Abstract Algebra: Homework #2

Joel Savitz

Wednesday 3 June 2020

Note: for the scope of this document, let $\ni$ denote "such that".

1 Chapter 4, Exercise A4

Suppose some $\{a, b, c, x\} \subseteq G$ for a group G with operation $*$.

Furthermore, suppose we have $ax^2 = b \wedge x^3 = e$.

Then, by the following logic:

$$\begin{aligned} ax^2 * x &= b * x && (1)\\ ax^3 &= bx && (2)\\ ae &= bx && (3)\\ b^{-1} * a &= b^{-1} * bx && (4)\\ b^{-1}a &= x && (5)\\ & && (6) \end{aligned}$$

We have that $x = b^{-1}a$.

2 Chapter 4, Exercise B2

Theorem 1. *For an arbitrary group G with operation $*$, it is not the case that $x^2 = a^2 \implies x = a$ for an arbitrary $x, a \in G$.*

Proof. Suppose G and $*$ are defined as on page 28 of Pinter. Then, the following counterexample proves theorem 1:

Counterexample 1.

$$\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$$
$$\wedge \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} \neq \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$$

This proves theorem 1. □

3 Chapter 4, Exercise B4

Theorem 2. *For an arbitrary group G with operation $*$, we have that $x^2 = x \implies x = e$.*

Proof. Suppose some $x \in G \ni x^2 = x$ where G is some group. Since $x*x = x$, we have that both right multiplication of x by x and left multiplication of x by x map to x and so x exactly fufills the definition of an identity element so we must have that x is in fact the identity element. Then, we have $x^2 = x \implies x = e$. This proves theorem 2. □

4 Chapter 4, Exercise B6

Theorem 3. *For an arbitrary group G with operation $*$, we have that:*

$$(\forall x, y \in G)(\exists z \in G \ni y = xz) \tag{7}$$

Proof. Suppose some $x, y \in G$. where G is some group. Then, let $z = x^{-1}y \in G$. Since G is closed under $*$ and since every element of a group has an inverse, we have some $y = xz = x(x^{-1}y) = (x^{-1}x)y = ey$. Then, we have $(\forall x, y \in G)(\exists z \in G \ni y = xz)$. This proves theorem 3. □

5 Chapter 4, Exercise C6

Theorem 4. *Some $a, b \in G$ — where G is some group — commute (i.e. $ab = ba$) if and only if for any $a, b \in G$, we have $aba^{-1} = b$.*

Proof. Suppose we have some $a, b \in G \ni ab = ba$. If we multiply each side on the right by a^{-1}, we have $aba^{-1} = b$. So we have:

$$(\forall a, b \in G)(ab = ba \implies aba^{-1} = b) \tag{8}$$

In the other direction, suppose we have some $a, b \in G \ni aba^{-1} = b$. If we multiply each side on the right by a, we have $ab = ba$. So we have:

$$(\forall a, b \in G)(aba^{-1} = b \implies ab = ba) \tag{9}$$

Finally, since we have propositions 8 and 9, we have the implication in both directions:

$$(\forall a, b \in G)(ab = ba \iff aba^{-1} = b) \tag{10}$$

This proves theorem 4. □

6 Chapter 4, Exercise D1

Theorem 5. *For any $a, b \in G$, where G is some group, we have $ab = e \implies ba = e$.*

Proof. Suppose we have some $ab = e$ for an arbitarary $a, b \in G$ and the identity e of G. Then, multiplying both sides on the left by a^{-1} gives us $b = a^{-1}$. Multiplying both sides of that result on the right by b^{-1} gives us $e = a^{-1}b^{-1}$. Since two elements are equal if and only if their inverses are equal, we have $e^{-1} = e = ba = (a^{-1}b^{-1})^{-1}$ since for any $x, z \in G$ we have $(xz)^{-1} = z^{-1}x^{-1}$. Then, we have that $ab = e \implies ba = e$ for any $a, b \in G$. This proves theorem 5. □

7 Chapter 4, Exercise D6

Theorem 6. *For any $a, b, c \in G$, where G is some group, we have:*

$$(abc)(abc) = e \implies \Big(\big((bca)(bca) = e\big) \wedge \big((cab)(cab) = e\big)\Big) \tag{11}$$

In other words, if some (abc) is it's own inverse, then both (bca) and (cab) are their own inverses.

Proof. Suppose we have some $a, b, c \in G$ where $(abc)(abc) = e$, that is to say, (abc) is its own inverse. In other terms, we have:

$$(abc) = (abc)^{-1} = c^{-1}b^{-1}a^{-1} \tag{12}$$

If we multiply the far left and far right of equation 12 on the right by a gives us $abca = c^{-1}b^{-1}$, then multiplying both sides of that result on the left by a^{-1} gives us $bca = a^{-1}c^{-1}b^{-1} = (bca)^{-1}$. So, we have that if some (abc) is its own inverse, then (bca) is its own inverse.

Alternatively, if we multiply the far left and far right of equation 12 on the left by c gives us $cabc = b^{-1}a^{-1}$, then multiplying both sides of that result on the right by c^{-1} gives us $cab = b^{-1}a^{-1}c^{-1} = (cab)^{-1}$. So, we have that if some (abc) is its own inverse, then (cab) is its own inverse.

Thus, we have that if some (abc) is it's own inverse, then both (bca) and (cab) are their own inverses. This proves theorem 6 □

8 Chapter 4, Exercise H2

Theorem 7. *For any $a, b \in G$ and $n \in \mathbb{Z}$, where G is some group, and n is positive, we have:*

$$ab = ba \implies (ab)^n = a^n b^n \tag{13}$$

Proof. We will prove theorem 7 by induction on n.

Let a and b be any two elements in some group G such that $ab = ba$,

First, we consider the base case and let $n = 1$. Then, almost trivially, we have $(ab)^1 = (ab) = ab = a^1b^1$.

Now, we will assume that $ab = ba \implies (ab)^n = a^n b^n$ for some positive integer n. We multiply both sides of the consequent of our induction hypothesis on the right by (ab) to get:

$$(ab)^{n+1} = (ab)^n * (ab) = a^n b^n * (ab) \tag{14}$$

Since a and b are associative in general and commutative in particular, we

have:

$$\begin{aligned} a^n b^n (ab) &= a^n b^{n-1} ab^2 && (15)\\ &= a^n b^{n-2} ab^3 && (16)\\ &... && (17)\\ &= a^n bab^n && (18)\\ &= a^n abb^n && (19)\\ &= a^{n+1} b^{n+1} && (20)\\ & && (21) \end{aligned}$$

by repeatedly applying the identity $ab = ba$.

Then we have that the following implication holds for some positive integer n:

$$\Bigg(ab = ba \implies (ab)^n = a^n b^n\Bigg) \implies \Bigg(ab = ba \implies (ab)^{n+1} = a^{n+1} b^{n+1}\Bigg) \tag{22}$$

Finally, by mathematical induction, we conclude that:

$$(\forall a, b \in G)(\forall n \in \mathbb{Z} \ni n > 0)(ab = ba \implies (ab)^n = a^n b^n) \tag{23}$$

This proves theorem 7 □

9 Chapter 5, Exercise B4

Let $\mathcal{C}(\mathbb{R})$ denote the set of all continuous functions from $\mathbb{R}$ to $\mathbb{R}$.

Supoose we have a group G defined by $\langle \mathcal{C}(\mathbb{R}), + \rangle$ and some set H defined such that $H = \{f \in \mathcal{C}(\mathbb{R}) \ni \int_0^1 f(x)dx = 0\}$.

Theorem 8. *H is a subgroup of G.*

Proof. First, we observe that the identity of G is $f(x) = 0$. Since $\int_0^1 0dx = 0$, $(f(x) = 0) \in H$. Now, suppose we have some $f, g \in H$. Then, $\int_0^1 f(x)dx = \int_0^1 g(x)dx = 0$ by the definition of H. Since integration is a linear operator, we have that $\int_0^1 f(x)dx + \int_0^1 g(x)dx = \int_0^1 \big(f(x) + g(x)\big)dx = 0$. Since $f + g \in H$, we have that H is closed under $+$.

Now consider that f^{-1} is simply some $(h(x) = -f(x)) \in G$ since $f(x) + (-f(x)) = 0$ for any real x. If $\int_0^1 f(x)dx = 0$ then:

$$-\int_0^1 f(x)dx = \int_0^1 -f(x)dx \tag{24}$$

$$= \int_0^1 f^{-1}(x)dx \tag{25}$$

$$= -0 = 0 \tag{26}$$

$$\tag{27}$$

so $f^{-1} \in H$ and any $f \in H \implies f^{-1} \in H$.

Finally, since $H \subseteq G$ is closed under $+$, any $f \in H \implies f^{-1} \in H$, and (trivally for a non-empty subset of G) the identity of G is also in H, we conclude that H is a subgroup of G. This proves theorem 8. □

10 Chapter 5, Exercise C2

Suppose we have some Abelian group G with an operation $*$ and some invariant $n \in \mathbb{Z} \ni n > 0$.

Let $H = \{x \in G \ni x^n = e\}$.

Theorem 9. *H is a subgroup of G.*

Proof. Suppose a and b are two elements of H. Since G is an Abelian group, we have $ab = ba$. by theorem 7, we have that

$$ab = ba \implies (ab)^n = a^n b^n \tag{28}$$

for any positive integer n. Since G is an Abelian group, commutivity holds in general, therefore the consequent of proposition 28 must hold in general.

By the definition of H, we must have $a^n = b^n = e$, and by the consequent of proposition 28 we also have $a^b b^n = (ab)^n = e$. Then since $(ab)^n = e$, we must have — by the definition of H — that $ab \in H$. Then, we have that H is closed under $*$.

Now we consider inverses. Since $a^n = (aa...a) = e$, we must have:

$$\begin{aligned}(a^n)^{-1} &= (aa...a)^{-1} && (29)\\ &= a^{-1}a^{-1}...a^{-1} && (30)\\ &= (a^{-1})^n && (31)\\ &= e = e^{-1} && (32)\\ & && (33)\end{aligned}$$

Then, since $(a^{-1})^n = e$, we must — again by the definition of H — have that $a^{-1} \in H$. Therefore, we have $x \in H \implies x^{-1} \in H$ for any $x \in H$, so every element of H has its inverse in G under $*$ in H as well.

As a trival side note, since G is closed under $*$ and since every element of H has an inverse in H, we have some $q \in H$ where $q^{-1}q = e \in H$, so the identity of G under $*$ is indeed in H.

Finally, since $H \subseteq G$ is closed under $*$, any $a \in H \implies a^{-1} \in H$, and the identity of G is also in H, we conclude that H is a subgroup of G. This proves theorem 9. □

11 Chapter 5, Exercise D1

Let G be some group with an operation $*$ and let H and K be two arbitarary subgroups of G.

Theorem 10. *$H \cap K$ is a subgroup of G*

Proof. Suppose some a and b are elements of M. Then, $a, b \in H \wedge a, b \in K$.

Since H and K are subgroups, they are both closed under $*$. Therefore we have: $ab \in K \wedge ab \in H$.

By the definition of set intersection, we have $x \in H \cap K \iff x \in H \wedge x \in K$. Then, since we have $ab \in K \wedge ab \in H$. we must also have $ab \in H \cap K$, so $H \cap K$ is closed under $*$.

Since H and K are subgroups, the truth of the proposition that some element is in either set implies that its inverse must also be in that set.

Then, since if any $a \in H \cap K$ then $a^{-1} \in H \wedge a^{-1} \in K \iff a^{-1} \in H \cap K$. So every element of $H \cap K$ has its inverse in $H \cap K$.

Of course, this implies that the identity of G must also be in $H \cap K$, since $a * a^{-1} = e$ and $H \cap K$ is closed under $*$.

Finally, since $H \cap K \subseteq G$ is closed under $*$, since $a \in H \cap K \implies a^{-1} \in H \cap K$, and since the identity of G is in $H \cap K$, we conclude that $H \cap K$ is a subgroup of G.

This proves theorem 10. □

12 Chapter 5, Exercise D3

Suppose we have some group G with an operation $*$.

Define the *center* of group G as some $C = \{x \in G \ni (\forall y \in G)(xy = yx)\}$, the largest possible commutative subset of G.

For the scope of this answer, let us denote the center of a group G with C.

Theorem 11. *C is a subgroup of G*

Proof. Suppose some $a, b \in C$ and $c \in G$ Then observe the following iterative application of the associative and commutative properties of C:

$$\begin{aligned}
(ab)c &= a(bc) && (34)\\
&= a(cb) && (35)\\
&= (ac)b && (36)\\
&= (ca)b && (37)\\
&= c(ab) && (38)\\
& && (39)
\end{aligned}$$

Then, for any $x, y \in C$, xy commutes with an arbitary $z \in G$, so $xy \in C$ by definition and C is closed under $*$.

Now, suppose some $d \in G$. We manipulate the commutative identity of $ad = da$ using the associative and commutative properties of C as adove. Then observe, with justification on the left:

$$\begin{aligned}
ad &= da && (\text{ initial identity }) && (40)\\
(ad)^{-1} &= (da)^{-1} && (a = b \implies a^{-1} = b^{-1}) && (41)\\
d^{-1}a^{-1} &= a^{-1}d^{-1} && ((ab)^{-1} = b^{-1}a^{-1}) && (42)\\
a^{-1} &= da^{-1}d^{-1} && (a = b \implies ca = cb) && (43)\\
a^{-1}d &= da^{-1} && (a = b \implies ac = bc) && (44)\\
& && && (45)
\end{aligned}$$

By this logic we see that if we have some a that commutes with any $x \in G$ we then also have that a^{-1} commutes with that same x, so for any $a \in C$, we indeed have that $a^{-1} \in C$ since a^{-1} commutes with any element of G which is the definition of set membership in C.

Then every element of C has its inverse in C

Additionally, the identity of G must also be in C, since $a * a^{-1} = e$ and C is closed under $*$.

Finally, since $C \subseteq G$ is closed under $*$, since $a \in C \implies a^{-1} \in C$, and since the identity of G is in C, we conclude that C is a subgroup of G.

This proves theorem 11. □

13 Cyclic subgroups of $\langle \mathbb{Z}_8, + \rangle$

The following is a list of all cyclic subgroups of $\langle \mathbb{Z}_8, * \rangle$. I have included the generator elements in parentheses following the subgroup.

$$\{0\}\ (\langle 0 \rangle) \tag{46}$$
$$\{0, 4\}\ (\langle 4 \rangle) \tag{47}$$
$$\{0, 2, 4, 6\}\ (\langle 2 \rangle, \langle 6 \rangle) \tag{48}$$
$$\{0, 1, 2, 3, 4, 5, 6, 7\}\ (\langle 1 \rangle, \langle 5 \rangle, \langle 7 \rangle, \langle 3 \rangle) \tag{49}$$
$$\tag{50}$$

14 An operation table

Suppose we have some group G and an operation $*$ where $G = \{e, a, b, ab, ba, aba\}$ with identity e and we have $a^2 = e \wedge b^2 = e \wedge (ab)^2 = ba$. Then, table 1 is the operation table for G under $*$

$*$	e	a	b	ab	ba	aba
e	e	a	b	ab	ba	aba
a	a	e	ab	b	aba	ba
b	b	ab	e	aba	a	ab
ab	ab	aba	a	ba	e	b
ba	ba	b	aba	e	ab	a
aba	aba	ab	ba	a	b	e

Table 1: Operation table for G under $*$

15 Proof of group operator bijection

Suppose with have some finite group G with an operation $*$.

Theorem 12. *In the operation table for G, no element of G appears more than once per row nor does an element of G appear more than once per column.*

Proof. Let a, b, c and d be some arbitrary elements of G.

Define the following functions $*_a : G \to G \ni *_a(b) = *(a, b)$ and $*'_a : G \to G \ni *'_a(b) = *(b, a)$. These functions contain the mappings of the elements of the group G to the corresponding row and column, respectively, in the operation table of G that contains the results of multiplying a and b

Another way to state theorem 12 is that the functions $*_a$ and $*'_a$ map each element of G to a unique element G since this means, by the definitions of $*_a$ and $*'_a$ that each element of G appears in each row and column no more than once.

Now suppose that $d = *_a(b) \wedge d = *_a(c)$ holds. Then, by the definition of $*_a$, we have $d = ab \wedge d = ac$. Then, $ab = ac$. We multiply both sides on the left by a^{-1} to get $b = c$. Then, we must have that $*_a$ maps each element of G to a unique element of G, for if we assume that it maps two elements to a single value we have that those two elements must be equal. So, each

element of G appears in the row of the operation table corresponding to a no more than once.

Alternatively suppose that $d = *'_a(b) \wedge d = *'_a(c)$ holds. Then, by the definition of $*'_a$, we have $d = ba \wedge d = ca$. Then, $ba = ca$. We multiply both sides on the right by a^{-1} to get $b = c$. Then, we must have that $*'_a$ maps each element of G to a unique element of G, by the same logic as we used for $*_a$. So, each element of G appears in the column of the operation table corresponding to a no more than once.

Finally, since we have both statements individually for an arbitarary $a \in G$, we must then have in general any element of G appears in any row or column of the operation table for G no more than once.

This proves theorem 12.

□

16 Proof of subgroup

Let $G = \{A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathbb{R}^{2\times 2} \ni \exists A^{-1} \in \mathbb{R}^{2\times 2} \ni AA^{-1} = A^{-1}A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\}$ be the group of invertible 2x2 matrices with $*$ denoting the operation of matrix multiplication.

Suppose that $S = \{x \in G \ni det(x) = 1\}$.

Theorem 13. *S is a subgroup of G.*

Proof. We know from linear algebra that the product of the determinant of any two matrices is the deternimant of the matrix product of those matrices, or in the specific case of G, we have:

$$\Big(\forall x, y \in G\Big)\Big(det(x) \cdot det(y) = det(x * y)\Big) \tag{51}$$

Now let a and b be some elements of S. By the definition of s, $det(a) = det(b) = 1$ so we must have by equation 51 that

$$\begin{aligned} det(a * b) =& det(a) \cdot det(b) && (52)\\ det(a * b) =& 1 \cdot 1 && (53)\\ det(a * b) =& 1 && (54)\\ & && (55) \end{aligned}$$

Then, $a * b \in S$, so we have in general that S is closed under $*$.

Another useful finding of linear algebra is that the determinant of the matrix inverse of some matrix is the inverse of the determinant of that matrix.

In symbolic terms with respect to the elements of G:

$$\Big(\forall x \in G\Big)\Big(det(x^{-1}) = \frac{1}{det(x)}\Big) \tag{56}$$

which reduces to equation 57 when we substitute 1 for $det(x)$

$$\Big(\forall x \in G\Big)\Big(det(x^{-1}) = 1\Big) \tag{57}$$

Then since for any $x \in S$ we have $det(x^{-1}) = 1$ and then by the definition of S, we also have that $x^{-1} \in S$, we must have in general that $a \in S \implies a^{-1} \in S$.

Since $det\left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right) = 1$, we have that the identity of G is in S.

Finally, since $S \subseteq G$ is closed under $*$, since $a \in S \implies a^{-1} \in S$, and since the identity of G is in S, we conclude that S is a subgroup of G.

This proves theorem 13. □

17 Endnote

This concludes my response to the second abstract algebra homework assignment. Did you like the formatting?