \\ 0 & dh \end{bmatrix}\right) = (ab, dh) = \varphi\left(\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}\right)\varphi\left(\begin{bmatrix} e & f \\ 0 & h \end{bmatrix}\right).$$

So  $\varphi$  is a homomorphism. Because its kernel is exactly the set  $H$ ,  $H \leq G$  and  $H$  is normal. This map is clearly surjective, and we have  $G/H$  is isomorphic to  $(\mathbb{R}^*)^2$ .

## 12 2.10.10

Define  $\varphi : \mathbb{C}^x \rightarrow U$  by  $\varphi(z) = \frac{z}{|z|}$ . We have  $\varphi(zw) = \frac{z}{|z|} \frac{w}{|w|} = \frac{zw}{|zw|} = \varphi(z)\varphi(w)$ , so  $\varphi$  is a homomorphism, and from elementary complex analysis, it is a surjective map onto  $U$ . Further,  $\frac{z}{|z|} = 1$  if and only if  $z \in P$ . Thus, by the first isomorphism theorem,  $\mathbb{C}^x/P$  is isomorphic to  $U$ .

Define  $\varphi : \mathbb{C}^x \rightarrow P$  by  $\varphi(z) = |z|$ . We have  $\varphi(zw) = |zw| = |z||w| = \varphi(z)\varphi(w)$ , so  $\varphi$  is a homomorphism, and from elementary complex analysis, it is a surjective map onto  $P$ . Further,  $|z| = 1$  if and only if  $z \in U$ . Thus, by the first isomorphism theorem,  $\mathbb{C}^x/U$  is isomorphic to  $P$ .