Blake Griffith

HW 2: Chapter 2, 5.2, 5.4, 6.2, 6.4, 6.7, 6.10, 7.2, 7.4, 8.3, 8.4, 8.5, 8.6 &
Pre-Lecture Problems: Chapter 2, 5.1, 6.1, 7.1, 8.1
M373K
Due 09/19, 2013

Exercise (5.2)**.** *Prove that the intersection $K \cap H$ of subgroups of a group G is a subgroup of H, and that if K is a normal subgroup of G, then $K \cap H$ is a normal subgroup of H.*

Proof.

(a) Show $K \cap H$ is a subgroup of H. Where K and H are subgroups of G:

$K \cap H$ is contained in H because it only contains items which are in both K and H.

We have closure. Consider a and b in $K \cap H$. Then ab is in K because a and b are in K and K is a group. Likewise ab is in H. So since ab is in both K and H, we know ab is in $K \cap H$.

We have inverses. Again considering a, a^{-1} must be in K and H since they both contain a and are groups. So $a^{-1} \in K \cap H$.

We have the identity, I. K and H are both groups so they must contain I. So $K \cap H$ must contain I.

(b) Show that if K is a normal subgroup of G, then $K \cap H$ is a normal subgroup of H:

By part (a), we know $K \cap H$ is a subgroup of H. So we must simply show it is normal to H. Recalling the definition of a normal subgroup we must have for every n in $K \cap H$ and every h in H, hnh^{-1} is in $K \cap H$.

To see this, we consider $hnh^{-1} = c$. We know c must be in K, since K is a normal subgroup of G and h is in G and n is in K.

We also know that c must be in H. Since h is in H, and n is $K \cap H$ and therefore in H. So n, h, and h^{-1}) are in the group H, so the result must be in H.

So c must be in H and K, therefore it is in $K \cap H$. Since hnh^{-1} is in $K \cap H$ it is a normal subgroup.

$\square$

Exercise (5.4)**.** *Let $f : \mathbb{R}^+ \to \mathbb{C}^\times$ be the map $f(x) = e^{ix}$. Prove that f is a homomorphism and determine its kernel and image.*

Proof. Let a and b be elements of $\mathbb{R}^+$ then we have

$$f(a+b) = e^{i(a+b)} f(a)f(b) = e^{ia}e^{ib} = e^{i(a+b)}$$

So f is a homomorphism since $f(a+b) = f(a)f(b)$.

To find the kernel of f we consider the identity of $\mathbb{C}^\times$ which is 1. Using this and Euler's equation to solve we see $e^{ix} = \cos(x) + i\sin(x) = 1$. Which requires $x = n2\pi$ for some integer n. So our kernel is

$$\ker f = K = \{x | x = n2\pi \text{ for any integer } n\}$$

The image of f is given by $f(x) = e^{ix}$ for all x in $\mathbb{R}^+$. This is simply a circle in the complex plane of radius one, centered at the origin. We can write this as

$$\mathrm{im} f = f(\mathbb{R}^+) \{z | 1 = |z| \text{ for any complex number } z\}$$

$\square$

Exercise (6.2)**.** *Describe all homomorphisms $\phi : \mathbb{Z}^+ \to \mathbb{Z}^+$. Determine which are injective, which are surjective and which are isomorphisms.*

Proof. For any ϕ, the image of ϕ must be either $\mathbb{Z}$ or $n\mathbb{Z}$. Since these are the only subgroups of $\mathbb{Z}^+$.

Any ϕ can be described by $\phi(1)$ since for any a in $\mathbb{Z}$ we can write $\phi(a) = \phi(\underbrace{1 + \cdots + 1}_{a \text{ times}}) = \underbrace{\phi(1) + \cdots + \phi(1)}_{a \text{ times}} = a\phi(1)$.

Each $\phi(1)$ gives a distinct homomorphism. In the case $\phi(1) \neq 0$ or 1, ϕ is injective but not surjective. Since nothing maps to 1. But each element of $\mathbb{Z}$ maps uniquely.

If $\phi(1) = 0$, ϕ is neither surjective (nothing $\mapsto 1$) nor injective (everything $\mapsto 0$).

If $\phi(1) = 1$, ϕ is the identity map so it is bijective (injective and surjective).

$\square$

Exercise (6.4)**.** *Prove that in a group, the products ab and ba are conjugate elements.*

Proof. For a, b in group G. The products ab and ba are conjugate elements if there exists an element g in G such that $ab = gbag^{-1}$. This is satisfied if we take $g = b^{-1}$. From this it follows that $ab = gbag^{-1} = b^{-1}bab = ab$ So ab and ba are conjugate elements.

$\square$

Exercise (6.7)**.** *Let H be a subgroup of G, and let g be a fixed element of G. The* conjugate subgroup *gHg^{-1} is defined to be the set of all conjugates ghg^{-1}, with h in H. Prove that gHg^{-1} is a subgroup of G.*

Proof. First, gHg^{-1} is closed in G. We see this is we take an arbitrary h in H then ghg^{-1} is in G since it is the product of elements in G which must be closed since it is a group.

Next, gHg^{-1} contains an inverse for each of its elements. Again consider h, and g, and let a be some arbitrary element in the conjugate subgroup, $a = ghg^{-1}$. Then h^{-1} must exist in H since it is a group, and it must map to some element in the conjugate subgroup, let it be $b = gh^{-1}g^{-1}$. Then a and b are inverse elements since $ab = ghg^{-1}gh^{-1}g^{-1} = ghh^{-1}g^{-1} = gg^{-1} = 1$ and $ba = gh^{-1}g^{-1}ghg^{-1} = gh^{-1}hg^{-1} = gg^{-1} = 1$. So the conjugate subgroup has its inverses.

Finally, gHg^{-1} contains the identity. Since H has an identity, then gHg^{-1} has the element $g1g^{-1} = gg^{-1} = 1$.

So gHg^{-1} is a subgroup of G.

$\square$

Exercise (6.10)**.** *Find all automorphisms of (a) a cyclic group of order* 10*. (b) the symmetric group* S_3*.*

Proof. For ϕ to be a automorphism we must have $\phi : G \to G$ and $\phi(ab) = \phi(a)\phi(b)$. This implies that for some x in ϕ, $|x| = |\phi(x)|$. Otherwise, ϕ would not be a homomorphism.

(a) Let G be the cyclic group with order $|G| = 10$ and it is generated by some element x. So $G = 1, x, x^2, \ldots x^9$. This group is completely determined by the map of $\phi(x)$, since $\phi(x^n) = \phi(x)^n$.

We know ϕ must map elements to the same order. For this to be the case $\phi(x)$ must map to elements that are coprime with the order. These are x, x^3, x^7, x^9. So there are a total of 4 possible automorphisms.

(b) First we note that ϕ must send elements to the same order. Grouping the elemnts of S_3 by order gives. Order 1 is 1. Order 2 is y, xy, x^2y. Order 3 is x and x^2. If we alter the representation of the book of S_3 it is clear that elements of order 3 can be generated by order 2.

$$\begin{array}{ccc} 1 & \to & 1 \\ y & \to & a \\ xy & \to & b \\ x^2y & \to & c \\ x & \to & ba \\ x^2 & \to & ca \end{array}$$

Since order 3 elements ba and ca are determined by order 2 elements determining $\phi(a)$, $\phi(b)$, $\phi(c)$ determines $\phi(ba)$ and $\phi(ca)$. There are 3 order 2 elements so there are $3! = 6$ different ways to map them. So we have 6 automorphisms.

□

Exercise (7.2)**.** *An equivalence relation on S is determined by the subset R of $S \times S$ consisting of those pairs (a, b) such that $a \sim b$. Write axioms for an equivalence relation in terms of the subset R.*

Proof.

Transitive If (a, b) and (b, c) are in R, then (a, c) is in R.

Symmetric If (a, b) is in R, then so is (b, a).

Reflexive If any pair of R contains a, then R contains (a, a).

□

Exercise (7.4)**.** *A relation R on the set of real numbers can be thought of a subset of the (x, y)-plane. With the notation of Exercise 7.2, explain the geometric meaning of the reflexive and symmetric properties.*

Proof.

Reflexive This implies that for every set of coordinates (x, y) in R the corresponding points (x, x) and (y, y) are also in R. And they lie on the line $x = y$.

Symmetric This implies that for every set of coordinates (x, y) in R. There is a corresponding point (y, x) which is also in R. This point is a reflection of (x, y) across the line $x = y$.

□

Exercise (8.3)**.** *Does every group whose order is a power of a prime p contain an element of order p?*

Proof. Yes. Suppose the group G is order $|G| = p^n$ where p is a prime and n is an integer.

If G contains some element a then $|a|$ must divide p^n. By Lagrange's theorem.

The subgroup generated by a must be order p, p^2, p^3, ..., p^n. If it is order p we are done. Otherwise, a is order p^i where $2 \leq i \leq n$. If $< a >$ had no subgroups then every element in it would generate $< a >$. But this is not the case since the order of a is p^i you could take any power of a less than p^i, which is not coprime to p^i, say a^{p^j}, and generate another subgroup which is smaller than $< a >$. So every group that is not of prim order has a subgroup. You could continue reducing the size of your subgroups generators by choosing an element whos order is coprime with the order untill you reach an element that is order p.

□

Exercise (8.4)**.** *Does every group of order* 35 *contain an element of order* 5*? of order* 7*?*

Proof. In this group G, consider some element a that is not the identity so $|a| \neq 1$. Let $x = |a|$. x must divide the order of G (see last problem) so it can be 5, 7, or 35.

If G contains an element a of order 35. Then a^7 and a^5 are in the group, and $(a^7)^5 = (a^5)^7 = a^{35} = 1$ so there are elements of order 5 and 7 in the group.

If G does not contain an element of order 35. Then it must contain elements of order 7 and/or 5.

If we assume there are only elements of order 5. Then each generator produces 4 unique elements. But there must be several (n) of these subgroups to fill G. But the number of elements produced by these n subgroups is $1 + 4n$ (the $+1$ is from the identity). But this cannot equal 35 so we have a contradiction.

Likewise, for a group of order 7 elements, we would need $|G| = 1 + 6n$ but this is a contradiction.

So G must have bothe order 7 and order 5 elements.

□

Exercise (8.5)**.** *A finite group contains an element x of order 10 and also an element y of order 6. What can be said about the order of G?*

Proof. By the counting theorem the least it can be is order 30. Since 30 is the LCM of 6 and 10.

□

Exercise (8.6)**.** *Let $\phi : G \to G'$ be a group homomorphism. Suppose that $|G| = 18, |G'| = 15$ and that ϕ is not the trivial homomorphism. What is the order of the kernel?*

Proof. Since $\ker \phi$ is a subgroup in G, its order must divide $|G| = 18$ so its order can be 1, 2, 3, 6, or 18.

Since $\text{im } \phi$ is a subgroup in G', its order must divide $|G'| = 15$ so its order can be 1, 3, 5, or 15.

We also know that $[G : \ker \phi] = |\text{im } \phi|$. And the counting formula applied here is $|G| = |\ker \phi|[G : \ker \phi]$. Combining these we see $|G| = |\ker \phi||\text{im } \phi|$. This constraint gives us the solution: $|\ker\ \phi| = 3$ and $|\text{im}\ \phi| = 5$.

$\square$

Pre-Lecture Problems

Exercise (5.1)**.** *Let $\phi : G \to G'$ be a surjective group homomorphism. Prove that if G is cyclic then G' is cyclic. If G is abelian then G' is abelian.*

Proof.

(a) Show G' is cyclic if G is cyclic.

Choose some b in G', since ϕ is surjective there exists some c in G such that $\phi(c) = b$. Since G is cyclic we can write $c = x^n$ where $< x >= G$ So we write

$$b = \phi(c) = \phi(x^n) = \phi(\underbrace{x \dots x}_{n \text{ times}}) = \underbrace{\phi(x) \dots \phi(x)}_{n \text{ times}} = \phi(x)^n$$

So any element in G' can be written as a power of $\phi(x)$. So G' is the cyclic group $< \phi(x) >$.

(b) Show G' is Abelian if G is Abelian.

Let a and b be elements of G'. Then since ϕ is surjective a and b correspond to some c and d in G where $a = \phi(c)$, $b = \phi(d)$. Knowing this and the fact that G is Abelian, we can write

$$ab = \phi(c)\phi(d) = \phi(cd) = \phi(dc) = \phi(d)\phi(c) = ba$$

So $ab = ba$, so G' is Abelian too.

$\square$

Exercise (6.1)**.** *Let G' be a group of real matrices of the form $\begin{pmatrix} 1 & x \\ & 1 \end{pmatrix}$. Is the map $\mathbb{R}^+ \to G'$ that sends x to this matrix an isomorphism?*

Proof. Let a and b be in $\mathbb{R}$. Then

$$\phi(a+b) = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix} \phi(a)\phi(b) = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix}$$

So ϕ is a homomorphism since $\phi(a+b) = \phi(a)\phi(b)$. To be an isomorphism, ϕ should be injective to its image. This is true if $\ker \phi = \{I_{\mathbb{R}^+}\}$. The identity element of $\mathbb{R}^+$ is 0. And clearly

$$\phi(0) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

But we must check that no other elements are in the kernel. To show this we assume there is another element, a in the kernel. So

$$\phi(a) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

But this implies $a = 0$. So $\ker \phi = \{0\}$. This implies that ϕ is injective. So ϕ is isomorphic to it's image.

□

Exercise (7.1)**.** *Let G be a group. Prove that the relation $a \sim b$ if $b = gag^{-1}$ for some g in G is an equivalence relation.*

Proof. The relation is transitive. If $a \sim b$ and $b \sim c$. Then for some g and g' in G we have $b = gag^{-1}$ and $c = g'bg'^{-1} \implies b = g'^{-1}cg'$. Combining these gives $g'^{-1}cg' = gag^{-1} \implies c = (g'g)a(g^{-1}g'^{-1})$. But $g'g$ and $g'^{-1}g^{-1}$ are elements of G since they are products of elements of G. So $a \sim c$.

The relation is symmetric. If $a \sim b$ then $b = gag^{-1}$ or $g^{-1}bg = a$ but g^{-1} and g are inverses and in G. So $b \sim a$.

The relation is reflexive. If $a \sim a$ then $a = gag^{-1}$. Which is true

So the relation is an equivalence relation.

□

Exercise (8.1)**.** *Let* H *be the cyclic subgroup of the alternating group* A_4 *generated by the permutation* (123)*. Exhibit the left and the right cosets of* H *explicitly.*

Proof. I used Python and the SymPy package to do this. Info about sympy is at sympy.org. The code is attached. The output is below. Note that the Permutations are indexed from zero, so `Permutation(0, 1, 3)` is (124). Each `PermutationGroup` is a set of permutations (not strictly a group). And `Permutation(3)` is just the identity permutation.

```
left cosets
PermutationGroup([
    Permutation(3),
    Permutation(3)(0, 1, 2),
    Permutation(3)(0, 2, 1)])
PermutationGroup([
    Permutation(1, 2, 3),
    Permutation(0, 1)(2, 3),
    Permutation(0, 2, 3)])
PermutationGroup([
    Permutation(1, 3, 2),
    Permutation(0, 1, 3),
    Permutation(0, 2)(1, 3)])
PermutationGroup([
    Permutation(0, 3, 1),
    Permutation(0, 3, 2),
    Permutation(0, 3)(1, 2)])
right cosets
PermutationGroup([
    Permutation(3),
    Permutation(3)(0, 1, 2),
    Permutation(3)(0, 2, 1)])
PermutationGroup([
    Permutation(1, 2, 3),
    Permutation(0, 2)(1, 3),
    Permutation(0, 3, 1)])
PermutationGroup([
    Permutation(1, 3, 2),
    Permutation(0, 3, 2),
    Permutation(0, 1)(2, 3)])
PermutationGroup([
    Permutation(0, 1, 3),
```

```
Permutation(0, 3)(1, 2),
Permutation(0, 2, 3)])
```

□