Abstract Algebra: Homework #8

Joel Savitz

Wednesday 15 July 2020

1 Chapter 15, Exercise A1

Suppose $G = \mathbb{Z}_{10} \wedge H = \{0, 5\}$.

Then, table 1 describes the operation table for G/H with respect to coset multiplication defined for cosets of an abelian group, denoted $*$.

I exclusively use multiplicative notation here because I like it better, but $aH \ni a \in G$ denotes the coset $a +_{10} H$. Since G is abelian, I use left and right cosets interchangably.

The following are the elements of G/H:

$$\begin{aligned} H0 &= \{0, 5\} \\ H1 &= \{1, 6\} \\ H2 &= \{2, 7\} \\ H3 &= \{3, 8\} \\ H4 &= \{4, 9\} \end{aligned}$$

$*$	H0	H1	H2	H3	H4
H0	H0	H1	H2	H3	H4
H1	H1	H2	H3	H4	H0
H2	H2	H3	H4	H0	H1
H3	H3	H4	H0	H1	H2
H4	H4	H0	H1	H2	H3

Table 1: Operation table for G/H under $*$

If we replace each HX in the table with an $\mathsf{f(HX)}$ where $\mathsf{f}: \mathsf{G/H} \to \mathbb{Z}_5 \ni \mathsf{f(HX)} = \mathsf{X}$ and replace $*$ by $+_5$, we construct the operation table for $\mathbb{Z}_5$. By table inspection, this f is an isomorphism from $\mathsf{G/H}$ to $\mathbb{Z}_5$, so clearly $\mathsf{G/H} \cong \mathbb{Z}_5$.

2 Chapter 15, Exercise A4

Denote the elements of D_4 as:

$$R_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \quad R_{\pi/2} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \quad R_\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \quad R_{3\pi/2} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \tag{1}$$

$$H = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \quad V = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \quad D = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \quad D' = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \tag{2}$$

The operation table for function composition $\circ$ on D_4 is given in table 1

$\circ$	R_0	$R_{\pi/2}$	R_π	$R_{3\pi/2}$	H	V	D	D'
R_0	R_0	$R_{\pi/2}$	R_π	$R_{3\pi/2}$	H	V	D	D'
$R_{\pi/2}$	$R_{\pi/2}$	R_π	$R_{3\pi/2}$	R_0	D'	D	H	V
R_π	R_π	$R_{3\pi/2}$	R_0	$R_{\pi/2}$	V	H	D'	D
$R_{3\pi/2}$	$R_{3\pi/2}$	R_0	$R_{\pi/2}$	R_π	D	D'	V	H
H	H	D	V	D'	R_0	R_π	$R_{\pi/2}$	$R_{3\pi/2}$
V	V	D'	H	D	R_π	R_0	$R_{3\pi/2}$	$R_{\pi/2}$
D	D	V	D'	H	$R_{3\pi/2}$	$R_{\pi/2}$	R_0	R_π
D'	D'	H	D	V	$R_{\pi/2}$	$R_{3\pi/2}$	R_π	R_0

Table 2: Operation table for D_4 under $\circ$

Now that we have better notation than Pinter, let $G = D_4 \land H \leq G \ni H = \{R_0, R_\pi, H, V\}$

Note that other than H, G/H contains only one other element since $(G : H) = 2$.

We can then fully describe $G/H = \Big\{\{R_0, R_\pi, H, V\}, \{R_{\pi/2}, R_{3\pi/2}, D, D'\}\Big\}$.

Table 3 give the operation table for G/H under coset multiplication:

$*$	H	HD
H	H	HD
HD	HD	H

Table 3: Operation table for G/H under coset multiplication

3 Chapter 15, Exercise C1

Suppose $H \trianglelefteq G$ where G is a group.

Theorem 1. $(\forall x \in G)(x^2 \in H) \iff (\forall X \in G/H)(X^2 = H)$

Proof. Suppose that $(\forall x \in G)(x^2 \in H)$. Let $X \in G/H$. Then, $X = Hx \ni x \in G$. Therefore, $XX = (Hx)(Hx) = H(x^2) = H$ since $x^2 \in H \implies h(x^2) \in H$ for any $h \in H$ since H is closed under the group operation. Then, $(\forall X \in G/H)(X^2 = H)$.

Conversely, suppose $(\forall X \in G/H)(X^2 = H)$. Let $x \in G$ and let $X = Hx$. Then, $X^2 == (Hx)(Hx) = Hx^2$. By assumption, $X^2 = Hx^2 = H$, and by Pinter chapter 15 theorem 5 part 2, we have $Hx^2 = H \iff x^2 \in H$.

The first implication and its converse thus proved demostrates bidirecitonal implication. This proves theorem 1. $\square$

4 Chapter 15, Exercise D1

Suppose $H \trianglelefteq G$ where G is a group.

Theorem 2. $|H| \in \mathbb{N} \wedge |G/H| \in \mathbb{N} \implies |G| \in \mathbb{N}$

Proof. Let $n = |H| \in \mathbb{N}$ and let $m = |G/H|$. Since G/H is the set of all left cosets of H with respect to G, we can write $|G/H|$ as $(G : H)$, the index of H with respect to G. By Lagrange's theorem, we have $|G| = (G : H) \cdot |H| = mn$. Since $m, n \in \mathbb{N}$ and the naturals are closed under multiplication, we must have $|G| \in \mathbb{N}$. This proves theorem 2. $\square$

5 Chapter 15, Exercise E2

Suppose $H \trianglelefteq G$ where G is a group.

Theorem 3. $m = (G : H) \implies (\forall x \in G/H)(\mathrm{ord}(x)|m)$

Proof. Suppose $m = (G : H)$. Then, since $(G : H) = |G/H|$, we have as a consequence of Lagrange's theorem that $(\forall x \in G/H)(\mathrm{ord}(x) \mid |G/H|)$, therefore $(\forall x \in G/H)(\mathrm{ord}(x)|m)$. This proves theorem 3. $\square$

6 Chapter 15, Exercise E5

Suppose $H \trianglelefteq G$ where G is a group.

Theorem 4. $m = (G : H) \implies a^m \in G$ *for any* $a \in G$

Proof. Suppose $m = (G : H)$ and let $a \in G$. Then, $a^m \in G$ since G is closed under multiplication. This proves theorem 4 for some reason. $\square$

7 Chapter 15, Exercise E6

Suppose $H \trianglelefteq G$ where G is a group.

Theorem 5. $(\forall x \in \mathbb{Q}/\mathbb{Z})(\mathrm{ord}(x) \in \mathbb{N})$

Proof. Suppose $x \in \mathbb{Q}/\mathbb{Z}$. Then x can be written as some $y+\mathbb{Z}$, where $y \in \mathbb{Q}$. Then, we can write $y = \frac{m}{n}$ for some $m, n \in \mathbb{Z}$ by the definition of $\mathbb{Q}$. We want to find an $n \in \mathbb{N}$ such that $n(y+\mathbb{Z}) = \mathbb{Z}$. Any $n(y+\mathbb{Z})$ is just $(ny+\mathbb{Z})$, however this n is no aribtrary integer, it is in fact the same n we see in the denominator of $y = \frac{m}{n}$, for then $(ny + \mathbb{Z}) = (n\frac{m}{n} = \mathbb{Z}) = (m + \mathbb{Z})$, and since $m \in \mathbb{Z}$, we have $m + \mathbb{Z} = \mathbb{Z}$, and every $x \in \mathbb{Q}/\mathbb{Z}$ satisfies $n(y + \mathbb{Z}) = \mathbb{Z}$ for any $y = \frac{m}{n} \in \mathbb{Q}$, therefore $\mathrm{ord}(x) = n \in \mathbb{N}$. This proves theorem 5. $\square$

8 The elements of factor group form an equivalence class

Define the equivalence relation $\sim$ by $r \sim s \iff r - s \in \mathbb{Z}$ for some $r, s \in \mathbb{Q}$. Let $[r]$ refer to the equivalence class of r with respect to $\sim$.

Theorem 6. $\mathbb{Q}/\mathbb{Z} = \{X : X = [r] \ni r \in \mathbb{Q}\}$.

Proof. Suppose $X \in \mathbb{Q}/\mathbb{Z}$. Then, X is a coset of the form $r + \mathbb{Z}$ where $r \in \mathbb{Q}$. Let $a, b \in X$. Then, $a = r + x_1 \ni x_1 \in \mathbb{Z}$ and $b = r + x_2 \ni x_2 \in \mathbb{Z}$. Therefore,

$a - b = (r + x_1) - (r + x_2) = x_1 - x_2 \in \mathbb{Z} \iff a \sim b \iff X = [r]$, therefore any $a, b \in X \implies a \sim b$, so any $X \in \mathbb{Q}/\mathbb{Z} \implies X = [r] \ni r \in \mathbb{Q}$.

Conversely, suppose $X = [r] \ni r \in \mathbb{Q}$. Then, any $a, b \in X$ can be written as $r + x_1 \ni x_1 \in \mathbb{Z}$. This is exactly the definition of a coset of the integers under the rationals, so we must have $X \in \mathbb{Q}/\mathbb{Z}$. Then, $X \in \mathbb{Q}/\mathbb{Z} \implies X = [r] \ni r \in \mathbb{Q} \wedge X = [r] \ni r \in \mathbb{Q} \implies X \in \mathbb{Q}/\mathbb{Z} \iff \mathbb{Q}/\mathbb{Z} = \{X : X = [r] \ni r \in \mathbb{Q}\}$ by the axiom of extentionality. This proves theorem 6. $\square$

9 Factoring the alternating group of four elements

Suppose $H = \{e, (12)(34), (13)(24), (14)(23)\}$ is a subgroup of the $A_4 = \{e, (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), (143)(234), (243)\}$ alternating group of four elements. In fact $H \trianglelefteq A_4$ by Homework 7 problem 12.

Then, we can write $A_4/H = \{H, H(123), H(132)\}$, and table 4 gives the operation table for A_4/H under coset multiplication.

$*$	H	$H(123)$	$H(132)$
H	H	$H(123)$	$H(132)$
$H(123)$	$H(123)$	$H(132)$	H
$H(132)$	$H(132)$	H	$H(123)$

Table 4: Operation table for A_4/H under coset multiplication

Theorem 7. $Ha \in A_4/H \ni a \notin H \implies \text{ord}(Ha) = 3$.

Proof. This is a simple proof by exhaustion. There are only two cases to check. First, observe that $(H(123))^2 = H(123)^2 = H(132)$, and $(H(123))^3 = H(132) \cdot H(123) = H((132)(123)) = H$, so $\text{ord}(H(123)) = 3$. Then, observe that $(H(132))^2 = H(132)^2 = H(123)$, and $(H(132))^3 = H(123) \cdot H(132) = H((123)(132)) = H$, so $\text{ord}(H(132)) = 3$. Since there are no other unique cosets where $a \notin H$, we have shown that theorem 7 holds for all possible cases, so this proves theorem 7 in general. $\square$

10 Digging up an old equivalence relation

Suppose $f, g \in \mathcal{F}(\mathbb{R})$.

Suppose we have the function $\phi : \mathcal{D}(\mathbb{R}) \to \mathcal{F}(\mathbb{R})$ defined by $\phi(f) = \frac{df}{dx}$ where x is the independent variable of f. By the result of Homework 7 problem 2, ϕ is an epimorphism from $\mathcal{D}(\mathbb{R})$ to $\mathcal{F}(\mathbb{R})$, so ϕ is a homomorphism from $\mathcal{D}(\mathbb{R})$ to $\mathcal{F}(\mathbb{R})$. Let $H = \ker(\phi)$ and define the relation $\sim$ as:

$$f \sim g \iff (\forall x \in \mathbb{R})(f(x) - g(x) = c \text{ for some } c \in \mathbb{R}) \tag{3}$$

Theorem 8. $(\forall f \in \mathcal{D}(\mathbb{R}))(f + H = \{g \in \mathcal{D}(\mathbb{R}) : g = f + c \ni c \in \mathbb{R})$

Proof. Suppose $f \in \mathcal{D}(\mathbb{R})$. Then, $[f] = \{g \in \mathcal{D}(\mathbb{R}) : g \sim f\}$, and let $g \in [f]$. $f \sim g \iff (\forall x \in \mathbb{R})(f(x) - g(x) = c \ni c \in \mathbb{R})$. Since the neutral element of $\mathcal{F}(\mathbb{R})$ is $\epsilon(x) = 0$ and only a $c \in \mathbb{R}$ satisfies $\frac{d}{dx}x = 0$, we can describe H entirely by $H = \mathbb{R}$, so clearly every $g \in [f]$ satisfies $g = f + c$ and this is exactly the definition of g being an element of the coset $f + H$, so any $g \in [f]$ satisfies $g \in f + H$. In fact, it works both ways, that any $g \in f + H$ can be written as some $g = f + c \ni c \in \mathbb{R}$, so $g - f = c \in \mathbb{R}$, implicitly for any value of the independent variable of the two functions. This is exactly the definition that $f \sim g$, so we have $g \in [f]$, and by the axiom of extentionality we must have $f + H = \{g \in \mathcal{D}(\mathbb{R}) : g = f + c \ni c \in \mathbb{R}\}$ for any $f \in \mathcal{D}(\mathbb{R})$. This proves theorem 8. □

11 A homomorphism on continuous functions

Suppose $G = \mathcal{C}(\mathbb{R})$ and define $\psi : G \to \mathbb{R} \ni \psi(f) = \int_0^1 f(x)dx$. We consider the group G under function addition and the group of the real numbers under conventional addition.

Theorem 9. ψ *is a homomorphism with kernel* $\ker(\psi) = H = \{f \in \mathcal{C}(\mathbb{R}) : \int_0^1 f(x)dx = 0 \in \mathbb{R}\}$.

Proof. Let $f, g \in \mathcal{C}(\mathbb{R})$. Then, $\psi(f + g) = \int_0^1 (f(x) + g(x)dx = \int_0^1 f(x)dx + \int_0^1 g(x)dx = \psi(f)\psi(g)$, so ψ is a homomorphism. Since the additive identity of $\mathbb{R}$ is 0 and any for any $f \in \mathcal{C}(\mathbb{R})$, we have $\psi(f) = \int_0^1 f(x)dx$, we can fully describe the kernel of ψ by $\ker(\psi) = \{f \in \mathcal{C}(\mathbb{R}) : \int_0^1 f(x)dx = 0 \in \mathbb{R}\}$. This proves theorem 9. □

By theorem 9, G/H is defined since the kernel of a homomorphism is a normal subgroup of the domain of that same homomorphism. Then, we can descibe this quotient group by $G/H = \{X : X = f + H \ni (\forall g \in H)(\int_0^1 (f(x) + g(x))dx = \int_0^1 g(x)dx)\}$.

12 Normal subgroups of the general linear group in two dimensions

Suppose $G = GL_2(\mathbb{R})$ and $H = \{X \in G : \det(X) = 1\} = SL_2(\mathbb{R})$ be a subgroup of G.

Theorem 10. $H \trianglelefteq G$

Proof. Define the function $\phi : GL_2(\mathbb{R}) \to \mathbb{R}^* \ni \phi(A) = \det(A) \ni A \in GL_2(\mathbb{R})$. Then every $X \in GL_2(\mathbb{R})$ satisfies $\phi(X) = \det(X) = 1 \iff X \in SL_2(\mathbb{R})$ because this is exactly the definition of an element being in $SL_2(\mathbb{R})$. Since for any $A, B \in GL_2(\mathbb{R})$, we have $\phi(AB) = \det(AB) = \det(A)\det(B) = \phi(A)\phi(B)$, we have that ϕ is a homomorphism from $GL_2(\mathbb{R})$ to $\mathbb{R}^*$ with $\ker(\phi) = SL_2(\mathbb{R})$. Then, since the kernel of a homomorphism is a normal subgroup of the domain, we have that $SL_2(\mathbb{R})$ is a normal subgroup of $GL_2(\mathbb{R})$, that is to say, $H \trianglelefteq G$ and this proves theorem 10. $\square$

We can describe G/H by $G/H = \{X : X = Y \cdot SL_2(\mathbb{R}) \ni Y \in GL_2(\mathbb{R})\}$.

13 Another look at $GL_2(\mathbb{R})$

Suppose $G = GL_2(\mathbb{R})$ and $H = \{X \in GL_2(\mathbb{R}) : \det(X) > 0$.

Define $\phi : G \to P$ where $P = \{-1, 1\}$ and for any $X \in GL_2(\mathbb{R})$, we have $\phi(X) = \begin{cases} 1 & \text{if } \det(X) > 0 \\ -1 & \text{if } \det(X) < 0 \end{cases}$.

Table 5 gives the operation table for the parity group P under multiplication.

Theorem 11. $H \trianglelefteq G$

Proof. Supppose $X \in GL_2(\mathbb{R})$. By definition of $GL_2(\mathbb{R})$, $\det(X) \neq 0$, so we must have either $\det(X) > 0$ or $\det(X) < 0$.

$*$	1	-1
1	1	-1
-1	-1	1

Table 5: Operation table for P under mulitplication denoted by $*$

We start with $X \in H \iff \det(X) > 0$, then $\phi(X) = 1$, and $X \in \ker(\phi)$. so $\det(X) > 0 \implies X \in \ker(\phi)$.

Alternatively, if we start with $X \notin H \iff \det(X) < 0$, then $\phi(X) = -1$, and $X \notin \ker(\phi)$ so $\det(X) < 0 \implies X \notin \ker(\phi)$. Since either $X \in H \vee X \notin H$, we have that $\det(X) > 0 \iff X \in H$ fully describes $\ker(\phi)$, so $X \in H \iff X \in \ker(\phi)$.

Introduce another aribtrary $Y \in GL_2(\mathbb{R})$. Then, $\det(X)\det(Y) = \det(XY) > 0$ so $\phi(XY) = \phi(X)\phi(Y)$, and ϕ is a homomorphism.

Since H is the kernel of a homomorphism from its group to some other group, H must be a normal subgroup of G, i.e. $H \trianglelefteq G$. This proves theorem 11. ☐

Now we consider G/H.

Theorem 12. $G/H = \{H, AH\}$ *for some* $A \in G \ni A \notin H$.

Proof. We first see that of course $e \in H \implies eH = H \in G/H$. then, any $x \in H$ satisfies $aH = H$. Suppose we have some $A \in G \notin H \iff \det(A) < 0$. We see that $AH \neq H$ since $A \notin H$, so $AH \in G/H$. Then, define $\psi : G/H \to P$ by $\psi(AH) = \phi(A)$ for any $A \in G$. Since for any $AH, BH \in G/H$, we have $\psi(AH)\psi(BH) = \phi(A)\phi(B) = \phi(AB) = \psi((AB))$, ψ is a homomorphism.

Suppose $\psi(AH) = \psi(BH)$. Then, $\phi(A) = \phi(B)$, so $\det(A) > 0 \iff \det(B) > 0$, which means $A \in XH \iff B \in HX$ for any $X \in GL_2(\mathbb{R})$. And since $A \in XH \iff AH = XH$ as well as $B \in XH \iff BH = XH$, we have $AH = BH$, so ψ is injective.

Suppose $x \in P$. Then, either $x = 1 \vee x = -1$. Suppose $A \in G \ni \det(A) > 0$. Then, $\psi(AH) = 1$. Suppose $B \in G \ni \det(B) < 0$. Then, $\psi(BH) = -1$. For every element x of P, we can find an element X of G/H such that $\phi(X) = x$, so by exhaustion, ψ is surijecive.

Since ψ is injective and surjective, ψ is an isomorphism so its domain and codomain must have the same cardinality. By inspection, we have $|P| = 2 \iff |G/H| = 2$. Above, we saw that $H \in G/H$ and that $\exists A \in G$ where $AH \neq H$ holds, so $\{H, AH\} \subseteq G/H$. But since $|G/H| = 2$, this must fully describe G/H and $G/H \subseteq \{H, AH\}$, so $G/H = \{H, AH\}$ for some $A \in G \ni A \notin H$ by the axiom of extentionality. This proves theorem 12. $\square$

14 Quotient of a Group by Its Center

Suppose $C \trianglelefteq G \ni C = \{x \in G : (\forall a \in G)(xa = ax)\}$. Then G/C is well-defined.

Assume that G/C is cyclic, i.e. we have that $\exists Ca \in G/C \ni \langle Ca \rangle = G/C$.

Theorem 13. *For any* $x \in G$*, there exists some* $m \in \mathbb{Z}$ *where* $Cx = Ca^m$ *holds.*

Proof. Suppose $x \in G$. Then, $Cx \in G/C$ by definition. Since G/C is cyclic, we have that any $Cx \in G/C$ can be written as some $Cx = (Cb)^n \in G/C$, where $n \in \mathbb{Z}$. But since $(Cb)^n = Cb^n$, we have $Cx = Cb^n$, which proves theorem 13. $\square$

Theorem 14. *For any* $x \in G$*, there exists some* $m \in \mathbb{Z}$ *where* $x = ca^m \ni c \in C$ *holds.*

Proof. By theorem 13, we have that $Cx = Ca^m$ for some integer m, for any $x \in G$. Then, by the definition of a coset, we have some integers $c_1, c_2 \in C$, where $c_1 x = c_2 a^m$ holds, but multiplication on the left by c_1^{-1} yields $x = c_1^{-1} c_2 a^m$, and since C is a subgroup, we have some $c = c_1^{-1} c2 = \in C$, so $x = ca^m \ni c \in C$, which proves theorem 14. $\square$

Theorem 15. *For any two* $x, y \in G$*, we have* $xy = yx$*.*

Proof. By theorem 14, any $x, y \in G$ can be written as $x = ca^m$ and $y = da^n$ for some $c, d \in C$ and some $m, b \in \mathbb{Z}$. Since by definition, any element of C commutes with any element of G, we have $xy = (ca^m)(da^n) = c(da^m)a^n = (dc)a^{m+n} = (dc)a^{n+m} = d(ca^n)a^m = (da^n)(ca^m) = yx$, which proves theorem 14. $\square$

Theorem 16. *If* G/C *is cyclic, then* G *is abelian.*

Proof. Suppose G/C were cyclic. Then, we have theorem 13, and by theorem 14, we have theorem 14, and by theorem 14, we have that for any two $x, y \in G$, we have $xy = yx$, so G is abelian. This proves theorem 16. $\square$