Homework 3

Walker Bagley and Hayden Gilkinson

February 10, 2023

Section 4

1. Not a group because $\mathscr{G}_3$ fails. Other than 1 and -1, no other inverses are contained by $\mathbb{Z}$
2. Is a group.
3. Not a group because $\mathscr{G}_1$ fails. $\sqrt{(a)\sqrt{bc}} \neq \sqrt{\sqrt{ab}(c)}$
7. The group $G = \langle U_{1000}, \cdot \rangle$ is abelian and has exactly 1000 elements.
10. Let $n\mathbb{Z} = \{nm | m \in \mathbb{Z}\}$
    (a) Show that $G = \langle n\mathbb{Z}, + \rangle$ is a group
    $\mathscr{G}_1$: addition is associative, and all elements of G are a multiple of the same n, so addition is closed
    $\mathscr{G}_2$: $n\mathbb{Z}$ always contains 0, the identity element
    $\mathscr{G}_3$: Any $a \in G$ can be expressed as nm for $m \in \mathbb{Z}$ so $a^{-1} = n(-m)$ which we know is contained in G, so the inverse exists and is closed
    (b) *Proof.*
    $$\text{Let } \phi : \mathbb{Z} \to n\mathbb{Z} \text{ be defined by } \phi(x) = nx$$
    $$\text{Then } \phi \text{ is one to one and onto and } \phi(x+y) = n(x+y) = nx + ny = \phi(x) + \phi(y)$$
    $$\text{Thus, } \langle n\mathbb{Z}, + \rangle \simeq \langle \mathbb{Z}, + \rangle$$
    □
11. Is a group
12. Is a group
13. Is a group
19. $S = \mathbb{R} \backslash \{-1\}$ and $a * b = a + b + ab$
    (a) Show that $*$ is a binary operation
    Proof.
    $$\text{Let } a * b = a + b + ab$$
    $$\text{Then for all } a, b \in S,\ (a * b) \in S \text{ since if } a, b \in \mathbb{R}\backslash\{-1\} \text{ then } (a + b + ab) \in \mathbb{R}\backslash\{-1\}$$
    $$\text{By excluding } -1, \text{ each } a * b \text{ will be assigned its own unique value}$$
    □
    (b) Show that $G = \langle S, * \rangle$ is a group
    $\mathscr{G}_1$: $a * (b * c) = a * (b + c + bc) = a + b + c + bc + ab + ac + abc = (a + b + ab) * c = (a * b) * c$
    $\mathscr{G}_2$: the identity element is 0 since $a * 0 = a + 0 + a(0) = a$ under $\mathbb{R}$
    $\mathscr{G}_3$: $a * a^{-1} = a + a^{-1} + aa^{-1} = 0 \Rightarrow a^{-1} + aa^{-1} = -a \Rightarrow a^{-1}(1 + a) = -a \Rightarrow a^{-1} = -\frac{a}{a+1}$ so any $a \in S$ has an inverse that is also contained in S

(c) $2 * x * 3 = 7 \Rightarrow (2 + x + 2x) * 3 = 7 \Rightarrow 2 + x + 3 + 2x + 6 + 3x + 6x = 7 \Rightarrow 12x = -4 \Rightarrow x = -\frac{1}{3}$

22. $\mathscr{G}_3\mathscr{G}_2\mathscr{G}_1, \mathscr{G}_3\mathscr{G}_1\mathscr{G}_2, \mathscr{G}_1\mathscr{G}_3\mathscr{G}_2$ are not acceptable since $\mathscr{G}_3$ relies on the veracity of $\mathscr{G}_2$. One cannot define an inverse without knowing the identity element.

23. (a) Expand on what it means for $*$ to be associative
    (b) Expand on the three conditions - what exactly they mean. Also a group is a binary structure not a set.
    (c) No mention of associativity and identifies the inverse before the identity, which is required for definition of the inverse. Also a group is a binary structure not a set.
    (d) The operation defined by $*$ is not necessarily addition, but should be associative. Also a group is a binary structure not a set.

25. (a) False
    (b) True
    (c) True
    (d) False
    (e) False
    (f) True
    (g) True
    (h) True
    (i) False
    (j) True

26. Given a common term on both sides a, use it's identity a' ($\mathscr{G}_3$) to cancel it on both sides, leaving the remaining terms.

27. By applying the identity on both sides of each equation, we can get that $x = a' * b$ and $y = b * a'$. We then show uniqueness of x and y by assuming two solutions and showing that they are equal with Theorem 4.15.

28. Given an isomorphism $\phi : G \to G'$, prove that for $a, a' \in G$ that $\phi(a)$ and $\phi(a')$ are inverses

    Proof.

    By definition, $a * a' = e$ in G
    By definition of isomorphism, $\phi(a * a') = \phi(a) *' \phi(a')$
    We have proved before that for $e \in G$, $e' = \phi(e)$ in G'
    Substituting the pair of inverses, $\phi(e) = e' = \phi(a) *' \phi(a')$
    So, $\phi(a)$ and $\phi(a')$ generate the identity element under G'

    □

31. Prove that a group has one idempotent element

    Proof.

    We have proven that every group has exactly one identity element e
    By definition of identity $\forall a \in G$, $a * e = e * a = a$
    We know $e \in G$, so this applies, leaving $e * e = e$
    Then e must be the idempotent element and unique

    □

32. Show that every group with $x * x = e$ for all $x \in G$ is abelian

Proof.

$$\begin{aligned}
\text{Taking any } a, b \text{ in } G, \text{ we want to show that } a * b = b * a \\
\text{We know that } a * b \text{ and } b * a \text{ are both in } G \text{ by definition} \\
\text{By associativity, } (a * b) * (b * a) = ((a * b) * b) * a = (a * (b * b)) * a \\
\text{By inverse, } = (a * e) * a \\
\text{By identity, } = a * a \\
\text{By definition then, } = e \\
\text{If } (a * b) * (b * a) = e, \text{ then by definition, } a * b = b * a \\
\text{Then } G \text{ is commutative and therefore abelian}
\end{aligned}$$

□

33. Prove that for all $a, b \in G$, $(a * b)^n = a^n * b^n$ if $c^n = c * c * c * \ldots c$ for all $c \in G$ and $n \in \mathbb{Z}^+$

Proof.

$$\begin{aligned}
\text{Base case: } n = 1. \text{ Then, } (a * b)^1 = a * b = a^1 * b^1 \\
\text{Assume that for some } n \in \mathbb{Z}^+, (a * b)^n = a^n * b^n \\
(a * b)^{n+1} = (a * b)^n * (a * b) \\
\text{By inductive hypothesis, } = a^n * b^n * (a * b) \\
\text{By association, } = a^n * a * b^n * b \\
\text{By definition of } c^n, \text{ then } = a^{n+1} * b^{n+1}
\end{aligned}$$

□

Section 5

1. Is a subgroup
2. Is not a subgroup because a^{-1} isn't in $\mathbb{Q}^+$
5. Is a subgroup
11. Not a subgroup since it isn't closed under matrix multiplication
12. Is a subgroup
14. (a) Not a subgroup under addition because $e \notin \tilde{F}$
    (b) This is the improper subgroup
20. $G_2 \leq G_8$
    $G_2 \leq G_7$
    $G_2 \leq G_1$
    $G_2 \leq G_4$
    $G_8 \leq G_7$
    $G_8 \leq G_1$
    $G_8 \leq G_4$
    $G_7 \leq G_1$
    $G_7 \leq G_4$
    $G_1 \leq G_4$
    $G_9 \leq G_3$
    $G_3 \leq G_5$
    $G_9 \leq G_5$
    $G_6 \leq G_5$

22.

$$\begin{bmatrix}0 & -1\\-1 & 0\end{bmatrix}\begin{bmatrix}0 & -1\\-1 & 0\end{bmatrix}=\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}\Rightarrow\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}\begin{bmatrix}0 & -1\\-1 & 0\end{bmatrix}=\begin{bmatrix}0 & -1\\-1 & 0\end{bmatrix}\Rightarrow\left\{\begin{bmatrix}0 & -1\\-1 & 0\end{bmatrix},\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}\right\}$$

23.

$$\begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}\begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}=\begin{bmatrix}1 & 2\\0 & 1\end{bmatrix}\Rightarrow\begin{bmatrix}1 & 2\\0 & 1\end{bmatrix}\begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}=\begin{bmatrix}1 & 3\\0 & 1\end{bmatrix}\Rightarrow H=\left\{\begin{bmatrix}1 & n\\0 & 1\end{bmatrix}|n\in\mathbb{Z}\right\}$$

26. G_1 is cyclic with $1, -1$ as generators
G_2 is not cyclic
G_3 is not cyclic
G_4 is cyclic with $6, -6$ as generators
G_5 is not cyclic
G_6 is not cyclic

36. (a)

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

(b) $\langle 0\rangle = \{0\}$
$\langle 1\rangle = \{1,2,3,4,5,0\}$
$\langle 2\rangle = \{2,4,0\}$
$\langle 3\rangle = \{3,0\}$
$\langle 4\rangle = \{4,2,0\}$
$\langle 5\rangle = \{5,4,3,2,1,0\}$

(c) 1 and 5 are generators

(d) 1: $\mathbb{Z}_6 = \langle 1\rangle = \langle 5\rangle$
2: $\langle 2\rangle = \langle 4\rangle$ $\langle 5\rangle$
3: $\langle 0\rangle$

39. (a) True
(b) False
(c) True
(d) False
(e) False
(f) False
(g) False
(h) False
(i) True
(j) False

42. *Proof.*

$$\begin{aligned}\text{There exists some } a\in G \text{ s.t. } G=\langle a\rangle\\ \text{Let some } b\in G' \text{ and there is some } x\in G \text{ s.t. } \phi(x)=b\\ \text{Since } G \text{ is cyclic, we have some } n\in\mathbb{Z} \text{ s.t. } x=a^n\\ b=\phi(a^n)=(\phi(a))^n\in\langle\phi(a)\rangle\\ b\in\langle\phi(a)\rangle\\ H\subseteq\langle\phi(a)\rangle \text{ so } H \text{ is cyclic}\end{aligned}$$

□

44. e is defined in condition 2, so we are unable to assert that $a \cdot a^{-1} = e$ without saying what e is

53. *Proof.* Reflexive: $a \sim a$ because $a \cdot a^{-1} = e$ is in any subgroup
Symmetric: $a \cdot b^{-1} \in H \Rightarrow a, b^{-1} \in H \Rightarrow a^{-1}, b \in H \Rightarrow b \cdot a^{-1} \in H$ since H is closed under the induced operation
Transitive: Let $a \cdot b^{-1} \in H, b \cdot c^{-1} \in H$ so $(a \cdot b^{-1})(b \cdot c^{-1}) = a(b \cdot b^{-1})c^{-1} = a \cdot c^{-1} \in H$ since H is closed under the induced operation □

54. *Proof.*

$$\text{First, } e \in H \text{ and } e \in K \Rightarrow e \in H \cap K$$
$$\text{So, } H \cap K \text{ is nonempty}$$
$$\text{Suppose } a, b \in H \text{ and } a, b \in K, \text{ so } a, b \in H \cap K$$
$$\text{Then } ab \in H \text{ and } ab \in K \text{ so } ab \in H \cap K \text{ making } H \cap K \text{ closed under the binary operation}$$
$$\text{Suppose } c \in H \text{ and } c \in K, \text{ then } c^{-1} \in H \text{ and } c^{-1} \in K, \text{ so } c, c^{-1} \in H \cap K$$
$$\text{Thus } H \cap K \text{ is closed under inverses}$$
$$\text{Additionally, } H \cap K \subseteq H \text{ and } H \cap K \subseteq K, \text{ therefore } H \cap K \leq G$$

□