Chapter 2 Homework

Homework #2.1 - Math 676

Maddie Wehn

#Math 676/Chapter 2

- **Section 2.1 - Introduction to Sets:** This is meant to be a review section, just use it a a reference when solving the assigned exercises.
  - Do exercises 9, 16, 17.
  - Choose two exercises among 18, 19, 20a, 20b, 21a, 21b, 21c, and 21d.

9) Provide some examples to explain the union, the intersection, and the difference of two (or more) sets, and the complement of a set in another set.

Let $A = \{1, 3, 5, 6, 7, 10\}$
$B = \{1, 2, 5, 8, 9, 12\}$

$U = \{x \in \mathbb{N} \mid 1 \leq x \leq 15\}$

The union is every element in both A or B.
So, $A \cup B = \{1, 2, 3, 5, 6, 7, 8, 9, 10, 12\}$

The intersection is every element in A and B.
So $A \cap B = \{1, 5\}$

The Difference $(A - B)$ is all elements in A but Not in B.
$A - B = \{3, 6, 7, 10\}$
$B - A = \{2, 8, 9, 12\}$

The Complement is all elements in U that aren't in A
$A^c = \{2, 4, 8, 9, 11, 12, 13, 14, 15\}$
$B^c = \{3, 4, 6, 7, 10, 11, 13, 14, 15\}$

---

16) Let A, B, C be three sets. Prove the following set identity via double inclusion.

$$(B\backslash A) \cup (C\backslash A) = (B \cup C)\backslash A$$

by using double inclusion.

Hint. We prove the inclusion $(B\backslash A) \cup (C\backslash A) \subseteq (B \cup C)\backslash A$ leaving the other one as an exercise.

Let us assume $x \in (B\backslash A) \cup (C\backslash A)$, we want to show that $x \in (B \cup C)\backslash A$. Let us translate $x \in (B\backslash A) \cup (C\backslash A)$ into words:

"x is in B (but not in A) or x is in C (but not in A)".

We can tell for sure that x is not in A since, being in A is not allowed in both cases, moreover, we know that x is in B or in C, therefore we can say that

"x is in B or in C, but x is not in A".

Since the last sentence translates as $x \in (B \cup C)\backslash A$, we have proved the inclusion $(B\backslash A) \cup (C\backslash A) \subseteq (B \cup C)\backslash A$.

Pf: We now need to prove $(B \cup C)\backslash A \subseteq (B\backslash A) \cup (C\backslash A)$.

Assume $x \in (B \cup C)\backslash A$. This means that $x \in B \cup C$ and $x \notin A$. Since $x \in B \cup C$, $x \in B$ or $x \in C$.

Cases.

① Let $x \in B$. Then, we know that $x \in B\backslash A$, since $x \notin A$ by what we said above. Since $x \in B\backslash A$, $x \in (B\backslash A) \cup (C\backslash A)$,
So $(B \cup C)\backslash A \subseteq (B\backslash A) \cup (C\backslash A)$

② WLOG, if $x \in C$, $x \in (B\backslash A) \cup (C\backslash A)$, using the same argument above.
Thus, $(B \cup C)\backslash A \subseteq (B\backslash A) \cup (C\backslash A)$

So, since $(B \cup C)\backslash A \subseteq (B\backslash A) \cup (C\backslash A)$ and $(B\backslash A) \cup (C\backslash A) \subseteq (B \cup C)\backslash A$

$$(B\backslash A) \cup (C\backslash A) = (B \cup C)\backslash A$$

∎

17) Let $A_i = \{1, 2, 3, \ldots, i\}$ for $i = 1, 2, 3, \ldots$. Determine the following sets:

(a) $\bigcup_{i=1}^{n} A_i$ = A_n

$A_1 = \{1\}$
$A_2 = \{1, 2\}$
$A_3 = \{1, 2, 3\}$
$\vdots$
$A_n = \{1, 2, 3, \ldots, n\}$

Since union of a family is all elements in at least 1 set, We know that since n is the largest index, A_n will have elements $1-n$, all of which are in $n-i$, where $1 \leq i \leq n-1$.

(b) $\bigcap_{i=1}^{n} A_i$ = 1

$A_1 = \{1\}$
$A_2 = \{1, 2\}$
$A_3 = \{1, 2, 3\}$
$\vdots$
$A_n = \{1, 2, 3, \ldots, n\}$

Since the intersection of a family is all elements that appear in every set, the only element is 1, as every other set A_k has additional numbers over A_{k-1}.

---

18) Complete the proof of Proposition 2.1.31 by demonstrating the following statement.
Let $\mathcal{A} := \{A_i\}_{i \in I}$ be a family of sets. Then we have the following inclusion for any $j \in I$:

Show if x then x

$$\bigcap_{i \in I} A_i \subseteq A_j.$$

Pf: Let $x \in \bigcap_{i \in I} A_i$. This means that $x \in A_i$ for all $i \in I$. Therefore it follows that $x \in A_j$, because $j \in I$.

So, $\bigcap_{i \in I} A_i \subseteq A_j$

---

19) Complete the proof of Proposition 2.1.32 by demonstrating the following statement.
Let $\mathcal{A} := \{A_i\}_{i \in I}$ be a family of sets relative to a universal set U. Then we have the following identity:

Show $\subseteq$ and $\supseteq$

$$\left(\bigcap_{i \in I} A_i\right)^c = \bigcup_{i \in I} (A_i)^c.$$

Pf: ① $\subseteq$ Let $x \in \left(\bigcap_{i=I} A_i\right)^c$. This means that $x \notin \bigcap_{i=I} A_i$. So, for atleast one $i \in I$, $x \notin A_i$.

Since $x \notin A_i$, $x \in (A_i)^c$. Because x is an element of atleast 1 $(A_i)^c$, $x \in \bigcup_{i \in I} (A_i)^c$

Thus, $\left(\bigcap_{i=I} A_i\right)^c \subseteq \bigcup_{i \in I} (A_i)^c$

② $\supseteq$ Let $x \in \bigcup (A_i)^c$ This means that $x \in (A_i)^c$ for at least 1 $i \in I$. So, for at least 1 $i \in I$, $x \notin A_i$. Therefore $x \notin \bigcap_{i=I} A_i$, so $x \in \left(\bigcap_{i=I} A_i\right)^c$.

Thus, $\left(\bigcap_{i=I} A_i\right)^c \supseteq \bigcup_{i \in I} (A_i)^c$

Since We have proven both inclusions, we know that $\left(\bigcap_{i=I} A_i\right)^c = \bigcup_{i \in I} (A_i)^c$. ∎

Homework #2.2 - Math 676

Mabie Kuehn

Section 2.2 - Introduction To Functions: This is meant to be a review section, just use it as a reference when solving the assigned exercises.

- Do exercises 10, 11, 12.
- Choose one exercise among 13, 14, 15.

10)

Consider the function

$$\begin{aligned} f : \mathbb{Q}[x]\backslash\{0\} &\to \mathbb{Z} \\ P(x) &\mapsto \deg\left(P(x)\right). \end{aligned}$$

In other words, f assigns to each non-zero polynomial, its degree. Determine $\mathrm{Im}(f)$ and $f^{-1}(3)$. (No need to prove your answer.)

$\mathrm{Im}(f) = \mathbb{N}$ → constant, deg 0; linear, deg 1; ⋮

$f^{-1}(3) = \{ ax^3 + bx^2 + cx + d \mid a \neq 0;\ a,b,c,d \in \mathbb{Q} \}$

---

11)

Let S be the set of non-negative integers less than 100. We can define the set S as a list of elements:

$$S := \{0, 1, 2, 3, \ldots, 98, 99\},$$

while, in set builder notation, we can define the set S as:

$$S := \{x \in \mathbb{Z} | 0 \leq x < 100\}.$$

Let us define a function $f : S \to S$. Let x be an element of x, we can write $x = 10a + b$, where a and b are digits (we define a digit as an integer from 0 to 9). By using the function notation (2.1), we define f as follows:

$$\begin{aligned} f : S &\to S \\ 10a + b &\mapsto a \cdot b. \end{aligned}$$

In other words, we take a two-digit integer (where integers with a single digit are considered two-digit integers with the first digit being equal to 0) and we multiply its digits. For example, we have $f(26) = 2 \cdot 6 = 12$.

(a) Determine whether the function f is one-to-one. If yes, prove that f is one-to-one, otherwise provide a counter-example.

f is not injective. Let $x_1 = 12$ and $x_2 = 21$ since $x_1 \neq x_2$, $f(x_1) \neq f(x_2)$. However, $f(x_1) = 1 \cdot 2 = 2$ and $f(x_2) = 2 \cdot 1 = 2$. Since $f(x_1) = f(x_2)$, f is not 1-1.

(b) Determine whether the function f is onto. If yes, prove that f is onto, otherwise provide a counter-example.

f is not surjective. The largest 2 digit number is 99. This also gives the largest $f(x)$. $f(99) = 9 \cdot 9 = 81$. Since 81 is the largest $f(x)$, f does not map to 82, 83, ..., 99. So, f is not onto.

↳ (Also other values smaller than 82!)

12) Let us define the function

$$f : \mathbb{R}^+ \to \mathbb{R}^+ \quad (0,\infty)$$
$$x \mapsto e^x$$

where $\mathbb{R}^+$ is the set of positive real numbers and e is the Euler's number

$$2.71828182845904523536028747135 27\ldots$$

(a) Determine whether the function f is one-to-one. If yes, justify your answer, otherwise provide a counter-example.

Pf Let $x_1, x_2 \in \mathbb{R}^+$. Assume $f(x_1) = f(x_2)$. We want to show that $x_1 = x_2$.

$$f(x_1) = f(x_2)$$
$$e^{x_1} = e^{x_2}$$
$$\ln(e^{x_1}) = \ln(e^{x_2})$$
$$x_1 = x_2 \checkmark$$

So, f is one-to-one.

(b) Determine whether the function f is onto. If yes, justify your answer, otherwise provide a counter-example.

We know $f(x) = e^x$ $\quad (1 = e^x)$

$y = e^x$

$\ln y = x$

However, if $y = 1$, $x = 0$, and $0 \notin \mathbb{R}^+$, So f does not map to 1, so it is not onto.

(c) Is f bijective? Justify your answer.

f is not bijective, because it is not both 1-1 and onto, it is only 1-1.

---

13) Let A, B, and C be three sets, and let $f : A \to B$ and $g : B \to C$ be two functions. Assume that $g \circ f : A \to C$ is one-to-one.

(a) Show that f is one-to-one.

We are given that $g \circ f : A \to C$ is 1-1. This means that if $(g \circ f)(x_1) = (g \circ f)(x_2)$, then $x_1 = x_2$, for $x_1, x_2 \in A$.
$g(f(x_1)) = g(f(x_2))$

Pf Let $x_1, x_2 \in A$. Assume $f(x_1) = f(x_2)$. If we apply g to both sides, $g(f(x_1)) = g(f(x_2))$, so by our given assumption, $x_1 = x_2$. So, f is 1-1.

(b) Give an example where $g \circ f$ in one-to-one, but g is not one-to-one.

Let $A = \mathbb{N}$, $B = \mathbb{Z}$, $C = \mathbb{N}$

$f : \mathbb{N} \to \mathbb{Z}$, $x \to x$

Clearly, f is 1-1, since it just maps x to itself.

$g : \mathbb{Z} \to \mathbb{N}$, $x \to |x|$

not 1-1

$g(-1) = g(1)$

$|-1| = |1|$

but $-1 \neq 1$

$g \circ f : \mathbb{N} \to \mathbb{N}$

Is 1-1: $g(f(x)) = g(x) = |x| = x$

$f(x)$: identity

all $x \in \mathbb{N}$ are non-negative, so there are no values that would map to a value already mapped.

Homework #2.3 - Math 676

Mabie Kuehn

Section 2.3 - Basic Properties of Groups.

- Choose 6 exercises.

8) Prove the cancellation laws, Theorem 2.3.8.

Theorem 2.3.8. Cancellation Property In a group G we have:

1. if $a \cdot b = a \cdot c$ then $b = c$;
2. if $b \cdot a = c \cdot a$ then $b = c$.

The above properties are called *left and right cancellation laws.*

Pf Let G be a group with identity element e, and $a, b, c \in G$.

① If $a \cdot b = a \cdot c$, then $b = c$. * Let a^{-1} be the inverse of a. Multiply both sides on the left by a^{-1}.

$a^{-1} \cdot (a \cdot b) = a^{-1} \cdot (a \cdot c)$ * Groups are associative.

$(a^{-1} \cdot a) \cdot b = (a^{-1} \cdot a) \cdot c$ * We know $a^{-1} \cdot a = e$

$e \cdot b = e \cdot c$ * $e \cdot x = e$

$b = c$. ✓

② If $b \cdot a = c \cdot a$, then $b = c$. * Let a^{-1} be the inverse of a. Multiply both sides on the right by a^{-1}.

$(b \cdot a) \cdot a^{-1} = (c \cdot a) \cdot a^{-1}$ * Groups are associative.

$b \cdot (a \cdot a^{-1}) = c \cdot (a \cdot a^{-1})$ * We know $a \cdot a^{-1} = e$

$b \cdot e = c \cdot e$ * $x \cdot e = e$

$b = c$ ✓

---

9) Let G be a group and let a and b be two elements of G. Prove that the equation $ax = b$ has a unique solution in G. $a, b \in G$.

Pf: First, we need to prove that there exists a solution:

$a \cdot x = b$ * We know that b/c $a \in G$, $a^{-1} \in G$, where a^{-1} is the inverse of a. Multiply both sides on the left by a^{-1}.

$a^{-1} \cdot (a \cdot x) = a^{-1} \cdot b$ * Associativity

$(a^{-1} \cdot a) \cdot x = a^{-1} \cdot b$ * $a^{-1} \cdot a = e$

$e \cdot x = a^{-1} \cdot b$ * $e \cdot x = x$

$x = a^{-1} \cdot b$.

So there exists a solution

To prove its unique, let x_1 and x_2 be two solutions. Thus $a \cdot x_1 = b$ and $a \cdot x_2 = b$

Since both equate to b, we know that $a \cdot x_1 = a \cdot x_2$ * left cancellation

$x_1 = x_2$ //

Thus, there can only be one solution for x.

So, $x = a^{-1}b$, and we have shown $ax = b$ has a unique solution in G.

4) In the following, determine the order of the given elements in the given group.

(a) 3 in $\mathbb{Z}_{15}$ $e=0$ (add mod 15)

$3+3=6$
$6+3=9$
$9+3=12$
$12+3=0$ (15%15)

So, $|3|=5$ in $\mathbb{Z}_{15}$

(b) i in $\mathbb{C}^*$ $e=1$ (multiplication)

$i \cdot i = i^2 = -1$
$-1 \cdot i = -i$
$-i \cdot i = -(-1) = 1$

So $|i|=4$ in $\mathbb{C}^*$

(c) $\sqrt{2}$ in $\mathbb{R}^*$ $e=1$ (multiplication)

$\sqrt{2} \cdot \sqrt{2} = 2$
$2 \cdot \sqrt{2} = 2\sqrt{2}$
$2\sqrt{2} \cdot \sqrt{2} = 2 \cdot 2 = 4$
$4 \cdot \sqrt{2} = 4\sqrt{2}$
$\vdots$

We can see that we will never multiply $\sqrt{2}$ to reach e.

So, $|\sqrt{2}|$ is infinite in $\mathbb{R}^*$

---

14) Write the Cayley table of $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

$\mathbb{Z}_2 \oplus \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1)\}$ Sum mod 2 in both coordinates

+	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,1)	(1,0)	(1,1)
(0,1)	(0,1)	(0,0)	(1,1)	(1,0)
(1,0)	(1,0)	(1,1)	(0,0)	(0,1)
(1,1)	(1,1)	(1,0)	(0,1)	(0,0)

---

17) Determine the order of the group $\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$.

Remark 2.3.26. We mention without proof the following two statements that may already be intuitive.

- If $|G_1| = n$ and $|G_2| = m$ then $|G_1 \times G_2| = nm$.

In other words, if the group G_1 has n elements and G_2 has m elements, then the external direct product $G_1 \times G_2$ has nm elements.

We know $|\mathbb{Z}_2| = 2$ $(0,1)$, $|\mathbb{Z}_3| = 3$ $(0,1,2)$, $|\mathbb{Z}_5| = 5$ $(0,1,2,3,4)$.

We know that $|\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5| = |\mathbb{Z}_2| \times |\mathbb{Z}_3| \times |\mathbb{Z}_5| = 2 \cdot 3 \cdot 5 = 30$

20) Determine the order of $(2,2,2)$ in $\mathbb{Z}_3 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_{15}$.

e=0

Order 2 in $\mathbb{Z}_3$: $2+2=1$ (4%3)
$1+2=0$ (3%3)

$|2|=3$

Order 2 in $\mathbb{Z}_9$: $2+2=4$
$4+2=6$
$6+2=8$
$8+2=1$ (10%9)
$1+2=3$
$3+2=5$
$5+2=7$
$7+2=0$ (9%9)

$|2|=9$

Order 2 in $\mathbb{Z}_{15}$: $2+2=4$
$4+2=6$
$6+2=8$
$8+2=10$
$10+2=12$
$12+2=14$
$14+2=1$ (16%15)
$1+2=3$
$3+2=5$
$5+2=7$
$7+2=9$
$9+2=11$
$11+2=13$
$13+2=0$ (15%15)

$|2|=15$

The $|(2,2,2)| = \text{lcm}(3,9,15) = 45$

$3 = 3^1$
$9 = 3^2$
$15 = 3^1 \times 5^1$
$\text{lcm} = 3^2 \times 5 = 45$

Homework #2.4 - Math 676

Section 2.4 - Subgroups. You can ignore Center of a Group and Centralizer of an Element.

- Choose 6 exercises.

1) Let G be an abelian group and define

$$H := \{g \in G \mid |g| < \infty\}$$

In other words, H is the set of elements of G of finite order. Prove that the set H is a subgroup of G.

Hint. *Make sure to show that the set H is non-empty and explain where you used the fact that G is abelian.*

Pf: Non-empty: We know that because G is a group, it contains e. Since $|e|=1$, $e \in H$, so H is non-empty.

Closure: Let $a, b \in H$. By def. a, b are also in G. Because $ab \in H$, the orders of a and b are finite, so $|a|=n$, and $|b|=m$.

This means that $a^n = e$ and $b^m = e$ by Definition 2.3.15. We need to show that ab has finite order

Consider

$$(ab)^{mn} = \underbrace{abababab\ldots ab}_{mn \text{ times}} \quad \text{expansion}$$

$$= \underbrace{aaa\ldots a}_{mn \text{ times}}\underbrace{bbb\ldots b}_{mn \text{ times}} \quad \text{because } G \text{ is abelian}$$

$$= a^{mn} b^{mn} \quad \text{Factoring}$$

$$= (a^n)^m (b^m)^n \quad \text{Power Rule}$$

$$= e^m e^n \quad \text{Substitution}$$

$$= e\,e = e \quad \text{Identity Property}$$

So, $ab \in H$.

Inverse: Let $a \in H$, so $a \in G$. We know $|a|$ is finite, so let $|a|=n$. We need to show a^{-1} is in H. $(a^n = e)$

$$a^n = e$$
$$(a^n)^{-1} = e^{-1} \quad \text{inverse}$$
$$(a^{-1})^n = e^{-1} \quad \text{Power of inverse = inverse of power}$$
$$(a^{-1})^n = e \quad \text{Identity}$$

So $|a^{-1}|=n$, so $a^{-1} \in H$.

Thus, H is a subgroup of G. ∎

3) Determine whether the following subsets are subgroups in the corresponding groups. Justify your answer.

(a) $\{0,2\}$ in $\mathbb{Z}_4$, ← nonempty finite subset. (Prove Closed!)

+	0	2
0	0	2
2	2	0

Closed under addition mod 4, so $\{0,2\} \leq \mathbb{Z}_4$

(b) $\{0,2\}$ in $\mathbb{Z}_3$,

+	0	2
0	0	2
2	2	1

Not closed! Since $2+2=1 \pmod 3$, $1 \notin \{0,2\}$, $\{0,2\}$ is not a subgroup of $\mathbb{Z}_3$.

(c) $\{2,4\}$ in $\mathbb{Z}_6$.

	2	4
2	4	0
4	0	2

Not closed! Since $2+4=0 \pmod 6$, and $0 \notin \{2,4\}$, $\{2,4\}$ is not a subgroup of $\mathbb{Z}_6$.

---

4) Give an example of a group G and two subgroups H and K such that $H \cup K$ is not a subgroup of G. Justify your answer.

$G = \mathbb{Z}_6$ ✓ $H = \{0,2,4\}$ ✓ $K = \{0,3\}$ ✓ $H \cup K = \{0,2,3,4\}$

+	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

Closed, so Subgroup!

+	0	3
0	0	3
3	3	0

Closed, so Subgroup!

+	0	2	3	4
0	0	2	3	4
2	2	4	5	0
3	3	5	0	1
4	4	0	1	2

↳ Not closed.

$2+3=5$, but neither $5, 1 \in H \cup K$ so it is not a subgroup!

$4+3=1 \pmod 6$

---

7) Let G be a group and let g be an element of G. Prove the following identity:

$$< g >= \{g^n \mid n \in \mathbb{Z}\}.$$

Proof. It is enough to show that the set $\{g^n \mid n \in \mathbb{Z}\}$ is a subgroup of G and that it is contained in $< g >$ which implies that $< g >= \{g^n \mid n \in \mathbb{Z}\}$ by minimality of $< g >$. We leave the details of the proof to the reader. See Exercise 7. □

Pf: Let $H = \{g^n \mid n \in \mathbb{Z}\}$ We want to show that $H \leq G$.

Non-empty: We know that H is nonempty. Since $n \in \mathbb{Z}$, let $n=0$. So $g^0 = e$, so since $e \in H$, H is non-empty

Closure: Let $g \in G$, and $g^m, g^n \in H$ s.t. $m,n \in \mathbb{Z}$. We want to show $g^m g^n \in H$.

$g^m g^n = g^{m+n}$ by product rules of exponents. Since $m+n \in \mathbb{Z}$, $g^m g^n \in H$.

Inverse: Let $g \in G$, and $g^n \in H$. Show inverse of $g^n \in H$.

$(g^n)^{-1} = g^{-n}$. Since $-n \in \mathbb{Z}$, $g^{-n} \in H$.

Thus $H \leq G$.

Now, show $H = \langle g \rangle$.

$\supseteq$ By definition, $\langle g \rangle$ is the smallest subgroup containing g, so any subgroup with g must have $\langle g \rangle$. Since $g^1 = g$ and $g^1 \in H$, $g \in H$. So $H \supseteq \langle g \rangle$.

$\subseteq$ Every element of H is of the form g^n, and $\langle g \rangle$ must have every integer power of g in order to be closed. So, for each $g^n \in H$, $g^n \in \langle g \rangle$, so $H \subseteq \langle g \rangle$.

So, $H = \langle g \rangle$.

Thus, If G is a group and $g \in G$, then $\langle g \rangle = \{ g^n \mid n \in \mathbb{Z} \}$. ∎

---

8) Determine all the elements of the following subgroups.

(a) $< 2 >$ in $\mathbb{Z}_6$, $\langle 2 \rangle = \{0, 2, 4\}$

$\langle 2 \rangle$ $2 + 2 = 4$

$4 + 2 = 0$ ✓ $(6+2) \cdot 2$

(b) $< 3 >$ in $\mathbb{Z}_7$, $\langle 3 \rangle = \{0, 1, 2, 3, 4, 5, 6\} = \mathbb{Z}_7$

$3 + 3 = 6$

$6 + 3 = 2 \pmod 7$ $(9 \bmod 7)$

$2 + 3 = 5$

$5 + 3 = 1 \pmod 7$ $(8 \bmod 7)$

$1 + 3 = 4$

$4 + 3 = 0 \pmod 7$ $(7 \bmod 7)$

(c) $< 4 >$ in $\mathbb{Z}_{10}$. $\langle 4 \rangle = \{0, 2, 4, 6, 8\}$

$4 + 4 = 8$

$8 + 4 = 2 \pmod{10}$ $(12 \bmod 10)$

$2 + 4 = 6$

$6 + 4 = 0 \pmod{10}$ $(10 \bmod 10)$

---

13) Let us consider the function $f : \mathbb{C}^* \to \mathbb{C}^*$ defined as $f(z) = z^3$. Prove that f is a group homomorphism and determine $\ker(f)$. $e = 1 \in \mathbb{C}^*$

Prove f is a group homomorphism: (Show $\phi(a*b) = \phi(a) * \phi(b)$)

Let $a, b \in \mathbb{C}^*$ We want to show that for all $a, b \in \mathbb{C}^*$, $f(ab) = f(a)f(b)$.

By def, $f(a) = a^3$ $f(b) = b^3$. $f(ab) = (ab)^3$

$= a^3 b^3$ Power Rule

$= f(a) f(b)$ Substitution.

So, f is a group homomorphism.

$\ker(f) = \{ z \in \mathbb{C}^* \mid f(z) = 1 \}$, So we need to solve $1 = z^3$

The $\ker(f)$ is all cubic roots of 1. So $\ker(f) = \{1, -\frac{1}{2} + \frac{\sqrt{3}}{2}i, -\frac{1}{2} - \frac{\sqrt{3}}{2}i\}$

From Notes 1.6

where ω is a non real cubic root of 1:

$$\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i,$$

while $\overline{\omega}$ is the conjugate of ω:

$$\overline{\omega} = -\frac{1}{2} - \frac{\sqrt{3}}{2}i,$$

Homework #2.5 - Math 676

Mabie Kuehn

Section 2.5 - Groups of Permutations. You can ignore Center and Centralizer of Symmetric Groups and Cayley's Theorem.

- Choose 6 exercises.

2) Let $\sigma = [3, 2, 1]$ and $\tau = [2, 1, 3]$ be two elements of S_3. Show that $\tau \circ \sigma = [3, 1, 2]$.

$\tau \circ \sigma$: $\tau(\sigma(1)) = \tau(3) = 3$
$\tau(\sigma(2)) = \tau(2) = 1$
$\tau(\sigma(3)) = \tau(1) = 2$

$\tau \circ \sigma = [3, 1, 2]$ ✓

---

3) Evaluate the following operations in S_3:

(a) $[2, 1, 3][2, 1, 3]$

$[2,1,3][2,1,3] = [1, 2, 3]$

(b) $[2, 3, 1][1, 3, 2]$

$[2,3,1][1,3,2] = [2, 1, 3]$

(c) $[2, 3, 1][2, 3, 1]$

$[2,3,1][2,3,1] = [3, 1, 2]$

(d) $[3, 1, 2]^{-1}$

$[3,1,2]^{-1} = [2, 3, 1]$

Check
$[3,1,2][2,3,1] = [1, 2, 3]$ ✓

(e) $[3, 2, 1]^{-1}$

$[3,2,1]^{-1} = [3, 2, 1]$

Check
$[3,2,1][3,2,1] = [1,2,3]$

4) List all the elements of S_4.

$|S_4| = 24$

[1 2 3 4]	[2 1 3 4]	[3 1 2 4]	[4 1 2 3]
[1 2 4 3]	[2 1 4 3]	[3 1 4 2]	[4 1 3 2]
[1 3 2 4]	[2 3 1 4]	[3 2 1 4]	[4 2 1 3]
[1 3 4 2]	[2 3 4 1]	[3 2 4 1]	[4 2 3 1]
[1 4 2 3]	[2 4 1 3]	[3 4 1 2]	[4 3 1 2]
[1 4 3 2]	[2 4 3 1]	[3 4 2 1]	[4 3 2 1]

---

5) For every element of S_4, determine its inverse, in particular, list all permutations which are "self-inverse", more precisely, determine all the elements $\sigma \in S_4$ such that $\sigma \circ \sigma = \text{id}$. Then write all the permutations in S_4 which are self-inverse in cycle notation. Do you notice anything peculiar about the self-inverse elements of S_4? Can you guess a generalization for S_n?

Perm	Inverse	Cycle	Perm	Inverse	Cycle
[1 2 3 4]	[1 2 3 4] *	( ) = e	[3 1 2 4]	[2 3 1 4]	
[1 2 4 3]	[1 2 4 3] *	(3 4)	[3 1 4 2]	[2 4 1 3]	
[1 3 2 4]	[1 3 2 4] *	(2 3)	[3 2 1 4]	[3 2 1 4] *	(1 3)
[1 3 4 2]	[1 4 2 3]	(2 4 3) → (2 3 4)	[3 2 4 1]	[4 2 1 3]	
[1 4 2 3]	[1 3 4 2]	(	[3 4 1 2]	[3 4 1 2] *	(1 3)(2 4)
[1 4 3 2]	[1 4 3 2] *	(2 4)	[3 4 2 1]	[4 3 1 2]	
[2 1 3 4]	[2 1 3 4] *	(1 2)	[4 1 2 3]	[2 3 4 1]	
[2 1 4 3]	[2 1 4 3] *	(1 2)(3 4)	[4 1 3 2]	[2 4 3 1]	
[2 3 1 4]	[3 1 2 4]		[4 2 1 3]	[3 2 4 1]	
[2 3 4 1]	[4 1 2 3]		[4 2 3 1]	[4 2 3 1] *	(1 4)
[2 4 1 3]	[3 1 4 2]		[4 3 1 2]	[3 4 2 1]	
[2 4 3 1]	[4 1 3 2]		[4 3 2 1]	[4 3 2 1] *	(1 4)(2 3)

All of the self-inverse elements only contain 2 cycles (except for the identity). Also, no perms that switch 3 elements around ([1 3 4 2] for example) are self-inverse elements.

In General, all elements for S_n that are self-inverse elements will only contain transpositions, so it can be undone in one move.

13) Determine the order of $[3, 5, 1, 2, 4]$ is S_5.

Cycle Notation: $(1\,3)(2\,4\,5)$ → Order is lcm of the orders of disjoint
2-cycle 3-cycle

$\text{lcm}(2,3) = 6$

Order of $[3\,5\,1\,2\,4] = 6$

---

14) Determine the order of $(2, 4, 5)(4, 1, 3)$ in S_5.

Cycles are not disjoint! Composition of Cycles (Right to Left): $[\underline{3}\ \underline{4}\ \underline{5}\ \underline{1}\ \underline{2}]$

$1 \to 3 \to 3$
$2 \to 2 \to 4$
$3 \to 4 \to 5$
$4 \to 1 \to 1$
$5 \to 5 \to 2$

Permutation: $[3,4,5,1,2] \overset{\text{cycle}}{=} (1,3,5,2,4)$

5-cycle!

Order of $(2,4,1)(4,1,3) = 5$

Check: (413) (245) ✓

$[1\,2\,3\,4\,5] \to [\underline{3}\ \underline{2}\ \underline{4}\ \underline{1}\ \underline{5}][3\ 4\ 5\ 1\ 2]$

Homework #2.6 - Math 676

Section 2.6 - Cosets and Lagrange's Theorem. You can ignore Example 2.6.9 about D6.

- Choose 3 exercises.

1)

List all the elements of each right cosets of $H = \{e, (1,2)\}$ in S_3 and all the elements of each left coset of H is S_3:

Note. In this example you will see that the left cosets of a subgroup are not always equal to the right cosets.

$S_3 = \{e, (12), (13), (23), (123), (132)\}$

Left Cosets

eH: $e \cdot e = e$, $e \cdot (12) = (12)$ $\rightarrow$ $eH = (12)H = \{e, (12)\}$

$(13)H$: $(13)e = (13)$, $(13)(12) = (123)$ $\rightarrow$ $(13)H = \{(13)(123)\}$

$(23)H$: $(23)e = (23)$, $(23)(12) = (132)$ $\rightarrow$ $(23)H = \{(23)(132)\}$

Right Cosets:

He: $e \cdot e = e$, $(12) \cdot e = (12)$ $\rightarrow$ $\{e, (12)\}$

$H(13)$: $e \cdot (13) = (13)$, $(12)(13) = (132)$ $\rightarrow$ $\{(13)(132)\}$

$H(23)$: $e(23) = (23)$, $(12)(23) = (123)$ $\rightarrow$ $\{(23)(123)\}$

---

8)

Let G be a group with an element of order 40 and an element of order 26. What is the minimum possible order of G? Justify your answer.

We know that if we have an element $g \in G$ the order of g divides $|G|$. Thus $|G|$ is a multiple of g. Since we have two elements, $|G|$ is a multiple of both, so we can find lcm of those elements' order.

$26 = 2 \cdot 13$ (2, 13)

$40 = 2^3 \cdot 5$ (2^3, 5)

So $\text{lcm}(26, 40) = 2^3 \cdot 5 \cdot 13 = 520$

So the minimum possible order of G is 520.

(27)

Show that the group $G = \{e, a, b, c\}$ satisfying the following Cayley table:

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Write the Cayley table of $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

$\mathbb{Z}_2 \oplus \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1)\}$

$+$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

A *group homomorphism* is a function $\phi : G \to H$ between two groups $(G, \oplus)$ and $(H, \odot)$, such that for all $a, b \in G$ we have:

$$\phi(a \oplus b) = \phi(a) \odot \phi(b).$$

In other words, the function ϕ preserves the operation.

To prove that G is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, we need to show that the group homomorphism $\phi: G \to H$ is bijective.

Let $\phi : G \to \mathbb{Z}_2 \oplus \mathbb{Z}_2$ be defined by:

$\phi(e) = (0,0)$
$\phi(a) = (0,1)$
$\phi(b) = (1,0)$
$\phi(c) = (1,1)$

Well-Defined: We know this is a well-defined function because each element in the domain has a unique corresponding element in the co-domain.

Homomorphism Show that for all $a, b \in G$, $\phi(a \cdot b) = \phi(a) + \phi(b)$

$e \cdot a$, $e \cdot b$, $e \cdot c$:
↳ $\phi(e \cdot a) = \phi(a) = (0,1)$ (same if reversed $\to \phi(a \cdot e) = \phi(a)$)
$\phi(e) + \phi(a) = (0,0) + (0,1) = (0,1)$ ✓

$b \cdot c$ $(c \cdot b)$:
↳ $\phi(b \cdot c) = \phi(a) = (0,1)$
$\phi(b) + \phi(c) = (1,0) + (1,1) = (0,1)$ ✓

$a \cdot a$ $(b \cdot b, c \cdot c)$:
↳ $\phi(a \cdot a) = \phi(e) = (0,0)$
$\phi(a) + \phi(a) = (0,1) + (0,1) = (0,0)$ ✓

$a \cdot c$ $(c \cdot a)$:
↳ $\phi(a \cdot c) = \phi(b) = (1,0)$
$\phi(a) + \phi(c) = (0,1) + (1,1) = (1,0)$ ✓

$a \cdot b$ $(b \cdot a)$:
↳ $\phi(a \cdot b) = \phi(c) = (1,1)$
$\phi(a) + \phi(b) = (0,1) + (1,0) = (1,1)$ ✓

Injective: Since each input maps to a different output, if $\phi(x) = \phi(y)$, then $x = y$. So, by definition, ϕ is 1-1.

Surjective: Since each element in $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ is mapped to, we know that ϕ is onto.

Since ϕ is a bijective homomorphism, G is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Homework #2.7 - Math 676

Section 2.7 - Normal Subgroups. You can ignore Example 2.7.13.

- Choose 3 exercises.

4) Determine all the normal subgroups of $S_3 = \{e, (12), (13), (23), (123), (132)\}$

Subgroups of S_3: $\{e\}$ (trivial), S_3, $\{e, (12)\}$, $\{e, (13)\}$, $\{e, (23)\}$, $A_3 = \{e, (123), (132)\}$

$\{e\}$ is Normal because $geg^{-1} \in \{e\}$ for each $g \in S_3$. $(geg^{-1} = gg^{-1} = e \in \{e\})$

S_3 is normal because $gS_3g^{-1} \in S_3$ for each $g \in S_3$

$\{e, (12)\}$ → since $geg^{-1} = e \in H$, if $g(12)g^{-1} \in H$ $\forall g \in S_3$, H is normal. $(13)(12)(13) = (23) \notin H$, so H is not normal.

By Similar Reasoning, Since $(12)(13)(12) = (23)$, and $(12)(23)(12) = (13)$, then $\{e, (23)\}$ and $\{e, (13)\}$ are not normal.

A_3: We know that A_3 is normal by Example 2.7.8.

Thus $\{e\}$, S_3, A_3 are all normal subgroups of S_3.

---

8) Prove that the function $\phi : S_n \to \mathbb{Z}_2$ defined for every element σ of S_3 as:

$$\phi(\sigma) = 0 \text{ if the permutation } \sigma \text{ is even,}$$
$$\phi(\sigma) = 1 \text{ if the permutation } \sigma \text{ is odd.}$$

is a group homomorphism.

Definition 2.5.27. A permutation that can be written as a product of an even (odd) number of transpositions is called an even (odd) permutation.

Let σ_1 and σ_2 be elements of S_n

Let σ_1 and σ_2 be even perms. So, σ_1 has $2n$ transpositions and σ_2 has $2m$ transpositions, where $m, n \in \mathbb{Z}$.

$\phi(\sigma_1 \cdot \sigma_2) = 0$, because $2n + 2m = 2(m+n)$ transpositions, so $\sigma_1 \cdot \sigma_2$ is even
$\phi(\sigma_1) \cdot \phi(\sigma_2) = 0 + 0 = 0$ ✓

Let σ_1 and σ_2 be odd perms. So, σ_1 has $2m+1$ transpositions and σ_2 has $2n+1$ transpositions, where $m, n \in \mathbb{Z}$.

$\phi(\sigma_1 \cdot \sigma_2) = 0$, because $(2m+1) + (2n+1) = 2(m+n+1)$ transpositions, so $\sigma_1 \cdot \sigma_2$ is even
$\phi(\sigma_1) \cdot \phi(\sigma_2) = 1 + 1 = 0$ ✓

Let σ_1 be and odd perm and σ_2 be an even perm. So, σ_1 has $2m+1$ transpositions and σ_2 has $2n$ transpositions, where $m, n \in \mathbb{Z}$.
(Similar reasoning for σ_2 = odd and σ_1 = even)

$\phi(\sigma_1 \cdot \sigma_2) = 1$, because $2m + 1 + 2n = 2(m+n) + 1$ transpositions, so $\sigma_1 \cdot \sigma_2$ is odd.
$\phi(\sigma_1) \cdot \phi(\sigma_2) = 1 + 0 = 1$ ✓

Thus, ϕ is a group homomorphism. ∎//

10) Let $\phi : \mathbb{Z}_{30} \to \mathbb{Z}_{30}$ such that $\ker(\phi) = \{0, 10, 20\}$ and $\phi(23) = 9$. Determine the preimage $\phi^{-1}(9)$.

Since $\phi(23)=9$, we know that $\phi^{-1}(9) = 23 + \ker(\phi)$.

So $\phi^{-1}(9) = 23 + \{0, 10, 20\}$

$23+0=23$

$23+10=33=3$

$23+20=43=13$

$\phi^{-1}(9) = \{3, 13, 23\}$

Homework #2.8 - Math 676

Section 2.8 - Quotient Groups. You can ignore Example 2.8.12, Cauchy's Theorem for Abelian Groups, and Quotient by the Center.

- Choose 3 exercises among 1, 2, 3, 4, 5, and 6.
- Exercise 12.
- Choose 2 exercises among 14, 15, 16.

1) Determine the internal product of the coset $(2,3) < (1,2) >$ with itself in S_3 by listing all the elements.

$\langle (1\ 2) \rangle = \{e, (12)\}$

$(23)\langle(12)\rangle = \{(23)e, (23)(12)\} = \{(23), (132)\}$

$1\to3,\ 2\to1,\ 3\to2$ (132)

So, $(23)\langle(12)\rangle(23)\langle(12)\rangle =$ $= \{e, (12), (13), (123)\}$

	(23)	(132)
(23)	e	(12)
(132)	(13)	(123)

$(23)(23) = 1\to1\to1,\ 2\to3\to2,\ 3\to2\to3$

$(132)(23) = 1\to1\to3,\ 2\to3\to2,\ 3\to2\to1$

$(23)(132) = 1\to3\to2,\ 2\to1\to1,\ 3\to2\to3$

$(132)(132) = 1\to3\to2,\ 2\to1\to3,\ 3\to2\to1$

---

4) Let $G = \mathbb{Z}_{24}$ and let H be the subgroup of $\mathbb{Z}_{24}$ generated by 4. Determine G/H up to isomorphism.

We know that $H = \{0, 4, 8, 12, 16, 20\} = \langle 4 \rangle$

$G/H = \mathbb{Z}_{24}/\langle 4 \rangle = \{0+\langle 4\rangle,\ 1+\langle 4\rangle,\ 2+\langle 3\rangle + 3+\langle 4\rangle 3\}$

$0+\langle 4\rangle = \langle 4\rangle$
$1+\langle 4\rangle = \{1, 5, 9, 13, 17, 21\}$
$2+\langle 4\rangle = \{2, 6, 10, 14, 18, 22\}$
$3+\langle 4\rangle = \{3, 7, 11, 15, 19, 23\}$

} The operation of $\mathbb{Z}_{24}/\langle 4\rangle$ are addition mod 4, so G/H is isomorphic to $\mathbb{Z}_4$.

6)

Let H be a normal subgroup of a group G and define the projection function:

$$\begin{aligned} \phi : G &\to G/H \\ \phi(g) &= gH. \end{aligned}$$

Prove that the function ϕ is a group homomorphism and H is the kernel of ϕ.

Prove ϕ is a group homomorphism: $\phi: G \to G/H$ is a homomorphism if $\forall g_1, g_2 \in G$, $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$

By def of ϕ, $\phi(g_1 g_2) = (g_1 g_2)H$.
Now, we must show $\phi(g_1)\phi(g_2) = (g_1 g_2)H$.

$\phi(g_1)\phi(g_2) = g_1 H g_2 H$ (H is normal - Thm 2.8.8)
$= (g_1 g_2)H$ ✓

So, ϕ is a group homomorphism

Prove $H = \ker(\phi)$:

$\ker(\phi) = \{g \in G \mid \phi(g) = H\}$
$gH = H$

So, $\ker(\phi) = \phi(g) = H$
$gH = H$, which is only true if $g \in H$.

So $\ker(\phi) = H$.

---

12) Prove that the quotient group $\mathbb{R}^*/\{1,-1\}$ (Non-Zero) is isomorphic to the group $\mathbb{R}^+$ (Positive) by providing a surjective group homomorphism $\phi : \mathbb{R}^* \to \mathbb{R}^+$ such that $\{1,-1\}$ is the kernel of ϕ, in other words, by applying Corollary 2.8.18.

Corollary 2.8.18. If $\phi : G \to K$ is a surjective group homomorphism, then the group K is isomorphic to the quotient group $G/\ker(\phi)$.

Pf: Let $\phi: \mathbb{R}^* \to \mathbb{R}^+$ be defined by $\phi(g) = |g|$. To show that ϕ is a group homomorphism, we must show that $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in \mathbb{R}^*$.

- $\phi(ab) = |ab| = |a||b|$ by the properties of absolute value.
- $\phi(a)\phi(b) = |a||b|$ ✓

Since this holds for all $a, b \in \mathbb{R}^*$, ϕ is a group homomorphism.

Now we want to show that ϕ is surjective. Thus, we need to show that each element in $\mathbb{R}^+$ has at least one preimage in $\mathbb{R}^*$.

So for any $b \in \mathbb{R}^+$, find $a \in \mathbb{R}^*$ s.t. $\phi(a) = |a| = b$

Let $a = b$ or $a = -b$. Since b is positive nonzero, both b and $-b \in \mathbb{R}^*$.

$\phi(b) = |b| = b$ $\phi(-b) = |-b| = b$. So ϕ is surjective.

Next, we must show that $\ker(\phi) = \{1, -1\}$. We know that $e \in \mathbb{R}^*$, that $e = 1$, since multiplying by 1 leaves the element unchanged. So, we need to find all $g \in \mathbb{R}^*$ s.t. $\phi(g) = 1$. This only works for $g = 1$ or $g = -1$.

$\phi(1) = |1| = 1$ ✓ $\phi(-1) = |-1| = 1$ ✓

So, $\ker(\phi) = \{1, -1\}$.

Thus, by Corollary 2.8.18, $\mathbb{R}^*/\{1,-1\}$ is isomorphic to $\mathbb{R}^+$. ∎

14) Prove that $\mathbb{Z}_n$ $(n \geq 2)$ is simple if and only if n is prime.

(⇒ ⇐)

Pf: ⇒ If $\mathbb{Z}_n$ is simple, then n is prime.

Since $\mathbb{Z}_n$ is simple, the only normal subgroups are $\{0\}$ and $\mathbb{Z}_n$. We know that the subgroups of $\mathbb{Z}_n$ are generated by the divisors of n. Because $\mathbb{Z}_n$ is abelian, every subgroup is normal. Because the only normal subgroups are $\{0\}$ and $\mathbb{Z}_n$, that means that the only divisors of n are 1 and n. Thus, n is prime

⇐ If n is prime, then $\mathbb{Z}_n$ is simple.

If n is prime, then the only divisors of n are 1 and n. Thus, by Lagrange's Theorem, the order of any subgroups of $\mathbb{Z}_n$ must be a divisor of the order of $\mathbb{Z}_n$. Thus, the only possible subgroups are $\{0\}$ and $\mathbb{Z}_n$.

Thus, $\mathbb{Z}_n$ is simple.

Theorem 2.6.10. Lagrange's Theorem Let G be a finite group and H a subgroup of G. Then the order of H is a divisor of the order of G. Moreover, the number of distinct right (left) cosets of H in G is equal to $|G|/|H|$.

---

15) Prove that the group A_3 is simple. $A_3 = \{e, (123), (132)\}$

Pf: We know that by Lagrange's Thm, the order of any subgroup must divide the order of the group. Since $|A_3| = 3$, subgroups can only be of order 1 or order 3. This means the only possible subgroups are $\{e\}$ and A_3, thus by definition, A_3 is simple.