MATH 315 CHAPTER 15

JACOB TERKEL

FEBRUARY 6, 2023

Problem 1, Chapter 15

Lemma 1. *For any $g, h, k \in G$ such that $g * h = e_*$ and $k * g = e_*$ we have that $h = k$.*

Proof. Consider some group G as well as $g, h, k \in G$ where g, h, and k are defined in accordance with the claim, by the associative property we have

$$(k * g) * h = k * (g * h).$$

However, this gives us that

$$e_* * h = k * e_*$$

which is equivalent to $h = k$, proving our claim. $\boxed{J\tau}$

Lemma 2. *For a group G, and $g \in G$ there is a unique g^{-1} such that $g * g^{-1} = g^{-1} * g = e_*$.*

Proof. By the inverse property of groups, we are guaranteed the existence of at least one inverse for any element in G. Assume that some element $g \in G$ has at least two distinct inverses, and let k and ℓ be two such inverses. We have that $g * k = e_*$ and $\ell * g = e_*$. However, by Lemma 1 this means that $\ell = k$, a contradiction to our assumption that k and ℓ are distinct, and thus our claim is proven as if an element cannot have zero or more than two inverses, that element must have exactly one inverse. $\boxed{J\tau}$

Lemma 3. *The identity of a group G must be unique.*

Proof. If a group has two identity elements, g and h then the value of $g * h$ is not well defined, and thus you cannot have two identity elements. $\boxed{J\tau}$

Claim (Part A). *For a group, G, and $a \in G$ where $a * G = \{a * g \mid g \in G\}$ and $G * a = \{g * a \mid g \in G\}$ we have that $a * G = G * a = G$ for all G.*

Proof. To prove the claim it suffices to prove that $a * G = G$ and $G * a = G$.

First, I will show that $a * G = G$. See that $a * G \subseteq G$ by closure, and so it suffices to prove that every element of G is in $a * G$. Consider any $g_1 \in G$. By closure and inverse, $a^{-1} * g_1 \in G$, and thus $a * (a^{-1} * g_1) \in a * G$. By associativity and inverse this gives us that

$$(a * a^{-1}) * g_1 = e_* * g_1 = g_1 \in a * G,$$

and so we have that $a * G = G$.

To prove that $G * a = G$ the process is seen to be almost identical and thus for brevity I will not be writing the full proof here.

With this, our claim has been proven. $\boxed{J\tau}$

Claim (Part B)**.** *All groups of order three are isomorphic to each other.*

Proof. By Lemma 3, there is a unique identity element in every group, so for a group of order three $G = \{a, b, c\}$ we will assume that $a \in G$ is the identity element, and thus any group of order three must have a Cayley Table of the form taken below

	a	b	c
a	a	b	c
b	b		
c	c		

Furthermore, by Part A, we must have that $G = G * b$, and $G = \{a, b, c\}$, this means that in the b row, there cannot be another b. However, $c * G = G$ as well, meaning there must be a b in the rightmost column, which means the b must be equal to $c * c$.

	a	b	c
a	a	b	c
b	b		
c	c		b

Furthermore, there must also be an a in the bottom row and rightmost column, of which there is only one possible spot for.

	a	b	c
a	a	b	c
b	b		a
c	c	a	b

Lastly, we know there must be a c in the middle column, and thus the last spot is filled and the Cayley Table for every group of order three takes the following form.

	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

Because every group of order three shares the same Cayley Table, they all must be isomorphic, and our claim is proven.

$\boxed{J\tau}$

Claim (Part C). *Every group of order four is isomorphic to either $\mathbb{Z}_4$ or the Klein 4-group.*

Proof. Let $G = \{a, b, c, d\}$ be a group of order four. Assume, WLOG that a is the identity element. We have that such a group must take the form

	a	b	c	d
a	a	b	c	d
b	b			
c	c			
d	d			

Now, because b is not the identity we may assume WLOG that $b * b = c$ or $b * b = a$, and thus our group takes one of the following forms

	a	b	c	d
a	a	b	c	d
b	b	c		
c	c			
d	d			

	a	b	c	d
a	a	b	c	d
b	b	a		
c	c			
d	d			

Let us first consider the case where $b * b = c$. By Part A, we must have that the b column contains an a and a d. We cannot have $b * d = d$, as that would make b the identity and so $b * d = a$, which implies that $b * c = d$. This same process works for the b row as well, giving us the following Cayley Table.

	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d		
d	d	a		

Now, we see that c must appear in the d row, but we cannot have that $c * d = c$, so we have that $d * d = c$, and thus by Part A we can fill out or table as follows.

	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

This table is seen to be isomorphic to $\mathbb{Z}_4$

Now, let us consider the other table form that we had at the start. I draw it again below.

	a	b	c	d
a	a	b	c	d
b	b	a		
c	c			
d	d			

Now, by Part A we must have either that $b * c = d$ or $b * c = c$ the latter cannot be true as b is not the identity element, which allows us to fill out the b column of the table, and like before the b row can be done identically.

	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d		
d	d	c		

Again, by Part A we must have either that $c * c = a$ or $c * c = b$. If $c * c = b$ then we will have that $d * c = a$ and $d * d = b$. However, this can be seen to be isomorphic to $\mathbb{Z}_4$ the isomorphism $f(a) = 0$, $f(b) = 2$, $f(c) = 1$, and $f(d) = 3$. So, either this table is also isomorphic to $\mathbb{Z}_4$ or $c * c = a$. However, by Part A this means that $c * d = d * c = b$ and $d * d = a$ which gives us the table

	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

which is isomorphic to the Klein 4-group. Thus, every group of order four is isomorphic to either $\mathbb{Z}_4$ or the Klein 4-group, as claimed.

$\boxed{J\tau}$

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

FIGURE 1. Group?

Claim (Part D). *The above table does not represent a group.*

Proof. By the above table, we have that $B*(C*D) = B*E = D$ and that $(B*C)*D = E*D = B$. However, by the associative property, we should have that $B*(C*D) = (B*C)*D$, which is seen to be violated above, and thus this table is not a group. $\boxed{J\tau}$

Remark. However, this structure is seen to satisfy Identity, Invertibility, and Closure. Such structures are called *Loops*, and have theier own interesting set of properties.

Claim.

Problem 2, Chapter 15

Claim (Part A). *For positive integer n we have that $|D_n| = 2n$.*

Proof. We first observe that $|D_n| \geq 2n$ by observing that every $360°/n$ rotation of a regular n-gon preserves rigidity, and is unique from each other. Furthermore, we can see that by reflecting the n-gon about any of its n axes. For odd n, these axes are all very similar, the pass-through one vertex, the center of the shape, and the midpoint of the opposite edge. For even n, there are $n/2$ axes that pass through opposing vertices, and $n/2$ axes that pass through the midpoint of opposing edges. All of these are seen to be distinct from the rotations as the numbers appear in counter-clockwise order when reflected, but clockwise when rotated. Furthermore, these reflections are distinct from each other as the reflections that pass through vertices all fix different vertices, and the reflections that pass through edges all swap different pairs.

Now, I claim that there can be no more than $2n$ rigid symmetries. After any rigid transformation takes place the same points that were adjacent to each other must remain adjacent to each other, meaning either the points are in the same "order" as they started in or they are in the reverse order, as for any x and y that were next to each other, to begin with after a rigid transformation we will have either that x is to the immediate left of y or x is to the immediate right of y. Since the order of the points in a rigid transformation must either be the same or reversed from the original order we can see that each possible position of the 1 and 2 points corresponds to at most one unique rigid transformation. We see that there are $2n$ of these possible orientations as there are n possible positions for a point 1, and point 2 can be either to the direct left or direct right of point 1, doubling the number of possible orientations to $2n$, the very maximum number of rigid transformations.

$\boxed{J\tau}$

Lemma 4. *D_n is associative.*

Proof. each element of D_n can be seen as a function from $\{1, 2, \ldots, n\}$ to itself, and thus D_n is associative from the fact that function composition is associative. $\boxed{J\tau}$

Claim (Part B)**.** *D_3 is a non-abelian group.*

TABLE 1. Rotations are clockwise

	0°	120°	240°	Ɩ	↊	↋
0°	0°	120°	240°	Ɩ	↊	↋
120°	120°	240°	0°	↋	Ɩ	↊
240°	240°	0°	120°	↊	↋	Ɩ
Ɩ	Ɩ	↊	↋	0°	120°	240°
↊	↊	↋	Ɩ	240°	0°	120°
↋	↋	Ɩ	↊	120°	240°	0°

Proof. In the table above we see that closure, identity, and inverse are satisfied as 0° is an identity and it appears in each column. Lastly D_3 is associative by Lemma 4.

It is seen to not commute as Ɩ $*$ ↊ $\neq$ ↊ $*$ Ɩ $\boxed{J\tau}$

Claim (Part C)**.** *D_4 is a non-abelian group.*

TABLE 2. Rotations are clockwise

	0°	90°	180°	270°	$\nearrow$	$\rightarrow$	$\searrow$	$\uparrow$
0°	0°	90°	180°	270°	$\nearrow$	$\rightarrow$	$\searrow$	$\uparrow$
90°	90°	180°	270°	0°	$\rightarrow$	$\searrow$	$\uparrow$	$\nearrow$
180°	180°	270°	0°	90°	$\searrow$	$\uparrow$	$\nearrow$	$\rightarrow$
270°	270°	0°	90°	180°	$\uparrow$	$\nearrow$	$\rightarrow$	$\searrow$
$\nearrow$	$\nearrow$	$\uparrow$	$\searrow$	$\rightarrow$	0°	270°	180°	90°
$\rightarrow$	$\rightarrow$	$\nearrow$	$\uparrow$	$\searrow$	90°	0°	270°	180°
$\searrow$	$\searrow$	$\rightarrow$	$\nearrow$	$\uparrow$	180°	90°	0°	270°
$\uparrow$	$\uparrow$	$\searrow$	$\rightarrow$	$\nearrow$	270°	180°	90°	0°

Proof. In the table above we see that closure, identity, and inverse are satisfied as 0° is an identity and it appears in each column. Lastly D_3 is associative by Lemma 4.

It is seen to not commute as $\uparrow * \searrow \neq \searrow * \uparrow$ $\boxed{J\tau}$

Problem 3, Chapter 15

Claim (Part A). *The twelve elements of A_4 are listed below in cycle notation are listed below.*

Proof.

$$A_4 = \left\{ \begin{array}{c} (1)(2)(3)(4), (12)(34), (123)(4), (124)(3), \\ (132)(4), (134)(2), (234)(1), (143)(2), \\ (142)(3), (243)(1), (13)(24), (14)(23) \end{array} \right\}$$

$\boxed{J\tau}$

Claim (Part B). *The Cayley Table of A_4 is too much work for me to want to do right now.*

Let $C_0 = (1)(2)(3)(4)$, let $C_1 = (123)(4)$, $C_2 = (132)(4)$, $C_3 = (124)(3)$, $C_4 = (142)(3)$, $C_5 = (134)(2)$, $C_6 = (143)(2)$, $C_7 = (234)(1)$, $C_8 = (243)(1)$, $C_9 = (12)(34)$, $C_{10} = (13)(24)$, and $C_{11} = (14)(23)$.

Claim (Part C). *A_4 is a group.*

Proof. Closure is shown in Part B. Associativity follows from the fact that function composition is associative. Identity is seen to be C_0. Inverse is also then verified by the table. $\boxed{J\tau}$

Claim (Part D). *A_4 is not an abelian group as $C_3 \circ C_2 \neq C_3 \circ C_2$.*

Problem 10, Chapter 15

Lemma 5. *Isomorphism is transitive.*

Proof. Let G, H, and K be groups such that $G \cong H$ and $H \cong K$. Let $f_1 : G \to H$ and $f_2 : H \to K$ be isomorphisms. We have that $f_2 \circ f_1$ is a bijection as f_1 and f_2 are bijections. Furthermore, we have that $f_1(g_1) + f_1(g_2) = f_1(g_1 g_2)$, and because f_2 is an isomorphism too we have that

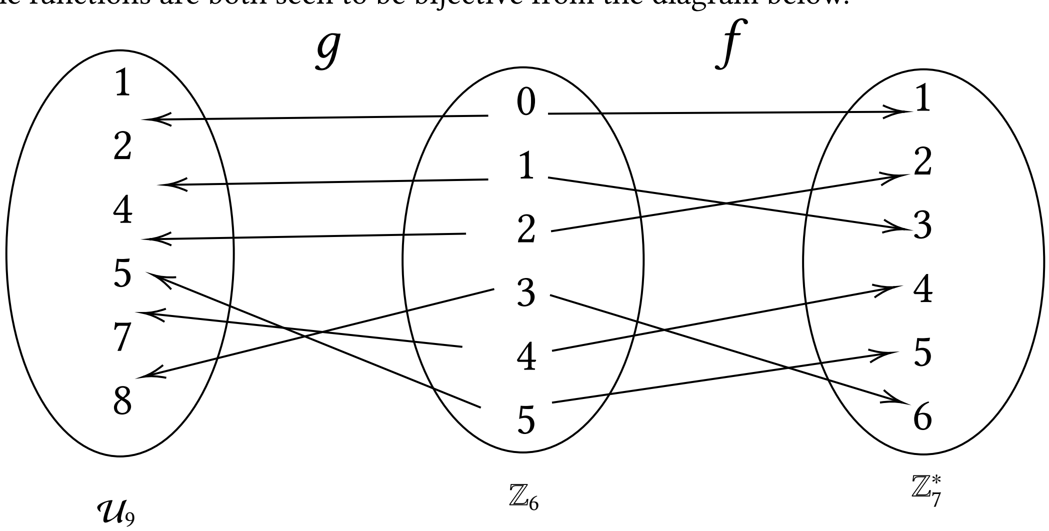
$$f_2(f_1((g_1)) + f_2(f_1(g_2)) = f_2(f_1(g_1 g_2)),$$

and so $f_2 \circ f_1$ is an isomorphism, meaning G and K are isomorphic. $\boxed{J\tau}$

Claim (Part A).

$$\mathbb{Z}_6 \cong \mathbb{Z}_7^* \cong \mathcal{U}_9.$$

Proof. Let $f : \mathbb{Z}_6 \to \mathbb{Z}_7^*$ be defined as $f(x) = 3^x$, and $g : \mathbb{Z}_6 \to \mathcal{U}_9$ be defined as $g(x) = 2^x$. The functions are both seen to be bijective from the diagram below.



Now, observe that

$$f(a) * f(b) = 3^a 3^b = 3^{a+b} = f(a+b)$$

and

$$g(a) \star g(b) = 2^a 2^b = 2^{a+b} = g(a+b).$$

Thus $\mathbb{Z}_6$ is isomorphic to $\mathbb{Z}_7^*$ and $\mathcal{U}_9$, and by Lemma 5 our claim follows.

$\boxed{J\tau}$

Lemma 6. *Isomorphism is identity preserving.*

Proof. Let G and H be isomorphic groups with $f : G \to H$ being an isomorphism. We have that $f(e_*) \diamond f(a) = f(e_* * a)$ for $a \in G$. This gives us $f(e_*) \diamond f(a) = f(a)$ which implies that $f(e_*)$ is the identity of H by Lemma 3. $\boxed{J\tau}$

Lemma 7. *If G and H are isomorphic finite groups, then they contain an equal number of elements that are their own inverses.*

Proof. We define $D(G)$ to be the *doubling constant* of a finite group G to be the number of elements in G that are their own inverses.

Let $f : G \to H$ be an isomorphism between finite groups. We have that $f(a) \diamond f(a) = f(a * a)$. Assume that a is an element in G such that $a * a = e_*$. Thus we have that

$$f(a) \diamond f(a) = f(e_*).$$

This then gives us that $f(a) \diamond f(a) = e_\diamond$ which implies that $f(a)$ is its own inverse, and because f is a bijection, for each a with that property in G there is distinct $f(a)$ in H with that property. Or that $D(H) \geq D(G)$. The other direction can be done symmetrically. $\boxed{J\tau}$

Claim (Part C)**.** *D_6 and A_4 are not isomorphic to each other.*

Proof. In D_6, there are seven elements that are their own inverses, but in A_4 there are only four, and so by Lemma 7 our claim follows. $\boxed{J\tau}$

Claim (Part D)**.** *$\mathbb{Z}$ is not isomorphic to $\mathbb{Q}$.*

Proof. Assume there exists some isomorphism f from $\mathbb{Z}$ to $\mathbb{Q}$. Let q be the rational number satisfying $f(1) = q$. Now, note that for any rational q, the value $q/2$ is rational and thus there is an integer m such that $m = f^{-1}(q/2)$, but we now have that

$$f(1) = q = \frac{q}{2} + \frac{q}{2} = f(m) + f(m) = f(m + m) = f(2m),$$

and because f is bijective this implies that $1 = 2m$, however, this cannot be as this would mean that 2 divides 1, which cannot be. $\boxed{J\tau}$

Problem 12, Chapter 15

Lemma 8.

$$(a * b)^{-1} = b^{-1}a^{-1}$$

Proof. This can be seen to hold as

$$(a * b) * (b^{-1}a^{-1}) = (a * (b * b^{-1}) * a^{-1}) = a * e_* * a^{-1} = a * a^{-1} = e_*$$

$\boxed{J\tau}$

Claim (Part A)**.** *Elementary Abelian 2-Groups are abelian.*

Proof. To show this, we consider some $a, b \in G$ where G is an Elementary Abelian 2-Group. We have the following:

$$a * b,$$

Elementary Abelian 2-Group:

$$= (a * b)^{-1},$$

Lemma 8:

$$= b^{-1}a^{-1},$$

Elementary Abelian 2-Group:

$$= b * a.$$

$\boxed{J\tau}$

Claim (Part B)**.** *Divisors of* 24.

Remark. On my website's third challenge problem set I offer a problem that contains multiple variations of this problem.
https://jacobterkel.github.io/ChallengeProblemsSet3.pdf