Homework 3 – Algebraic Structures

Ch 2: 8.8, 8.9, 8.10, 10.3, 10.4, 10.5, 11.2, 11.5, 11.6, 11.9,
12.4, 12.5, M.3 &
Pre-lect: Chapter 2, 9.1, 10.1, 11.1, 12.1

Blake Griffith

Exercise (8.8)**.** *Let G be a group of order 25. Prove that G has at least one subgroup of order 5, and that if it contains only one subgroup of order 5, then it is a cyclic group.*

Proof. Suppose G is cyclic with some generator x. Then x^5 generates a subgroup of order 5. $< x^5 >= \{1, x^5, x^{10}, x^{15}, x^{20}\}$.

Suppose G is not cyclic. Then there is no element that generates all of G. So taking some element x in G (where x is not the identity). This element must generate a subgroup smaller than G. By Lagrange's theorem, this subgroup can only be order 5.

So G must contain at least one subgroup of order 5.

Now if G only contains one proper subgroup, H, and H is order 5. Then any element x in G but not in H must generate G otherwise it would generate a proper subgroup. So since $< x >= G$, G is cyclic.

□

Exercise (8.9)**.** *Let G be a finite group. Under what circumstances is the map $\phi : G \to G$ defined by $\phi(x) = x^2$ an automorphism of G?*

Proof. First every element other than the identity must have odd order. Otherwise, if we had some element x with even order $2N$ so that $x^{2N} = 1$ then $\phi(x^N) = 1 = \phi(1)$. So ϕ would not be injective. Therefore ϕ could not be an automorphism since $|\text{img } \phi| < |G|$ so $\text{img } \phi \neq G$.

Now since each element has odd order, no element can be its own inverse, since if some element x was its own inverse it would generate the even ordered subgroup $< x >= \{1, x\}$. So for each (non identity) element in our group there is a distinct corresponding inverse, so the elements must come in pairs. So there is an even number of non identity elements.

So there is some even number of non identity elements plus the identity, so the order of the group must be odd.

So we can say ϕ can be an automorphism on a group G if G has odd order and every non identity element has odd order.

□

Exercise (8.10)**.** *Prove that every subgroup of index* 2 *is a normal subgroup, and show by an example that a subgroup of index* 3 *need not be normal.*

Proof. First, there are the same number of right cosets as left cosets. This is because there is a bijection between left and right cosets. Let this bijection be ϕ such that $\phi(gH) = Hg^{-1}$.

ϕ is well defined, if we have some a and b such that $aH = bH$ then $a^{-1}b \in H$. So $\phi(aH) = Ha^{-1}$ and $\phi(bH) = Hb^{-1}$. Now $Ha^{-1} \subseteq Hb^{-1}$ since for any h_1 in H there is some h_2 such that $h_1a^{-1}b = h_2 \implies h_1a^{-1} = h_2b^{-1}$. Likewise $Ha^{-1} \supseteq Hb^{-1}$. So ϕ is well defined.

ϕ is injective. Suppose there exists some xH and yH such that $\phi(xH) = \phi(yH) \implies Hx^{-1} = Hy^{-1}$ then $x^{-1} = hy^{-1}$ for some h in H then $yx^{-1} \in H$. Then $xH \subseteq yH$ because for any $h_1 \in H$ there is a $h_2 \in H$ such that $y^{-1}xh_1 = h_2 \implies xh_1 = yh_2$. Likewise $xH \supseteq yH$. So $xH = yH$. So

ϕ is surjective. Let Hx be some right coset, then it's preimage is $x^{-1}H$ since $\phi(x^{-1}H) = Hx$.

This establishes that there are the same number of left cosets as right cosets.

Call this group with index 2 H. Then of the 2 left cosets that partition the group, one of them must be H since for any h in H $hH = H$. Likewise $H = Hh$.

Let the other left coset be g_1H for any $g_1 \in G-H$. And let the corresponding right coset be Hg_2 for any $g_2 \in G-H$. Since these cosets partition the group, we have $G = H \cup g_1H = H \cup Hg_2$ or $g_1H = Hg_2$. If we take $g_1 = g_2 = g$ then $gH = Hg$. So for any h_1 in H, g in G, there exists a h_2 such that $gh_1 = h_2g \implies gh_1g^{-1} = h_2$. So H is a normal subgroup.

For an example of a subgroup that is index 3 and not normal. See the subgroup $< y >$ in S_3. Its left cosets are $\{1, y\}$, $\{x, xy\}$, and $\{x^2, x^2y\}$ so its index is 3. And it is not normal in S_3 since $xyx^{-1} = xyx^2 = xy$, which is not in $< y >$.

□

Exercise (10.3)**.** *Let G and G' be cyclic groups of order* 12 *and* 6*, generated*

by elements x and y, respectively, and let $\phi : G \to G'$ be the map defined by $\phi(x^i) = y^i$. Exhibit the correspondence referred in the Correspondence Theorem explicitly.

Proof. ϕ is surjective, if we take y^i in G' this is mapped by x^i in G.

$\ker \phi$ is all $x^i \in G$ such that $\phi(x^i) = 1 = y^6$. This is given by $\ker \phi = \{1, x^6\}$.

First we find the groups in G that contain $\ker \phi$. G and K are obvious the others are generated by x^n where n divides 6. So $G_3 = \{1, x^3, x^6, x^9\}$ and $G_2 = \{1, x^2, x^4, x^6, x^8, x^{10}\}$. There are four of these.

Now we find all the subgroups of G'. These are given by $\phi(K)$, $\phi(G)$, $\phi(G_3)$, and $\phi(G_2)$. So they are $\{1\}$, G', $G'_2 = \{1, y^2, y^4\}$, and $G'_3 = \{1, x^3\}$.

So there are 4 subgroups of G which contain K and 4 subgroups of G'. So there is a bijection between the two since they are the same size.

□

Exercise (10.4)**.** *With the notation of the Correspondence Theorem, let H and H' be corresponding groups. Prove that $[G : H] = [G' : H']$.*

Proof.

$$
\begin{aligned}
[G : H] &= \frac{|g|}{|H|} && \text{By counting theorem} \\
&= \frac{|K|[G : K]}{|H|} && \text{By counting theorem} \\
&= \frac{|K||\text{img } \phi}{|H|} && \text{Left cosets of } \ker \phi \text{ are in bijection with img } \phi \\
&= \frac{|K||G'|}{H|} && \phi \text{ is surjective so img } \phi = G' \\
&= \frac{|K||G'|}{|K||H'|} && \text{By correspondence theorem} \\
&= \frac{|G'|}{|H'|} && \text{Cancellation} \\
&= [G' : H'] && \text{By counting theorem}
\end{aligned}
$$

So $[G : H] = [G' : H']$.

□

Exercise (10.5)**.** *With the reference to the homomorphism $S_4 \to S_3$ described in Example 2.5.13, determine the six subgroups of S_4 that contain K.*

Proof. From the example we know $K = \{1, (\mathbf{12})(\mathbf{34}), (\mathbf{13})(\mathbf{24}), (\mathbf{14})(\mathbf{23})\}$ so $|K| = 4$. From the correspondence theorem we know that for a subgroup H in S_4 and its corresponding subgroup H' in S_3, $|H| = |K||H'|$. So the corresponding subgroups in S_4 are order 4, 8×3, 12 and 24. Obviously the order 4 and 24 subgroups are K and S_4, respectively. We know A_4 in S_3 is order 12 and contains all the even permutations and all the permutations in K are even, so A_4 must correspond with $< x >$ in S_3.

Now we must find the subgroups in S_4 that correspond to $< y >, < xy >, < x^2y >$ in S_3. First consider $< y >$, by the definition of the homomorphism we can see

$$y = (\mathbf{12}) = \{\Pi_1, \Pi_2\} \implies \Pi_1 : \{1, 2\} \cup \{3, 4\} \rightsquigarrow \Pi_2 : \{1, 3\} \cup \{2, 4\}$$

So the corresponding cycle in S_4 must be $(\mathbf{23})$. This cycle and K gives the subgroup: $K + \{(\mathbf{23}), (\mathbf{1243}), (\mathbf{1342}), (\mathbf{14})\}$.

Now the same process for x^2y yields a corresponding subgroup of $K + \{(\mathbf{34}), (\mathbf{1324}), (\mathbf{12}), (\mathbf{1423})\}$.

With xy this yields a corresponding subgroup of $K+\{(\mathbf{24}), (\mathbf{1234}), (\mathbf{13}), (\mathbf{1432})\}$.

□

Exercise (11.2)**.** *What does Proposition 2.11.4 tell us when, with the usual notation for the symmetric group S_3, K and H are the subgroups $\langle y \rangle$ and $\langle x \rangle$?*

Proof. We are treating $< x >$ as H and $< y >$ as K.

- $< x > \cap < y >= 1$ so f is injective.
- $yx = x^2y \neq xy$ so f is not a group homomorphism from $< x > \times < y >$ to S_3.
- To check if $< x >$ is a normal subgroup we check if its index is 2 (See exercise 8.10). Obviously the cosets $1 < x >$, $x < x >$, and $x^2 < x >$

are $< x >$. So we compute the nontrivial cases.

$$\begin{aligned} y < x > &= \{y, yx, yx^2\} &&= \{y, x^2y, xy\} \\ xy < x > &= \{xy, xyx, xyx^2\} &&= \{y, x^2y, xy\} \\ x^2y < x > &= \{x^2y, x^2yx, x^2yx^2\} &&= \{y, x^2y, xy\} \end{aligned}$$

So $[S_3 :< x >] = 2$, so $< x >$ is normal in S_3. So $< x >< y >$ is a subgroup of S_3.

- $< y >$ is not normal in S_3 since $xyx^{-1} = xyx^2 = xy$ which is not in $< y >$. So f is not an isomorphism from $< x > \times < y >$ to S_3.

□

Exercise (11.5)**.** *Let G_1 and G_2 be groups and let Z_i be the center of G_i. Prove that the center of the product group $G_1 \times G_2$ is $Z_1 \times Z_2$.*

Proof. If $Z_1 \times Z_2$ is in the center C of $G_1 \times G_2$ then for all g in $G_1 \times G_2$ and z in $Z_1 \times Z_2$, $zg = gz$.

We can rewrite g and z using the definition of a product group. $g = (g_1, g_2)$ for some g_1 in G_1 and g_2 in G_2 likewise $z = (z_1, z_2)$ for some z_1 in Z_1 and z_2 in Z_2. So

$$\begin{aligned} zg &= (z_1, z_2)(g_1, g_2) \\ &= (z_1g_1, z_2g_2) && \text{by definition of product group} \\ &= (g_1z_1, g_2z_2) && \text{since } z_1 \text{ and } z_2 \text{ are in the center} \\ &= (g_1, g_2)(z_1, z_2) && \text{definition of product group} \\ &= gz \end{aligned}$$

So any element in $Z_1 \times Z_2$ commutes with any element of $G_1 \times G_2$. So $Z_1 \times Z_2$ is in the center of $G_1 \times G_2$, i.e. $Z_1 \times Z_2 \subseteq C$

Any element in the center must commute with any element of the group. So we take some arbitrary element c in the center C. By definition of the center we must have $cg = gc$ for any g in G. We can rewrite c and g using the definition of product groups. $c = (c_1, c_2)$ for some c_1, c_2 in C_1 and C_2. And $g = (g_1, g_2)$ for some g_1, g_2 in G_1 and G_2.

$$cg = (c_1, c_2)(g_1, g_2) = (c_1 g_1, c_2 g_2) = (g_1 c_1, g_2 c_2) = (g_1, g_2)(c_1, c_2) = gc$$

So any element in C_1 commutes with any element of G_1, likewise for C_2. So C_1 must in the center Z_1 of G_1 likewise C_2 is in the center Z_2 of G_2. So $C \subseteq Z_1 \times Z_2$.

□

Exercise (11.6)**.** *Let G be a group that contains normal subgroups of order* 3 *and* 5*, respectively. Prove that G contains an element of order* 15*.*

Proof. We denote the order 3 subgroup as H and the order 5 group as K. Note that H and K must be cyclic since they are prime order.

We apply proposition 2.11.4.d to show that there is a isomorphism between a subgroup S of G and the product group $H \times K$; which is a cyclic group of order 15 by proposition 2.11.3 and therefore has an element of order 15.

We take $HK = S$. S is guaranteed to be a group by proposition 2.11.4.C, since H and K are normal. Since H, and K are normal in G they are normal in its subgroups, i.e. S.

We check $H \cap K = \{1\}$. Suppose H and K shared some non identity element x. Since H and K are prime order each of their elements must generate the whole group. So x would have to generate H and K, but this is impossible. So x does not exist and $H \cap K = \{1\}$.

So $H \cap K = \{1\}$, $HK = S$, and H, K are normal in G. Therefore there is an isomorphism between $H \times K$ and S.

Since $H \times K$ is the product of two cyclic groups of order 3 and 5 its order is $3 \times 5 = 15$. Also $H \times K$ is cyclic because its factors have coprime order. So since $H \times K$ is cyclic and order 15 its generator is order 15. Since $H \times K$ is isomorphic to a subgroup of G there must be an element in G that is order 15.

□

Exercise (11.9)**.** *Let H and K be subgroups of a group G. Prove that the product set HK is a subgroup of G if and only if $HK = KH$.*

Proof. If HK is a subgroup of G it must be closed. So that $HKHK = HK$. This is true only if $HK = KH$ since it implies $HKHK = HHKK = HK$.

If $HK = KH$ then H is a group because it is

- Has inverses. If we take some element a in HK. Then we can factor it to hk where h is in H and k is in K. So $a^{-1} = (a)^{-1} = (hk)^{-1} = k^{-1}h^{-1}$. $h^{-1}k^{-1}$ is in HK since h^{-1} is in H and k^{-1} is in K.
- Has identity (1). 1 is in H and K so $1 = 1 \cdot 1$ is in HK.
- Has closure. $HKHK = HHKK$ since $HK = KH$. So $HKHK = HHKK = HK$.

□

Exercise (12.4)**.** *Let $H = \{\pm 1, \pm i\}$ be the subgroup of $G = \mathbb{C}^\times$ of fourth roots of unity. Describe the cosets of H in G explicitly. Is G/H isomorphic to G?*

Proof. For some element $a + ib$ of $\mathbb{C}^\times$. The coset is $(a + ib) = \{a + ib, -a - ib, -b + ia, b - ia\}$.

We can see that G/H is not isomorphic to G if we note $(1+i)H = (-1-i)H = \{1 + i, -1 - i, -1 + i, 1 - i\}$. So a map π between G/H and G could not be isomorphic since $\pi(1 + i) = \pi(-1 - i)$.

□

Exercise (12.5)**.** *Let G be the group of upper triangular matrices $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$, with a and d different from 0. For each of the following subsets determine whether or not S is a subgroup, and whether or not S is a normal subgroup. If S is a normal subgroup, identify the quotient group G/S.*

1. *S is the subset defined by $b = 0$.*
2. *S is the subset defined by $d = 1$.*
3. *S is the subset defined by $a = d$.*

Proof. Note that for some matrix g in G. Where $g = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$, It's inverse is $g^{-1} = \begin{bmatrix} 1/a & -b/(da) \\ 0 & 1/d \end{bmatrix}$.

1. S is a subgroup. To see this consider some element s in S where $s = \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix}$. S contains inverses, $s^{-1} = \begin{bmatrix} 1/a & 0 \\ 0 & 1/d \end{bmatrix}$. S contains the identity matrix. S is closed since $ss = \begin{bmatrix} a^2 & 0 \\ 0 & d^2 \end{bmatrix} \in S$.

   However S is not normal, consider some matrix g in G $g = \begin{bmatrix} a' & b' \\ 0 & d' \end{bmatrix}$

   Then $gsg^{-1} = \begin{bmatrix} a & b'(d-a)/d' \\ 0 & d \end{bmatrix}$. Which is not in S.

2. S is a subgroup. To see this consider some element s in S where $s = \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$. S contains inverses, $s^{-1} = \begin{bmatrix} 1/a & -b/a \\ 0 & 1 \end{bmatrix}$. S contains the identity matrix. S is closed since $ss = \begin{bmatrix} a^2 & b(a+1) \\ 0 & 1 \end{bmatrix} \in S$.

   S is normal in G. Consider some matrix g in G $g = \begin{bmatrix} a' & b' \\ 0 & d' \end{bmatrix}$ Then $gsg^{-1} = \begin{bmatrix} a & b'(1-a)/d' \\ 0 & 1 \end{bmatrix}$. Which is in S.

   S is the kernel of the homomorphism $\phi G \to G'$ where $\phi(X) = X \begin{bmatrix} 1/x_{1,1} & x_{1,2}/x_{1,1} \\ 0 & 1 \end{bmatrix}$. Where $X_{i,j}$ is the element in ith row and jth column of X. So by the first isomorphism theorem, G/S is isomorphic to $\phi(G)$.

3. S is a subgroup. To see this consider some element s in S where $s = \begin{bmatrix} a & b \\ 0 & a \end{bmatrix}$. S contains inverses, $s^{-1} = \begin{bmatrix} 1/a & -b/a^2 \\ 0 & 1/a \end{bmatrix}$. S contains the identity matrix. S is closed since $ss = \begin{bmatrix} a^2 & 2ab \\ 0 & a^2 \end{bmatrix} \in S$.

   S is normal in G. Consider some matrix g in G $g = \begin{bmatrix} a' & b' \\ 0 & d' \end{bmatrix}$ Then

$gsg^{-1} = \begin{bmatrix} a & (-a'b + b'a + a')/d \\ 0 & a \end{bmatrix}$. Which is in S.

S is the kernel of the homomorphism $\phi G \to G'$ where $\phi(X) = X \begin{bmatrix} 1/x_{1,1} & -x_{1,2}/(x_{1,1}x_{2,2} \\ 0 & 1/x_{2,2} \end{bmatrix}$. Where $X_{i,j}$ is the element in ith row and jth column of X. So by the first isomorphism theorem, G/S is isomorphic to $\phi(G)$.

□

Exercise (M.3)**.** *Classify groups of order* 6 *by analyzing the following cases:*

1. *G contains an element of order* 6*.*
2. *G contains an element of order* 3 *but none of order* 6*.*
3. *All elements of G have order 1 or* 2*.*

Proof. 1. G is isomorphic to a cyclic group of order 6. This is clear because the element of order 6 must generate the group since it is the same order as the group.

2. So we know this group has an element of order 3, call it x. So $< x >= \{1, x, x^2\}$. This leaves 3 more elements in G. There cannot be anymore elements of order 3 because these come in pairs, and would account for the remaining 3 elements (since there cannot be another element of order 1). So the remaining elements must all be of order 2. If we call these y, xy, and x^2y we clearly have S_3.

3. This is impossible. To see this suppose G exists.

   The only element in G of order 1 is the identity. So all remaining elements would have to be order 2. So we can write G as the identity and 5 distinct elements.

$$G = \{1, a, b, c, d, e\}, \quad a^2 = b^2 = c^2 = d^2 = e^2 = 1$$

   Note that these elements are abellian $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$. We can define the products of this group, consider ab. It cannot be $1, a$, or b, since 1 would violate the uniqueness of the inverse, or a, b since it would violate the uniqueness of the identity. So without loss of

generality we choose $ab = c$. Likewise for ab we choose $ad = e$, since it cannot be $1, a, b, c, d$. Now if we consider bd. It obviously cannot be $1, b$, or d. Choosing $bd = a$ leads to $a = c$. Choosing $bd = c$ leads to $a = d$. Choosing $ab = e$ leads to $a = d$. So bd cannot violate the group, this violates closure of the group so we have a contradiction.

□

Pre-Lecture Problems

Exercise (9.1)**.** *For which integers n does 2 have a multiplicative inverse in $\mathbb{Z}/\mathbb{Z}n$?*

Proof. Let a be such that $2a = a2 = 1$. For a given n we know that $n = 1 = 2a \implies a = n/2$. a must be an integer so n must be even.

□

Exercise (10.1)**.** *Describe how to tell from the cycle decomposition whether a permutation is odd or even.*

Proof. The parity of a cycle decomposition can be determined from the number of 2-cycles, or transpositions, it can be written as. If a cycle can decomposed into an even number of 2-cycles, it is even. If it can be decomposed into an odd number of 2-cycles then it is odd.

□

Exercise (11.1)**.** *Let x be an element of order r of a group G, and let y be an element of G' of order s. What is the order of (x, y) in the product group $G \times G'$?*

Proof. The order of (x, y) is the least common multiple of r and s, lcm (r, s). Let $n = \text{lcm}\ (r, s)$. Then $(x, y)^n = (x^n, y^n) = (1, 1)$ since n is the smallest integer that r and s divide by definition of the lcm .

□

Exercise (12.1)**.** *Show that if a subgroup H of a group G is not normal, there are left cosets aH and bH whose product is not a coset.*

Proof. S_3's subgroups $< x >$ and $< y >$ are not normal.Consider the cosets $x < y >$ and $y < x >$. Their product is $y < x > x < y >= \{x^2y, x^2, xy, x, y, 1\}$. Since this product is order 6. It cannot be produced by a coset of a proper subgroup of S_3. Therefore $y < x > x < y >$ is not a coset.

□