

Abstract Algebra: Homework #6

Joel Savitz

Wednesday 1 July 2020

1 Chapter 13, Exercise A3

Suppose H is a subgroup of some group G . Furthermore, suppose $G = \mathbb{Z}_{15} \wedge H = \langle 5 \rangle$. Then, denoting $+_{15}$ as $+$, the following are the cosets of H :

$$H + 0 = \{0, 5, 10\}$$

$$H + 1 = \{1, 6, 11\}$$

$$H + 2 = \{2, 7, 12\}$$

$$H + 3 = \{3, 8, 13\}$$

$$H + 4 = \{4, 9, 14\}$$

2 Chapter 13, Exercise A4

Denote the elements of D_4 as:

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

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

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

Suppose H' is a subgroup of some group G . Furthermore, suppose $G = D_4 \wedge H' = \{R_0, D'\}$

\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 1: Operation table for G under \circ

Then, using multiplicative notation for \circ , we have the following cosets of H'

$$\begin{aligned}
H'R_0 &= \{R_0, D'\} \\
H'R_{\pi/2} &= \{R_{\pi/2}, H\} \\
H'R_\pi &= \{R_\pi, D\} \\
H'R_{3\pi/2} &= \{R_{3\pi/2}, V\} \\
H'H &= \{H, R_{\pi/2}\} \\
H'V &= \{V, R_{3\pi/2}\} \\
H'D &= \{D, R_\pi\} \\
H'D' &= \{D', R_0\}
\end{aligned}$$

3 Chapter 13, Exercise B1

Suppose $H = \langle 3 \rangle$ where $3 \in \mathbb{Z}$.

Then, we can describe the three cosets of H as follows:

$$\begin{aligned}
H + 0 &= \{x \in \mathbb{Z} : \exists k \in \mathbb{Z} \ni x = 3k\} \\
H + 1 &= \{x \in \mathbb{Z} : \exists k \in \mathbb{Z} \ni x = 3k + 1\} \\
H + 2 &= \{x \in \mathbb{Z} : \exists k \in \mathbb{Z} \ni x = 3k + 2\}
\end{aligned}$$

4 Chapter 13, Exercise C2

Suppose G is some group such that $\text{ord}(G) = pq$ for some prime natural p and q .

Theorem 1. G is not cyclic if and only if every $x \in G \ni x \neq e \in G$ satisfies $\text{ord}(x) = p \vee \text{ord}(x) = q$.

Proof. Suppose G is cyclic. Then, some $x \in G$ satisfies $\langle x \rangle = G \iff \text{ord}(x) = pq$ and we have some $x \in G$ where $\text{ord}(x) = p \vee \text{ord}(x) = q$ does not hold.

Conversely, suppose G is not cyclic. Then, let x be some member of G where $x \neq e \in G$. By Lagrange's theorem, we must have that $\text{ord}(x)$ divides $\text{ord}(G)$, and so we have that $\text{ord}(x)$ divides pq . Then, $\text{ord}(x) \in \{1, p, q, pq\}$. We also have $(\text{ord}(x) = 1 \iff x = e) \wedge \text{ord}(x) \neq e \implies \text{ord}(x) \neq 1$. And of course $\text{ord}(x) \neq pq$, since otherwise $\langle x \rangle = G$, violating our assumption that G is not cyclic. We have deduced that $\text{ord}(x) = p \vee \text{ord}(x) = q$ holds.

This proves theorem 1. \square

5 Chapter 13, Exercise C3

Suppose G is some group where $\text{ord}(G) = 4$.

Theorem 2. G is not cyclic if and only if every element of G is its own inverse.

Proof. Suppose G is cyclic. Then, we have an $x \in G$ such that $\langle x \rangle = G$. We can write G as $\{e, x, x^2, x^3\}$. By inspection we see that $x^2 \neq e$ and we have an element of G that is not its own inverse, so it is false that every element of G is its own inverse when G is cyclic.

Suppose G is not cyclic. By Lagrange's theorem, the order of every element of G must divide the order of G , so the non identity elements of G must have order 2 or order 4. Since G is not cyclic, no element has order 4, for if it did, that element would generate G and G would not be cyclic. Since every $x \in G$ satisfies $\text{ord}(x) = 2$, we must have $x^2 = e$ for every $x \in G$ and then every element of G is its own inverse.

This proves theorem 3. \square

Theorem 3. Every group of order 4 is abelian.

Proof. Suppose G is not cyclic. Then, by theorem 2, we have that every $x \in G$ satisfies $x^{-1} = x$. Applying this identity, we find that $ab = a^{-1}b^{-1} = (ba)^{-1} = ba$ so any $a, b \in G$ commute and G is abelian.

Instead, suppose G is cyclic. Then, G has a generator x where $G = \{e, x, x^2, x^3\}$. Then, we can write any $y \in G$ as $y = x^i$ for any $i \in \{0, 1, 2, 3\}$. If $a = x^\alpha \in G$ and $b = x^\beta$ are two such sets, we observe that $ab = x^\alpha x^\beta = x^{\alpha+\beta} = x^{\beta+\alpha} = x^\beta x^\alpha = ba$ and see that any two $a, b \in G$ commute and G is abelian.

Since G is abelian if G is cyclic and G is abelian if G is not cyclic, we see by the law of the excluded middle that G is abelian and in general, every group of order 4 is abelian.

This proves theorem 3. \square

6 Chapter 13, Exercise D1

Suppose H and K are subgroups of a finite group G .

Theorem 4. $H \subseteq K \implies (G : H) = (G : K)(K : H)$

Proof. Let $n = \text{ord}(G)$ and let $h = \text{ord}(H) \wedge k = \text{ord}(K)$. Then, by Lagrange's theorem, we must have that $h|n$ and $k|n$. $(G : H) = \frac{\text{ord}(G)}{\text{ord}(H)}$ and $(G : K) = \frac{\text{ord}(G)}{\text{ord}(K)}$. Since H is a subgroup of G , we must have that $x \in H \implies x^{-1} \in H$ and $(\forall x, y \in H)(xy \in H)$. Then, since we have $H \subseteq K$, we must have that H is a subgroup of K , and therefore $(K : H) = \frac{\text{ord}(K)}{\text{ord}(H)}$. By these identities, we must have:

$$(G : H) = \frac{\text{ord}(G)}{\text{ord}(H)} \tag{3}$$

$$(G : H) = \frac{\text{ord}(G) \text{ord}(K)}{\text{ord}(H) \text{ord}(K)} \tag{4}$$

$$(G : H) = \frac{\text{ord}(G)}{\text{ord}(K)} \frac{\text{ord}(K)}{\text{ord}(H)} \tag{5}$$

$$(G : H) = (G : K)(K : H) \tag{6}$$

This proves theorem 4. \square

7 Chapter 13, Exercise E1

Suppose H is a subgroup of some group G and let $a, b \in G$.

Theorem 5. $Ha = Hb \iff ab^{-1} \in H$

Proof. Suppose $Ha = Hb$. Then, we have $a \in Hb$ so there is an $x \in H$ where $xb = a$, but then we can multiply both sides on the right by b^{-1} to see that $x = ab^{-1} \in H$.

Conversely, suppose $ab^{-1} \in H$. Then, $a \in Hb$ since $(ab^{-1})b \in Hb$, but $a \in Hb \iff Ha = Hb$.

This proves theorem 5. □

8 Chapter 13, Exercise E3

Suppose H is a subgroup of some group G and let $a, b \in G$.

Theorem 6. $aH = Ha \wedge bH = Hb \implies (ab)H = H(ab)$

Proof. Suppose $aH = Ha \wedge bH = Hb$. If $x \in H$, then we have $xa = ax \wedge xb = bx$. We can isolate the x in each equation by multiplication of the first on the right by a^{-1} and multiplication of the second on the right by b^{-1} to get the identities $x = axa^{-1} \wedge x = bxb^{-1}$ and substitute an x in the first equation with an equivalent value in the second to get $x = a(bxb^{-1})a^{-1} = (ab)x(ab)^{-1}$. But then we can just multiply on the right by (ab) to get $x(ab) = (ab)x$ and thus $x \in H(ab) \wedge x \in (ab)H \iff (ab)H = H(ab)$. This proves theorem 6. □

9 The affine group and her little brother

Suppose G is the affine group defined as $G = \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \in GL_2(\mathbb{R}) : a \neq 0 \right\}$.

Let $H = \left\{ \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} : x \in \mathbb{R} \right\}$.

Theorem 7. H is a subgroup of G

Proof. Suppose $x \in H$. We see that $x_{1,1} \in \mathbb{R} \ni a \neq 0$ and of course that $x_{1,2} \in \mathbb{R}$, as well as the fact that $x_{2,1} = 0 \wedge x_{2,2} = 1$, so we conclude that $x \in G$ and since $x \in H \implies x \in G$, we have $H \subseteq G$.

Consider an $x = \begin{bmatrix} 1 & p \\ 0 & 1 \end{bmatrix} \in H$ and a $y = \begin{bmatrix} 1 & q \\ 0 & 1 \end{bmatrix} \in H$. Then, $xy = \begin{bmatrix} 1 & p+q \\ 0 & 1 \end{bmatrix} \in H$ since $p+q \in \mathbb{R}$ and we see that H is closed under matrix multiplication.

Let $x = \begin{bmatrix} 1 & \alpha \\ 0 & 1 \end{bmatrix} \in H$. Then, $x^{-1} = \frac{1}{1-0 \cdot \alpha} \begin{bmatrix} 1 & -\alpha \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -\alpha \\ 0 & 1 \end{bmatrix}$ and clearly $x^{-1} \in H$ since $-\alpha \in \mathbb{R}$. We also see that $xx^{-1} = x^{-1}x = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in H$.

Then, since H is a subset of G closed under matrix multiplication, where every element $x \in H$ has its inverse $x^{-1} \in H$, we conclude that H is a subgroup of G . This proves theorem 7. \square

We can describe the right cosets of H for some $a = \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \in G$ by $Ha = \left\{ k : k = \begin{bmatrix} a & b+x \\ 0 & 1 \end{bmatrix} \wedge k = yk \ni y = \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \in H \right\}$.

10 Cosets of some permutation group

Suppose H is a subgroup of $G = A_4$, where we can write A_4 as:

$$\{e, (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), (143), (234), (243)\} \quad (7)$$

and we let $H = \{e, (12)(34), (13)(24), (14)(23)\}$.

We can calculate $(G : H) = \frac{\text{ord}(G)}{\text{ord}(H)} = \frac{12}{4} = 3$.

The three cosets of H with respect to G are:

$$He = \{e, (12)(34), (13)(24), (14)(23)\} \quad (8)$$

$$H(123) = \{(123), (134), (243), (142)\} \quad (9)$$

$$H(132) = \{(132), (143), (234), (124)\} \quad (10)$$

11 A bunch of proofs

Suppose $B_1 = \{1, \dots, k\}$ and $B_2 = \{k+1, \dots, n\}$ where $k \in \mathbb{Z} \ni 1 \leq k \leq n-1$ for some $n \in \mathbb{N}$.

Then, define the following two subgroups of S_n :

$$G_1 = \{f \in S_n : (\forall x \in B_1 \cup B_2)(x \in B_1 \implies f(x) \in B_1 \wedge x \in B_2 \implies f(x) = x)\} \quad (11)$$

$$G_2 = \{f \in S_n : (\forall x \in B_1 \cup B_2)(x \in B_2 \implies f(x) \in B_2 \wedge x \in B_1 \implies f(x) = x)\} \quad (12)$$

Furthermore, define $H = \{f \circ g : f \in G_1, g \in G_2\}$.

11.1 Elements of G_1, G_2 , and H , plus $(S_5 : H)$

Consider the concrete case of S_5 . Let $B_1 = \{1, 2\}$ and let $B_2 = \{3, 4, 5\}$. Then, we can write the elements of G_1, G_2 , and H as follows:

$$\begin{aligned} G_1 &= \{e, (12)\} \\ G_2 &= \{e, (34), (35), (45), (345), (354), \} \\ H &= \{e, (34), (35), (45), (345), (354), \\ &\quad (12), (12)(34), (12)(35), (12)(45), (12)(345), (12)(354)\} \end{aligned}$$

Since $\text{ord}(S_5) = 5! = 120$ and $\text{ord}(H) = 12$, we have $(S_5 : H) = \frac{120}{12} = 10$.

11.2 Proof of $H \leq S_n$ in general

First, I need to prove general commutativity:

Theorem 8. *Any element of G_1 commutes with any element of G_2 under \circ*

Proof. Let $f \in G_1$ and let $g \in G_2$. Consider some $x \in B_1 \cup B_2$. We look at the possible values of $(f \circ g)(x) = f(g(x))$. If $x \in B_1$, then $g(x) = x$ and $f(g(x)) = f(x)$, but if $x \in B_2$, then $f(g(x)) = g(x)$. Alternatively, consider the possible values of $(g \circ f)(x) = g(f(x))$. If $x \in B_1$, then $g(f(x)) = f(x)$. but if $x \in B_2$, then $f(x) = x$ and $g(f(x)) = g(x)$. Since $\neg(x \in B_1) \iff (x \in B_2)$, we have that $(f \circ g)(x) = (g \circ f)(x)$ for any $f \in G_1$ and $g \in G_2$. This proves theorem 8. \square

Now, I can prove the following theorem:

Theorem 9. *H is a subgroup of S_n*

Proof. Let $x, y \in H$. By definition, we can write each $a \in H$ as some $f \circ g \ni f \in G_1 \wedge g \in G_2$. As such, let $p \in G_1$ and $q \in G_2$ be such that $x = p \circ q$ and let $r \in G_2$ and $s \in G_2$ be such that $y = r \circ s$. We can compose these to identities to get $x \circ y = (p \circ q) \circ (r \circ s)$. Then by theorem 8 and the associativity of \circ , we have $x \circ y = (p \circ r) \circ (q \circ s)$, and since $(p \circ r) \in G_1$ and $(q \circ s) \in G_2$ due to the closure of \circ on subgroups G_1 and G_2 , we have that $x \circ y$ is the composition of some element of G_1 and some element of G_2 , and this is exactly the definition of $x \circ y \in H$. Then, H is closed under \circ .

If have $x = p \circ q \in H$, then we must have $x^{-1} = (p \circ q)^{-1} = (q^{-1} \circ p^{-1})$, and this is verified by $x^{-1} = (p \circ q) \circ (q^{-1} \circ p^{-1})$. Thus every $x \in H$ has its inverse $x^{-1} \in H$.

With this last fact and with the fact that H is closed under \circ , we conclude that H is a subgroup of S_n and this proves theorem 9. \square

11.3 Abstract counting

Theorem 10. $(S_n : H) = \frac{n!}{k!(n-k)!}$

Proof. Since G_1 contains permutations on elements of B_1 only with all points in B_2 fixed and $|B_1| = k$, we have $\text{ord}(G_1) = k!$. Then, since G_2 contains permutations on elements of B_2 only with all points in B_1 fixed and $|B_2| = n - k$, we have $\text{ord}(G_2) = (n - k)!$. Since we construct H by constraining the set to some $k!$ elements of G_1 composed with $(n - k)!$ elements of G_2 , where every composition is unique since they are on mutually exclusive intervals of \mathbb{Z} , we have $\text{ord}(G) = k!(n - k)!$. Finally because $\text{ord}(S_n) = n!$, we must have by definition that $(S_n : H) = \frac{n!}{k!(n-k)!}$. This proves theorem 10. \square

12 A few equivalent propositions

Suppose $a, b \in H$ where H is a subgroup, of some group G .

Theorem 11. $a \in Hb \iff ab^{-1} \iff Ha = Hb$

Proof. By theorem 5, we have $ab^{-1} \iff Ha = Hb$. Because $(Ha = Hb \iff (x \in Ha \iff x \in Hb))$, we must have $Ha = Hb \iff a \in Hb$

since clearly $a = ea \iff a \in Ha$. By transitivity and commutivity of bidirective implication, we have $a \in Hb \iff ab^{-1} \iff Ha = Hb$. This proves theorem 11. \square

13 Normal subgroups

Define a normal subgroup of G to be some H such that $h \in H \wedge a \in G \implies aha^{-1} \in H$.

Theorem 12. $\left((\forall a \in H)(aH = Ha) \right) \implies H \text{ is a normal subgroup of } G$.

Proof. Suppose that $aH = Ha$ for any $a \in G$. Then, let h be some element of H . Following our assumption, we must have $ha = ah$, which when each equivalent value is multiplied on the right by a^{-1} yields $h = aha^{-1} \in H$. Thus some $h \in H$ and any $a \in G$ implies $aha^{-1} \in H$, so H is a normal subgroup of G . This proves theorem 12. \square

14 Index 2 subgroups are normal

Theorem 13. *If H is a subgroup of some G where $(G : H) = 2$, then H is a normal subgroup of G .*

Proof. Suppose H is a subgroup of some G where $(G : H) = 2$ holds. Let h be some element of H and let a be some element of G . We have $a \in He = H$ if and only if $Ha = He = H$ by theorem 11. $a \in aH \iff Ha = aH$, and clearly $ae = a \in aH$, so $aH = Ha$ when $a \in H$. We have $a \notin He \iff Ha \neq He = H$ by theorem 11, and then of course $a \notin eH \iff aH \neq eH = H$. Since there are only two possible cosets of H by the fact that $(G : H) = 2$, and by the fact that cosets of H are disjoint partitions of the group G , we must have $aH \neq H \wedge Ha \neq H \iff aH = Ha$, so for any $a \in G$, we have $aH = Ha$. Then by theorem 12, if we have that any $a \in G$ satisfies $aH = Ha$, then H is a normal subgroup of G . Since this is indeed the case with our generic subgroup H where $(G : H) = 2$, we must have $(G : H) = 2 \implies H$ is a normal subgroup of G . This proves theorem 13. \square