MTH 343 Homework 2

Philip Warton

April 17, 2020

(1) 3.4.6

Create a multiplication table for $U(12)$. The integers that are co-prime to 12 are $\{1, 5, 7, 11\}$ and their respective equivalence classes. We now compute the multiplication table.

	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

(2) 3.4.7

Let $S = \mathbb{R} \setminus \{-1\}$ and define a binary operation on S by $a * b = a + b + ab$. Prove that $(S, *)$ is an abelian group.

Proof. $\boxed{\text{Commutativity}}$ We want to show that $(S, *)$ is commutative. If $a * b = b * a \forall a, b \in S$, then the group is commutative. Let $a, b \in S$ be arbitrary. Then,

$$\begin{aligned} a * b &= a + b + ab \\ &= b + a + ab \\ &= b + a + ba \\ &= b * a \end{aligned}$$

The group $(S, *)$ is commutative.

$\boxed{\text{Associativity}}$ To show associativity, we must show that $(a * b) * c = a * (b * c) \forall a, b, c \in S$. Let $a, b, c \in S$, then,

$$\begin{aligned} (a * b) * c &= (a + b + ab) * c \\ &= (a + b + ab) + c + (a + b + ab)c \\ &= a + b + c + ab + ac + bc + abc \\ &= a + (b + c + bc) + a(b + c + bc) \\ &= a * (b + c + bc) \\ &= a * (b * c) \end{aligned}$$

The group $(S, *)$ is associative.

$\boxed{\text{Identity}}$ We want to show that $\exists e \in S$ such that $e * a = a * e = a \quad \forall a \in S$. Let $x \in (S = \mathbb{R} \setminus \{1\})$.

Denote the identity element e, then $x * e = x$. This can be written as

$$\begin{aligned} x * e = x &= x + e + xe \\ \implies 0 &= e + xe \\ 0 &= e(1+x) \\ \implies e &= 0 \end{aligned}$$

Since $0 \in S$, and for any $s \in S, 0 * s = s = s * 0$, we have an identity.

$\boxed{\text{Inverse}}$ We want to show that $\forall a \in S, \exists a' : s * s' = e$. Let $a \in S$ be arbitrary, then we want to find a' such that.

$$\begin{aligned} a * a' &= e \\ a + a' + aa' &= 0 \\ a'(1+a) &= -a \\ a' &= \frac{-1}{1+a} \end{aligned}$$

If $a = -1$, then no a' exists, but since $-1 \notin S$, this situation will never occur. The inverse of 0 is $-1 \notin S$, but since 0 is the identity, it need not have an inverse.

$\boxed{\text{Closure}}$ We want to show that $\forall a, b \in S, a * b \in S$. Let $a, b \in S$. Then,

$$a * b = a + b + ab$$

Since $\mathbb{R}$ is closed under addition and multiplication, the only thing we have to check is that it does not ever produce -1. Suppose that $a * b = -1$. Then

$$\begin{aligned} a + b + ab &= -1 \\ a(1+b) + b &= -1 \\ a &= \frac{-1-b}{1+b} \\ a &= \frac{-(1+b)}{(1+b)} \\ a &= -1 \end{aligned}$$

This is a contradiction since $a = -1 \notin S$. Therefore $a * b$ cannot equal -1. Since all of these conditions are met, we say that $(S, *)$ is an abelian group. $\square$

(3) 3.4.21

For each $a \in \mathbb{Z}_n$ find an element $b \in \mathbb{Z}_n$ such that $a + b \equiv 0$ (mod n).

Let $a \in \mathbb{Z}_n$. Then $a \in \{0, 1, \cdots n-1\} = \{n-n, \cdots, n-2, n-1\}$. We can write $a = n - m$ where $m \in \mathbb{N} : 1 \leqslant m \leqslant n$. Define $b = m \in \mathbb{Z}_N$. Then $a + b = n - m + m = n \equiv 0$ (mod n).

(4) 3.4.40

Let G consist of 2×2 matricies of the form

$$\begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix}$$

where $\theta \in \mathbb{R}$. Prove that $G \leq SL_2(\mathbb{R})$.

Proof. Since $G \leq SL_2(\mathbb{R}) \iff ab^{-1} \in G \quad \forall a, b \in G$, we will show the right hand side. Let $A, B \in G$ such that

$$A = \begin{bmatrix} \cos(a) & -\sin(a) \\ \sin(a) & \cos(a) \end{bmatrix}, \qquad B = \begin{bmatrix} \cos(b) & -\sin(b) \\ \sin(b) & \cos(b) \end{bmatrix}$$

Then we know by properties of rotation matricies that

$$B^{-1} = \begin{bmatrix} \cos(-b) & -\sin(-b) \\ \sin(-b) & \cos(-b) \end{bmatrix}$$

Computing AB^{-1} we get the following result,

$$\begin{aligned} AB^{-1} &= \begin{bmatrix} \cos(a) & -\sin(a) \\ \sin(a) & \cos(a) \end{bmatrix} \begin{bmatrix} \cos(-b) & -\sin(-b) \\ \sin(-b) & \cos(-b) \end{bmatrix} \\ &= \begin{bmatrix} \cos(a)\cos(-b) - \sin(a)\sin(-b) & -\cos(a)\sin(-b) - \sin(a)\cos(-b) \\ \sin(a)\cos(-b) + \cos(a)\sin(-b) & \cos(a)\cos(-b) - \sin(a)\sin(-b) \end{bmatrix} \\ &= \begin{bmatrix} \cos(a-b) & -\sin(a-b) \\ \sin(a-b) & \cos(a-b) \end{bmatrix} \in G \end{aligned}$$

Therefore $G \leq SL_2(\mathbb{R})$. □

(5) 3.4.41

Let $G = \{a + b\sqrt{2} : a, b \in \mathbb{Q}, \;\; a \neq 0 \text{ or } b \neq 0\}$. Show $G \leq \mathbb{R}^*$ under multiplication.

Proof. Let $\alpha, \beta \in G$. We want to show that $\alpha\beta^{-1} \in G$. Denote

$$\alpha = a_1 + b_1\sqrt{2}, \quad \beta = a_2 + b_2\sqrt{2}$$

Then $\beta^{-1} = \dfrac{1}{a_2 + b_2\sqrt{2}}$. We can compute the product

$$\begin{aligned} \alpha\beta^{-1} &= (a_1 + b_1\sqrt{2})\left(\frac{1}{a_2 + b_2\sqrt{2}}\right) \\ &= \frac{a_1 + b_1\sqrt{2}}{a_2 + b_2\sqrt{2}} \\ &= \frac{a_1 + b_1\sqrt{2}}{a_2 + b_2\sqrt{2}} \cdot \frac{a_2 - b_2\sqrt{2}}{a_2 - b_2\sqrt{2}} \\ &= \frac{a_1a_2 - a_1b_2\sqrt{2} + a_2b_1\sqrt{2} - 2b_1b_2}{a_2^2 - 2b_2^2} \\ &= \frac{a_1a_2 - 2b_1b_2}{a_2^2 - 2b_2^2}(1) + \frac{a_2b_1 - a_1b_2}{a_2^2 - 2b_2^2}(\sqrt{2}) \end{aligned}$$

We say that this final result is an element of G. Suppose the denominator was equal to 0, then

$$\begin{aligned} a_2^2 - 2b_2^2 &= 0 \\ a_2^2 &= 2b_2^2 \\ |a_2| &= \sqrt{2}|b_2| \\ \implies a_2 \notin \mathbb{Q} &\text{ or } b_2 \notin \mathbb{Q} \qquad \text{(contradiction)} \end{aligned}$$

If both numerators are 0, it would mean $\alpha\beta^{-1} = 0$, since neither $\alpha = 0$ or $\beta = 0 = \beta^{-1}$ this is impossible. □

(6) 3.4.45

Show that the intersection of two subgroups is also a subgroup.

Proof. Let $H, K \leq G$. We want to show that $H \cap K \leq G$. Let $a, b \in H \cap K$, then we need to show that $ab^{-1} \in H \cap K$. We know that $a, b \in H$, and since H is a subgroup $b^{-1} \in H$ as well. Therefore $ab^{-1} \in H$. Similaryly $a, b^{-1} \in K$, with the same inverse as G and as H, and thus $ab^{-1} \in K$. Therefore $ab^{-1} \in H \cap K$. $\square$

(7) 3.4.46

If $H, K \leq G$, it is not implied that $H \cup K \leq G$.

Proof. Let $H, K \leq G$ where neither $H \subset K$ or $K \subset H$. Then $\exists a \in H \setminus K$ and $\exists b \in K \setminus H$. Suppose by contradiction that $H \cup K$ is a subgroup of G. Then $ab^{-1} \in H \cup K$. This means that either $ab^{-1} \in H$ or $ab^{-1} \in K$. If $ab^{-1} \in H$, since $a \in H$ we must have $a^{-1} \in H$. This would mean $a^{-1}ab^{-1} \in H \implies b \in H$ (contradiction). Otherwise $ab^{-1} \in K$ therefore $ab^{-1}b \in K \implies a \in K$ (contradiction). Hence $H \cup K$ is not a subgroup of G. $\square$

(8) 4.4.1

(a)

Prove or disprove that all generators of $\mathbb{Z}_{60}$ are prime.

Proof. Take the number $49 \in \mathbb{Z}_{60}$. Since $\gcd(49, 60) = 1$, we know that $\langle 49 \rangle = \mathbb{Z}_{60}$. However, 49 is not prime. $\square$

(b)

Prove or disprove that $U(8)$ is cyclic.

Proof. If $U(8) = \{1, 3, 5, 7\}$ then there exists $a \in U(8)$ such that $\langle a \rangle = U(8)$. Let us check each element,

$$\begin{aligned}
\langle 1 \rangle &= \{1\} \\
\langle 3 \rangle &= \{1, 3\} \\
\langle 5 \rangle &= \{1, 5\} \\
\langle 7 \rangle &= \{1, 7\}
\end{aligned}$$

Since none generate $U(8)$, the group is not cyclic. $\square$

(e)

(9) 4.4.2

Find the order of the element in the group.

(a)

$5 \in \mathbb{Z}_{12}$

We know that the least common multiple of 5 and 12 is $60 = 5(12)$. Therefore 5 is order 12.

(b)

$\sqrt{3} \in \mathbb{R}$

Since $\mathbb{R}$ is infinite, there is no natural degree which will result in the identity, so we say that the order is infinite. Order of $\sqrt{3} = \infty$.

(d)

$-i \in \mathbb{C}^*$

We know that

$$\begin{aligned} -i &= -i \\ -i^2 &= -1 \\ -i^3 &= i \\ -i^4 &= 1 \end{aligned}$$

Therefore i is order 4.

(10) 4.4.3

List every...

(a)

Element of $7\mathbb{Z}$.

$$7\mathbb{Z} = \{\cdots, -14, -7, 0, 7, 14, \cdots\}$$

(b)

Element generated by $15 \in \mathbb{Z}_{24}$.

$$\langle 15 \rangle = \{0, 3, 6, 9, 12, 15, 18, 21\}$$

(c)

Subgroups of $\mathbb{Z}_{12}$

$$\begin{aligned} &\{0\} \\ &\{0, 6\} \\ &\{0, 4, 8\} \\ &\{0, 3, 6, 9\} \\ &\{0, 2, 4, 6, 8, 10\} \\ &\mathbb{Z}_{12} \end{aligned}$$

(d)

Subgroups of $\mathbb{Z}_{60}$.

$$\begin{aligned}
&\{0\}\\
&\{0,30\}\\
&\{0,20,40\}\\
&\{0,15,30,45\}\\
&\{0,12,24,\cdots,48\}\\
&\{0,10,20,30,\cdots,50\}\\
&\{0,6,12,18,\cdots,54\}\\
&\{0,5,10,15,\cdots,55\}\\
&\{0,4,8,12,\cdots,56\}\\
&\{0,3,6,9,\cdots,57\}\\
&\{0,2,4,6,\cdots,58\}\\
&\mathbb{Z}_{60}
\end{aligned}$$

(e)

Subgroups of $\mathbb{Z}_{13}$.

$$\begin{gathered}
\{0\}\\
\mathbb{Z}_{13}
\end{gathered}$$

(f)

Subgroups of $\mathbb{Z}_{48}$.

$$\begin{aligned}
&\{0\}\\
&\{0,24\}\\
&\{0,16,32\}\\
&\{0,12,24,36\}\\
&\{0,8,16,\cdots,40\}\\
&\{0,6,12,\cdots,42\}\\
&\{0,4,8,12,\cdots,40,44\}\\
&\{0,3,6,9,\cdots,42,45\}\\
&\{0,2,4,6,\cdots,44,46\}\\
&\mathbb{Z}_{48}
\end{aligned}$$

(g)

The subgroup generated by $3 \in U(20)$.

$$\langle 3\rangle = \{1,3,7,9\}$$