

## ALGEBRA HW 3

CLAY SHONKWILER

I.(A)

(i) In  $S_3$ , the only subgroups of order 2 are:  $\{1, (12)\}$ ,  $\{1, (13)\}$ ,  $\{1, (23)\}$

(ii) In  $S_3$ , the only subgroup of order 3 is:  $\{1, (123), (132)\}$ .

In  $S_4$ , the only subgroups of order 3 are:  $\{1, (123), (132)\}$ ,  $\{1, (124), (142)\}$ ,  $\{1, (134), (143)\}$ ,  $\{1, (234), (243)\}$ .

I.(B)

Show that if  $h$  is an automorphism of  $S_3$ , then there exists  $\sigma \in S_3$  such that  $h(\tau) = \sigma\tau\sigma^{-1}$  for all  $\tau \in S_3$ .

*Proof.* Since an automorphism cannot change the order of an element, there are only three possibilities for  $h((12))$ :  $(12)$ ,  $(13)$ ,  $(23)$  and 2 for  $h((123))$ :  $(123)$ ,  $(132)$ . Suppose  $h((12)) = (13) = (23)(12)(23)$  and  $h((123)) = (132) = (23)(123)(23)$ . Then  $h((132)) = (123) = (23)(132)(23)$  since  $h$  is an automorphism ( $(132)$  must map to an element of order 3 other than itself, since  $(123) \mapsto (132)$ ) and:

$$h((23)) = h((12)(123)) = h((12))h((123)) = (13)(132) = (23) = (23)(23)(23)$$

and

$$h((13)) = h((12)(132)) = h((12))h((132)) = (13)(123) = (12) = (23)(13)(23).$$

Hence,  $h(\tau) = (23)\tau(23)$  for each  $\tau \in S_3$ . Similarly, if  $h((12)) = (13) = (132)(12)(123)$  and  $h((123)) = (123) = (132)(123)(123)$ , then

$$h((132)) = (132) = (132)(132)(123),$$

$$h((23)) = h((12)(123)) = h((12))h((123)) = (13)(123) = (12) = (132)(23)(123)$$

and

$$h((13)) = h((12)(132)) = h((12))h((132)) = (13)(132) = (23) = (132)(13)(123).$$

Again, for all  $\tau \in S_3$ ,  $h(\tau) = \sigma\tau\sigma^{-1}$ , in this case where  $\sigma = (132)$ . This same calculation can be done for all six possible automorphisms of  $S_3$ , demonstrating the desired result.  $\square$

## II

**Theorem 0.1.** *If  $G$  is a finite group, then except for 2 such  $G$ , there is always an automorphism,  $h$ , of  $G$  which is not the identity. The groups which are exceptions are:  $\{1\}$  and  $\mathbb{Z}/2\mathbb{Z}$ .*

*Proof.* Suppose  $G$  is not abelian. Then there exist  $a, b \in G$  such that  $bab^{-1} \neq a$ . Define the map  $h : G \rightarrow G$  by

$$h(x) = bxb^{-1}.$$

Clearly  $h$  is not the identity map. Now, suppose  $h(x) = h(y)$  for some  $x, y \in G$ . Then

$$bxb^{-1} = byb^{-1} \Leftrightarrow bx = by \Leftrightarrow x = y$$

so  $h$  is injective. Furthermore, for any  $x \in G$ ,

$$h(b^{-1}xb) = bb^{-1}xbb^{-1} = x$$

so  $h$  is surjective. Finally, for any  $x, y \in G$ ,

$$h(xy) = bxyb^{-1} = bx(b^{-1}b)yb^{-1} = (bxb^{-1})(byb^{-1}) = h(x)h(y)$$

so  $h$  is a non-trivial isomorphism.

On the other hand, suppose  $G$  is an abelian group with at least one element  $c$  or order greater than 2. Then  $c^{-1} \neq c$ . Hence, if we define  $h : G \rightarrow G$  by

$$h(x) = x^{-1},$$

$h$  is not the identity map.  $h$  is clearly bijective, so we need only check that it is a homomorphism. To that end, let  $x, y \in G$ . Then

$$h(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = h(x)h(y).$$

Finally, if  $G$  is an abelian group with every non-identity element of order 2, then choose two elements  $a, b \in G$  such that  $a \neq b$ . Let  $h(a) = b$  and  $h(b) = a$  and then construct  $h$  by extending in the natural way. That is to say, for all  $\alpha \in G$ ,

$$\alpha = a^{\delta_1}b^{\delta_2}\alpha_3 \cdots \alpha_n$$

where  $\delta_1, \delta_2$  are either 0 or 1, so let

$$h(\alpha) = a^{\delta_2}b^{\delta_1}\alpha_3 \cdots \alpha_n.$$

It is immediately clear that  $h$  is non-trivial and bijective, and, to see that it is a homomorphism, let  $\alpha, \beta \in G$ . Then  $\alpha = a^{\delta_{\alpha_1}}b^{\delta_{\alpha_2}}\alpha_3 \cdots \alpha_n$ ,  $\beta = a^{\delta_{\beta_1}}b^{\delta_{\beta_2}}\beta_3 \cdots \beta_m$  for  $n, m \in \mathbb{N}$ , and each of the  $\delta$ 's either 0 or 1. Then

$$\begin{aligned} h(\alpha\beta) &= a^{\delta_{\alpha_2} + \delta_{\beta_2}}b^{\delta_{\alpha_1} + \delta_{\beta_1}}\alpha_3 \cdots \alpha_n\beta_3 \cdots \beta_m \\ &= a^{\delta_{\alpha_2}}b^{\delta_{\alpha_1}}\alpha_2 \cdots \alpha_n a^{\delta_{\beta_2}}b^{\delta_{\beta_1}}\beta_2 \cdots \beta_m \\ &= h(\alpha)h(\beta) \end{aligned}$$

where addition of exponents is done modulo 2. Hence,  $h$  is non-trivial automorphism. Hence, we've shown any finite group  $G$  except  $\{1\}$  and  $\mathbb{Z}/2\mathbb{Z}$

(which cannot have a non-trivial automorphism) has a non-trivial automorphism. In fact, we didn't even use the hypothesis that  $G$  is finite, so the result holds as well for infinite groups.  $\square$

## III

(a) We made a map  $k \mapsto \begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix}$  of  $\mathbb{Z}$  into  $SL_2(\mathbb{Z})$ ; identify  $\mathbb{Z}$  with its image. There is also a map  $k \mapsto \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$  of  $\mathbb{Z} \rightarrow SL_2(\mathbb{Z})$ , and again it is an injection and we can identify  $\mathbb{Z}$  with its image. Let  $\underline{\mathbb{Z}}$  and  $\overline{\mathbb{Z}}$  be these two images, respectively. What are

$$(SL_2(\mathbb{Z}) : \underline{\mathbb{Z}}), (SL_2(\mathbb{Z}), \overline{\mathbb{Z}})?$$

**Answer:** Suppose  $A = \begin{pmatrix} 1 & a \\ 1 & a+1 \end{pmatrix}$  and  $B = \begin{pmatrix} 1 & b \\ 1 & b+1 \end{pmatrix}$  are both elements of the same coset  $\begin{pmatrix} b & c \\ d & e \end{pmatrix} \underline{\mathbb{Z}}$  of  $\underline{\mathbb{Z}}$  in  $SL_2(\mathbb{Z})$ . Then

$$\begin{pmatrix} 1 & a \\ 1 & a+1 \end{pmatrix} = \begin{pmatrix} b & c \\ d & e \end{pmatrix} \begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix} = \begin{pmatrix} b+ck & c \\ d+ek & e \end{pmatrix}$$

and

$$\begin{pmatrix} 1 & b \\ 1 & b+1 \end{pmatrix} = \begin{pmatrix} b & c \\ d & e \end{pmatrix} \begin{pmatrix} 1 & 0 \\ j & 1 \end{pmatrix} = \begin{pmatrix} b+cj & c \\ d+ej & e \end{pmatrix}$$

for some  $k, j \in \mathbb{Z}$ . This implies that  $a = c = b$ , so  $A = B$ . Hence, each element of  $SL_2(\mathbb{Z})$  of the form demonstrated by  $A$  and  $B$  must lie in a separate coset of  $\underline{\mathbb{Z}}$  from every other matrix of that form. Since there are infinitely many such matrices (one for each integer), we see that  $\underline{\mathbb{Z}}$  must have infinitely many cosets, or

$$(SL_2(\mathbb{Z}) : \underline{\mathbb{Z}}) = \infty.$$

Similarly, distinct matrices of the form  $\begin{pmatrix} x & 1 \\ x-1 & 1 \end{pmatrix}$  must lie in distinct cosets of  $\overline{\mathbb{Z}}$  in  $SL_2(\mathbb{Z})$ , so

$$(SL_2(\mathbb{Z}) : \overline{\mathbb{Z}}) = \infty.$$



(b) What are

$$(GL_2(\mathbb{Z}) : SL_2(\mathbb{Z}))$$

$$(GL_2(\mathbb{Z}) : \underline{\mathbb{Z}})$$

$$(GL_2(\mathbb{Z}) : \overline{\mathbb{Z}})?$$

**Answer:** The answer to the last two is clearly  $\infty$ , since  $GL_2(\mathbb{Z}) \supset SL_2(\mathbb{Z})$ . To answer the first, let  $A, B \in GL_2(\mathbb{Z})$  such that  $A$  and  $B$  are

in the same coset,  $CSL_2(\mathbb{Z})$ . Hence,  $A = CD$  and  $B = CE$  for some  $D, E \in SL_2(\mathbb{Z})$ . Now,

$$\det(A) = \det(CD) = \det(C) \det(D) = \det(C)$$

and

$$\det(B) = \det(CE) = \det(C) \det(E) = \det(C),$$

so we see that  $\det A = \det C = \det B$ . That is to say that it is necessary for  $A$  and  $B$  to have the same determinant if they are to lie in the same coset of  $SL_2(\mathbb{Z})$ , which is to say there are at least as many cosets as there are possible determinants for matrices in  $GL_2(\mathbb{Z})$ . Hence

$$(GL_2(\mathbb{Z}) : SL_2(\mathbb{Z})) = \infty.$$



(c) Is  $\underline{\mathbb{Z}}$  a normal subgroup of  $SL_2(\mathbb{Z})$ ? What about  $\overline{\mathbb{Z}}$ ? Answer the same question *vis a vis*  $\underline{\mathbb{Z}}$  and  $GL_2(\mathbb{Z})$  and  $\overline{\mathbb{Z}}$  and  $GL_2(\mathbb{Z})$ .

**Answer:** The answer is no to all four questions. In fact, if we can demonstrate that neither  $\underline{\mathbb{Z}}$  nor  $\overline{\mathbb{Z}}$  are normal subgroups in  $SL_2(\mathbb{Z})$ , then it is clear that they cannot be normal subgroups in  $GL_2(\mathbb{Z})$ , either. Now,  $\begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix} \in \underline{\mathbb{Z}}$ ,  $\begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix} \in \overline{\mathbb{Z}}$  and  $\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \in SL_2(\mathbb{Z})$  with inverse  $\begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix}$ , but

$$\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix} \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 9 & -4 \\ 16 & -7 \end{pmatrix} \notin \underline{\mathbb{Z}}$$

and

$$\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} -3 & 4 \\ -4 & -5 \end{pmatrix} \notin \overline{\mathbb{Z}}.$$

Hence, neither  $\underline{\mathbb{Z}}$  nor  $\overline{\mathbb{Z}}$  is normal in either  $SL_2(\mathbb{Z})$  or  $GL_2(\mathbb{Z})$ .



(d) Let  $\sigma = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$  and  $\tau = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$ . Compute  $o\{\sigma\}$ ,  $o\{\tau\}$ . Now compute  $o\{\sigma\tau\}$ . What sobering fact has this example shown?

**Answer:**

$$\begin{aligned} \sigma^4 &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \end{aligned}$$

so  $o\{\sigma\} = 4$ . Also,

$$\begin{aligned}\tau^3 &= \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\end{aligned}$$

so  $o\{\tau\} = 3$ . However,

$$\sigma\tau = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$

which has infinite order, as

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^k = \begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix}.$$

Hence, the sobering fact that we discover is that order is not a multiplicative property.



#### IV

Let  $G$  be a finite group and suppose  $G$  possesses an automorphism,  $h$ , having two properties:

- a)  $h(\sigma) = \sigma \Leftrightarrow \sigma = 1$
- b)  $(\forall \sigma \in G)(h(h(\sigma)) = \sigma)$

Prove that  $G$  must be an abelian group.

#### V

Say  $H_1, H_2$  are two subgroups of a (possibly infinite) group,  $G$ . Suppose  $(G : H_1) < \infty$  and  $(G : H_2) < \infty$ . Prove that  $(G : H_1 \cap H_2) < \infty$ .

*Proof.* Suppose  $a(H_1 \cap H_2)$  and  $b(H_1 \cap H_2)$  are distinct cosets of  $H_1 \cap H_2$ , but  $aH_1 = bH_1$  and  $aH_2 = bH_2$ . Let  $x \in a(H_1 \cap H_2)$ . Then, since  $a(H_1 \cap H_2)$  and  $b(H_1 \cap H_2)$  are distinct,  $x \notin b(H_1 \cap H_2)$ . Then  $x = ah$  for some  $h \in H_1 \cap H_2$ . Hence, we see that

$$x \in aH_1 = bH_1$$

and

$$x \in aH_2 = bH_2.$$

That is to say that  $x = bh'_1$  and  $x = bh'_2$  for some  $h'_1 \in H_1$  and  $h'_2 \in H_2$ .

$$bh'_1 = x = bh'_2 \Leftrightarrow h'_1 = h'_2,$$

which means that  $h'_1 = h'_2 \in H_1 \cap H_2$ , which in turn implies that

$$x \in b(H_1 \cap H_2),$$

contradicting our assumption that  $a(H_1 \cap H_2)$  and  $b(H_1 \cap H_2)$  are distinct. Hence, if  $a(H_1 \cap H_2)$  and  $b(H_1 \cap H_2)$  are to be distinct, it must be the case that  $aH_1 \neq aH_2$  or  $bH_1 \neq bH_2$ . As such, we have at most

$$(G : H_1)(G : H_2)$$

possible distinct cosets of  $H_1 \cap H_2$ , which is another way of saying that

$$(G : H_1 \cap H_2) < \infty.$$

□

## VI

Suppose  $G$  is a (possibly infinite) group and  $G$  possesses a subgroup  $H$  for which  $(G : H) < \infty$ . Prove that  $G$  possesses a normal subgroup  $N$  so that  $(G : N) < \infty$ .

## VII

Suppose  $G$  is a finite simple group and let  $p$  be a prime number. List the elements of order  $p$  in  $G : \sigma_1, \dots, \sigma_n$  (suppose these exist). Show that

$$G = Gp\{\sigma_1, \dots, \sigma_n\}.$$

*Proof.* Suppose  $G \neq Gp\{\sigma_1, \dots, \sigma_n\}$ . Then there exists  $\tau \in G$  such that  $\tau \notin Gp\{\sigma_1, \dots, \sigma_n\}$ . Note that

$$(\tau\sigma_i^m\tau^{-1})^p = \tau(\sigma_i^m)^p\tau^{-1} = \tau(\sigma_i^p)^m\tau^{-1} = \tau\tau^{-1} = 1$$

for all  $i = 1, \dots, n$ ,  $m \in \mathbb{Z}$ . Now, let  $\sigma = \sigma_1^{a_1} \dots \sigma_n^{a_n} \in Gp\{\sigma_1, \dots, \sigma_n\}$ . Then

$$\begin{aligned} \tau\sigma\tau^{-1} &= \tau(\sigma_1^{a_1} \dots \sigma_n^{a_n})\tau^{-1} \\ &= \tau(\sigma_1^{a_1}(\tau^{-1}\tau)\sigma_2^{a_2}(\tau^{-1}\tau) \dots (\tau^{-1}\tau)\sigma_n^{a_n})\tau^{-1} \\ &= (\tau\sigma_1^{a_1}\tau^{-1}) \dots (\tau\sigma_n^{a_n}\tau^{-1}) \in Gp\{\sigma_1, \dots, \sigma_n\} \end{aligned}$$

since each term in the product is in  $Gp\{\sigma_1, \dots, \sigma_n\}$ . Hence,  $Gp\{\sigma_1, \dots, \sigma_n\}$  is a normal subgroup of  $G$ . However, this contradicts our assumption that  $G$  is simple. From this contradiction, we conclude that, in fact,  $G = Gp\{\sigma_1, \dots, \sigma_n\}$ . □