Abstract Algebra: Homework #4

Joel Savitz

Wednesday 17 June 2020

1 Chapter 9, Exercise A3

Suppose G_1, G_2, and G_3 are groups and let $f : G_1 \to G_2$ and $g : G_2 \to G_3$ be isomorphisms.

Theorem 1. $g \circ f : G_1 \to G_3$ *is an isomophism* $\iff G_1 \cong G_3$

Proof. Suppose $a, b \in G_1$. Then, since f is an isomorphism from G_1 to G_2, we have $f(ab) = f(a)f(b)$. Then, since g is an isomorphism grom G_2 to G_3, we have $g(f(ab)) = g(f(a))g(f(b))$ since $f(ab), f(a), f(b) \in G_2$. Since $g \circ f$ is defined as $g(f(x))$ for any $x \in G_1$, we have:

$$(g \circ f)(ab) = \big((g \circ f)(a)\big)\big((g \circ f)(b)\big) \tag{1}$$

Since the composition of two bijective functions is bijective in general, and since f and g are bijections, we have that $(g \circ f)$ is a bijeciton. This fact, along with the fact that equation 1 holds, is exactly the criteria we need to conclude that $(g \circ f)$ is an isomorphism from G_1 to G_3, or in other words, $G_1 \cong G_3$. Not only does this prove theorem 1, but this demonstrates the transitivity property of the isomorphism relation in general. □

2 Chapter 9, Exercise B3

Suppose that G_1 and G_2 are groups and $f : G_1 \to G_2$ is an isomorphism.

Theorem 2. *If* G_1 *is a cyclic group with a generator element* $a \in G_1$ *then* G_2 *is a cyclic group with a generator element* $f(a) \in G_2$.

Proof. Assume that G_2 is a cyclic group generated by $a \in G_1$. Let $n = |G_1|$. Since G_1 is generated by a, we can write G_1 as:

$$G_1 = \bigcup_{i=1}^{n} a^i \tag{2}$$

We will show by induction on i that $f(a)$ generates every element in G_2. First, consider the base case of $i = 1$. Since $f(a)^1 = f(a) \in G_2$, we have a subset of G_2 that we can write as follows:

$$\bigcup_{i=1}^{1} f(a)^i = \{f(a)\} \subseteq G_2 \tag{3}$$

Now we make the induction hypothesis that:

$$\bigcup_{i=1}^{m} f(a)^i \subseteq G_2 \tag{4}$$

holds for for some natural $m \leq n$.

Then, if we take the union of both sides of proposition 4 with $f(a)^{m+1}$, we have:

$$\bigcup_{i=1}^{m} f(a)^i \cup f(a)^{m+1} \subseteq G_2 \cup f(a)^{m+1} \tag{5}$$

$$\tag{6}$$

Which simplifies to:

$$\bigcup_{i=1}^{m+1} f(a)^i \subseteq G_2 \tag{7}$$

Since $f(a) \in G_2$ and $\Big(f(a)^m \in G_2 \wedge f(a)^{m+1} = f(a)^m f(a)\Big) \implies f(a)^{m+1} \in G_2$ by the definition of f.

By strong induction on i, we have that proposition 7 holds for any value of $m \leq n$ so it must hold for n as well.

Then we have:

$$\bigcup_{i=1}^{n} f(a)^i \subseteq G_2 \tag{8}$$

However, since the set $\bigcup_{i=1}^{n} f(a)^i$ has the same cardinality as G_2, we must have that any element in G_2 must be an element of $\bigcup_{i=1}^{n} f(a)^i$. Then, by the axiom of extensionality:

$$\left(G_2 \subseteq \bigcup_{i=1}^{n} f(a)^i\right) \wedge \left(\bigcup_{i=1}^{n} f(a)^i \subseteq G_2\right) \iff \bigcup_{i=1}^{n} f(a)^i = G_2 \tag{9}$$

We can rephrase proposition 9 by saying that $f(a)$ generates G_2.

Finally, since G_2 is generated by a single element $f(a)$, we have that G_2 is a cyclic group generated by $f(a)$. This proves theorem 2. □

3 Chapter 9, Exercise E1

Suppose $E = \{x \in \mathbb{Z} \mid \exists k \in \mathbb{Z} \ni x = 2k\}$.

Theorem 3. $\mathbb{Z} \cong E$ *with respect to addition.*

Proof. Let $f : \mathbb{Z} \to E$ such that $f(x) = 2x$. Let $a, b \in \mathbb{Z}$. We then have $f(a) = 2a$ and $f(b) = 2b$. Notice that:

$$2(a+b) = 2a + 2b \tag{10}$$
$$f(a+b) = f(a) + f(b) \tag{11}$$

Suppose that we have some $c \in \mathbb{Z}$ where $f(c) = f(a)$. Then, $2c = 2a \iff c = a$. Thus f is an injection from $\mathbb{Z}$ to E.

Suppose we have some $d \in E$. Then, by the definition of E there exists some integral p where $d = 2p$, so we have $f(p) = 2p = d$. Thus f is a surjection from $\mathbb{Z}$ to E.

Then, since f is an injection and a surjection, we have that f is a bijection.

Since f is a bijection from $\mathbb{Z}$ to E where equation 11 holds, we have that f is an isomorphism from $\mathbb{Z}$ to E with respect to addition.

Then since there exists an isomorphism from $\mathbb{Z}$ to E with respect to addition, we have that $\mathbb{Z}$ is isomorphic to E with respect to addition, i.e. $\mathbb{Z} \cong E$. This proves theorem 3. □

4 Chapter 9, Exercise F2

Suppose $G = S_3$ and $G' = \{e, a, b, ab, aba, abab\}$ where $*$ is an operation on G' and we have $a^2 = e \wedge b^2 = e \wedge bab = aba$.

For the group S_3, denote the rotations by r_1, r_2, r_3 for a rotation r_n of $\frac{2n\pi}{3}$ radians, and denote the flips about each axis of symmetry by f_1, f_2, f_3.

More precisely, denote the above permutations as follows:

$$r_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad r_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \qquad r_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \tag{12}$$

$$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \qquad f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \tag{13}$$

Then, table 1 describes the behavior of G under function composition.

$\circ$	r_3	r_1	r_2	f_1	f_2	f_3
r_3	r_3	r_1	r_2	f_1	f_2	f_3
r_1	r_1	r_2	r_3	f_3	f_1	f_2
r_2	r_2	r_3	r_1	f_2	f_3	f_1
f_1	f_1	f_3	f_2	r_3	r_2	r_1
f_2	f_2	f_1	f_3	r_1	r_3	r_2
f_3	f_3	f_2	f_1	r_2	r_1	r_3

Table 1: Operation table for G under $\circ$

By the above defining equations, table 2 is the operation table for the group G' with respect to $*$:

$*$	e	a	b	ab	aba	$abab$
e	e	a	b	ab	aba	$abab$
a	a	e	ab	b	$abab$	aba
b	b	$abab$	e	aba	ab	a
ab	ab	aba	a	$abab$	b	e
aba	aba	ab	$abab$	a	e	b
$abab$	$abab$	b	aba	e	a	ab

Table 2: Operation table for G' under $*$

Now, define the bijection $\phi : G \to G'$ as follows:

$$\begin{aligned}
r_3 &\mapsto e \\
r_1 &\mapsto ab \\
r_2 &\mapsto abab \\
f_1 &\mapsto b \\
f_2 &\mapsto aba \\
f_3 &\mapsto a
\end{aligned}$$

Then, ϕ is a one-to-one correspondence from elements of G that satsify the defining equations of G' to the elements of G' that satisfy themselves satisfy those equations:

$$\begin{aligned}
\phi(a^2) = \phi(e) = r_3 &= f_1 \circ f_1 \\
\phi(b^2) = \phi(e) = r_3 &= f_3 \circ f_3 \\
\phi(aba) = \phi(bab) = \phi(a)\phi(b)\phi(a) &= \phi(b)\phi(a)\phi(b) \\
&= f_1 \circ f_3 \circ f_1 = f_3 \circ f_1 \circ f_3 = f_2
\end{aligned}$$

Since we have a bijection between G and G' where corresponding elements satisfy the same defining equations, tables 1 and 2 are actually redudant and we can immediately conclude that $G \cong G'$

5 Chapter 9, Exercise I3

Suppose G is a group and $a \in G$

Theorem 4. $f : G \to G$ *such that* $f(x) = axa^{-1}$ *is an automorphism of* G.

Proof. Let $x, y \in G$. Then, $f(x) = axa^{-1}$ and $f(y) = aya^{-1}$. Furthermore, $f(xy) = axya^{-1}$ and $f(x)f(y) = axa^{-1}aya^{-1}$. Since $axa^{-1}aya^{-1} = axeya^{-1} = axya^{-1}$, we have:

$$f(xy) = f(x)f(y) \tag{14}$$

Now suppose that there exists some $z \in G$ where $f(z) = f(x) = axa^{-1}$. We also must have, $f(z) = aza^{-1}$ by the definition of f, so we have $aza^{-1} =$

axa^{-1}. Multiplying both sides of that on the right by a gives us $az = ax$, and multiplying both sides of that on the left by a^{-1} gives us $z = x$. Therefore, f is injective.

Let d be some element of G and let $p = a^{-1}da$. Notice that $f(p) = aa^{-1}daa^{-1} = ede = d$, therefore g is surjective.

Since f is injective and surjective, it is bijective, and since f is a bijection that satisfies equation 14, we have that f is an isomorphism from G to itself, or in other words, f is an automorphism of G. This proves theorem 4. $\square$

6 Chapter 10, Exercise B2

Let $10 \in \mathbb{Z}_{25}$

Consider the following equation:

$$\sum_{i=1}^{n} 10 = 0 \tag{15}$$

Since the first natural number that satisfies equation 15 is 25, we have that $\text{ord}(10) = 25$.

7 Chapter 10, Exercise B3

Let $6 \in \mathbb{Z}_{16}$

Consider the following equation:

$$\sum_{i=1}^{n} 6 = 0 \tag{16}$$

Since the first natural number that satisfies equation 16 is 24, we have that $\text{ord}(6) = 24$.

8 Chapter 10, Exercise C4

Suppose G is a group with operator $*$ and $a, b \in G$

Theorem 5. $\text{ord}(a) = \text{ord}(bab^{-}1)$

Proof. Let $n = \text{ord}(a)$. Then, $a^n = e$. Consider the product:

$$\prod_{i=1}^{n} bab^{-1} = \underbrace{bab^{-1}bab^{-1}...bab^{-1}}_{n \text{ times}} \tag{17}$$

Since each $b^{-1}b$ in equation 17 can be replaced with e, we can rewrite it like so:

$$\prod_{i=1}^{n} bab^{-1} = b\underbrace{aa..a}_{n \text{ times}}b^{-1} = ba^nb^{-1} \tag{18}$$

Then, since $a^n = e$, we have:

$$\prod_{i=1}^{n} bab^{-1} = e \tag{19}$$

Now suppose there exists some $m \leq n$ where:

$$\prod_{i=1}^{m} bab^{-1} = e \tag{20}$$

Then:

$$\prod_{i=1}^{m} bab^{-1} = b\underbrace{aa..a}_{m \text{ times}}b^{-1} = e \tag{21}$$

$$ba^mb^{-1} = e \tag{22}$$

$$ba^m = e \tag{23}$$

$$a^m = e \iff m = n \tag{24}$$

Thus n is the smallest integer such that $(bab^{-1})^n = e$ so $\text{ord}(bab^{-1}) = n$ and finally $\text{ord}(a) = \text{ord}(bab^{-1})$. This proves theorem 5.

□

9 Chapter 10, Exercise C5

Suppose G is a group with operator $*$ and $a \in G$

Theorem 6. $\text{ord}(a) = \text{ord}(a^{-1})$

Proof. Let $\mathfrak{n} = \text{ord}(a)$. Then, we have $a^n = \underbrace{aa..a}_{n \text{ times}} = e$. Now consider exponentiation of a^{-1}. We have in general that $(a^{-1})^m = (a^m)^{-1}$ for some integer m. Therefore, $(a^{-1})^n = (a^n)^{-1} = e^{-1} = e$. There is no other smaller positive integer that satisfies $a^n = e$ by the definition of the order of an element of a group, therefore $\text{ord}(a^{-1}) = n$ and $\text{ord}(a) = \text{ord}(a^{-1})$. This proves theorem 6. □

10 Chapter 10, Exercise D5

Supose G is a group with an element a that has finite order.

Let n, r, s be some integers.

Theorem 7. $\text{ord}(a) = n \wedge a^r = a^s \implies \exists k \in \mathbb{Z} \ni nk = r - s$ *i.e.* n *is a factor of* $r - s$.

Proof. First we note that $n > 0$ must hold since $\text{ord}(a) = n$ only holds when n is positive. Since $r, s, n \in \mathbb{Z} \wedge n > 0$, we can apply the division algorithm. Let p, q be the unique integers such that $r = np + q$ and $0 \leq q < n$ and let x, y be the unique integers such that $s = nx + y$ and $0 \leq y < n$. Then:

$$r - s = (np + q) - (nx + y) = n(p - x) + (q - y) \tag{25}$$

So we have:

$$\begin{aligned}
a^r &= a^s \\
a^{np+q} &= a^{nx+y} \\
a^{np}a^q &= a^{nx}a^y \\
(a^n)^p a^q &= (a^n)^x a^y \\
e^p a^q &= e^x a^y \\
a^q &= a^y
\end{aligned}$$

Since $0 \leq q < n \wedge 0 \leq y < n$, we must have that $q = y$ and then we can simpify equation 25:

$$r - s = n(p - x) \tag{26}$$

Since $(p - x) \in \mathbb{Z}$, we have some integer $z = p - x$ such that $nz = r - q$, or in other words, n is a factor of $r - s$. This proves theorem 7. □

11 Isomorphism involving some matricies

Suppose we have the following matrices:

$$I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \quad B = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \tag{27}$$

$$C = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad D = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \quad E = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \tag{28}$$

Define the set $G = \{I, A, B, C, D, E\}$. Define the operation $*$ on G as $A * B = BA$

Then, table 3 is the operation table for G.

$*$	I	D	E	A	B	C
I	I	D	E	A	B	C
D	D	E	I	C	A	B
E	E	I	D	B	C	A
A	A	C	B	I	E	D
B	B	A	C	D	I	E
C	C	B	A	E	D	I

Table 3: Operation table for G under $*$

Then, utilizing the notation defined by equations 12 and 13 in section 4 and considering table 1, define the bijection $\psi : S_3 \to G$ as follows:

$$\begin{aligned} r_3 &\mapsto I \\ r_1 &\mapsto D \\ r_2 &\mapsto E \\ f_1 &\mapsto A \\ f_2 &\mapsto B \\ f_3 &\mapsto C \end{aligned}$$

We can see by inspection of tables 1 and 3 that ψ is an isomorphism from S_3 to G, therefore $S_3 \cong G$.

12 Find the order

Suppose $1 \in \mathbb{R}^*$

Then, $1^1 = e$ since $1 = e$, therefore $\text{ord}(1) = 1$ with respect to multiplication.

Now suppose $1 \in \mathbb{R}$.

Consider the following equation:

$$\sum_{i=1}^{n} 1 = 0 \tag{29}$$

There is no value of n that will satisfy this equation, therefore $\text{ord}(1) = \infty$, i.e. 1 has infinite order with respect to addition.

13 Find the order again

Suppose $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in GL_2(\mathbb{R})$.

Consider the following equation:

$$\prod_{i=1}^{n} A = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \tag{30}$$

Since n never has the value 0, there does not exist a positive value of n such that the right hand side of equation 30 is $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

Therefore, $\text{ord}(A) = \infty$, i.e. A has infinite order.

14 Find the order yet again

Suppose $f(x) = \frac{1}{1-x} \in S_A$ where $A = \mathbb{R} - \{0, 1\}$

We want to find $\text{ord}(f)$, i.e the smallest positive integer such that $f^n(x) = e$, — where e is the identity function — or infinity if such a numer does not exist.

First, we find $f^2(x)$:

$$\frac{1}{1-\frac{1}{1-x}} \tag{31}$$
$$\frac{1}{\frac{1-x-1}{1-x}} \tag{32}$$
$$\frac{1}{\frac{-x}{1-x}} \tag{33}$$
$$\frac{1-x}{-x} \tag{34}$$
$$\frac{x-1}{x} \tag{35}$$
$$1-\frac{1}{x} \tag{36}$$

Then, we plug out simplified $f^2(x)$ back into f and simplify to find $f^3(x)$:

$$\frac{1}{1-(1-\frac{1}{x})} \tag{37}$$
$$\frac{1}{\frac{1}{x}} \tag{38}$$
$$x \tag{39}$$

Therefore $f^3(x) = x$ and then by inspection, we have $\mathrm{ord}(f) = 3$.

15 Subgroup problems

This problem contains three subproblems. I have divided these among the following three subsections.

15.1 Permutations

Suppose $G_1 = \{f \in S_{\mathbb{R}} \mid f(x) = ax + b \ni a \neq 0 \wedge a, b \in \mathbb{R}\}$

Theorem 8. G_1 *is a subgroup of* $S_{\mathbb{R}}$ *with respect to function composition.*

Proof. Let $f, g \in G_1$ such that $f(x) = ax + b$ for some nonzero real a and some real b and $g(x) = cx + d$ for some nonzero real c and some real d Then, we have $(g \circ f)(x) = g(f(x)) = c(ax+b)+d = cax+(cb+d)$. Since $c \neq 0 \neq a \implies ca \neq 0$ and $ca \in \mathbb{R}$ as well as $(cb + d) \in \mathbb{R}$, we have that $(g \circ f)(x) \in G_1$, therefore G_1 is closed under $\circ$.

Let $h(x) = a^{-1}x + (-ba^{-1})$. a^{-1} is defined since $a \neq 0$ and $a^{-1} \in \mathbb{R} \wedge -ba^{-1} \in \mathbb{R} \implies h(x) \in G$. Then, we see that:

$$\begin{aligned}
(h \circ f)(x) &= a^{-1}(ax + b) + -ba^{-1} \\
&= x + ba^{-1} - ba^{-1} \\
&= x \\
(f \circ g)(x) &= a(a^{-1}x + -ba^{-1}) + b \\
&= x + -b + b \\
&= x
\end{aligned}$$

Since $(f \circ h)(x) = (h \circ f)(x) = x \in G_1$ is the identity function, we have that the identity of $S_{\mathbb{R}}$ is in G_1 and also that $h(x) = f^{-1}(x)$, so it follows that every element in G_1 has its inverse in G_1.

Finally, since G_1 is a closed with respect to $\circ$ and since every element in G_1 has its inverse in G_1, we have that G_1 is a subgroup of $S_{\mathbb{R}}$. This proves theorem 8. $\square$

15.2 The General Linear Group

Suppose $G_2 = \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \in GL_2(\mathbb{R}) \mid a \neq 0 \right\}$

Theorem 9. *G_2 is a subgroup of $GL_2(\mathbb{R})$ with respect to matrix multiplication.*

Proof. Let $A = \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} c & d \\ 0 & 1 \end{bmatrix}$ be two elements of G_2.

Then, we see that $AB = \begin{bmatrix} ac & ad + b \\ 0 & 1 \end{bmatrix}$. Since $a \neq 0 \neq c \implies ac \neq 0$ and since $ad \in \mathbb{R} \wedge ad + b \in reals$, we must have that $AB \in G_2$ by its definition. Therefore, G_2 is closed under matrix multiplication.

Let $C = \frac{1}{a1-b0}\begin{bmatrix} 1 & -b \\ -0 & a \end{bmatrix} = \begin{bmatrix} a^{-1} & -ba^{-1} \\ 0 & 1 \end{bmatrix}$, then, we can see by inspection that $C \in G_2$. We then have $CA = AC = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I \in G_2$, so we also have that $C = A^{-1}$ and that $e = I$, the identity of $GL_2(\mathbb{R})$, is in G_2.

Finally, since G_2 is a closed with respect to matrix multiplication and since every element in G_2 has its inverse in G_2, we have that G_2 is a subgroup of $GL_2(\mathbb{R})$. This proves theorem 9.

□

15.3 Isomorphism

Define the function $T : G_1 \to G_2$ as $T(f) = \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$ where G_1 and G_2 denote the same groups as in subsections 15.1 and 15.2 and $f \in G_1$ is some $f(x) = ax + b$ for some nonzero real a and some real b.

Theorem 10. $G_1 \cong G_2$

Proof. Let $f, g \in G_1$ be such that $f(x) = ax + b$ and $g(x) = cx + d$ where $a, b, c, d \in \mathbb{R} \wedge a \neq 0 \neq c$.

Then, $T(f) = \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \wedge T(g) = \begin{bmatrix} c & d \\ 0 & 1 \end{bmatrix}$. We see that $T(f)T(g) = \begin{bmatrix} ac & ad + b \\ 0 & 1 \end{bmatrix}$, and also that $T(f \circ g) = T((ac)x + (ad + b)) = \begin{bmatrix} ac & ad + b \\ 0 & 1 \end{bmatrix}$, therefore:

$$T(f \circ g) = T(f)T(g) \tag{40}$$

Let $h \in G_1$ be defined as $h(x) = px + q$ for some $a, b \in \mathbb{R} \ni a \neq 0$ such that $T(h) = T(f)$. Then, we must have:

$$\begin{bmatrix} p & q \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \iff p = a \wedge q = b \tag{41}$$

Therefore $h = f$ and T is injective.

Let $Q = \begin{bmatrix} y & z \\ 0 & 1 \end{bmatrix}$ for some nonzero real y and some real z. We can see by inspection that $Q \in G_2$, and we can construct a $\phi \in G_1$ where $\phi(x) = yx + z$ and it is readily apparent that $T(\phi) = Q$. Therefore T is surjective.

Since T is injective and surjective, it is bijective. Then, since T is a bijection that satisfies equation 40, T is an isomorphism from G_1 to G_2. Finally, since there exists some isomorphism from G_1 to G_1, we have that G_1 is isomorphic to G_2, or $\mathsf{G}_1 \cong \mathsf{G}_2$. This proves theorem 10.

$\square$