Group Theory Homework 1 Solutions

Karthik Boyareddygari
Professor Alexandru Suciu

Problem 1:

For both parts, the Euclidean algorithm will be used in its matrix form as demonstrated by Dr. Suciu during lecture. In particular, augmented matrices will serve to condense the notation according to

$$\left[\begin{array}{cc|c} c_1 & c_2 & d_1 \\ c_3 & c_4 & d_2 \end{array}\right] \equiv \begin{bmatrix} c_1 & c_2 \\ c_3 & c_4 \end{bmatrix}\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} d_1 \\ d_2 \end{bmatrix}.$$

(a)

$$\left[\begin{array}{cc|c} 1 & 0 & 35 \\ 0 & 1 & 14 \end{array}\right] \xrightarrow{R_1-2R_2} \left[\begin{array}{cc|c} 1 & -2 & 7 \\ 0 & 1 & 14 \end{array}\right] \implies 7 = 35(1) + 14(-2) \implies \boxed{m = 1, n = -2.}$$

(b)

$$\left[\begin{array}{cc|c} 1 & 0 & 15 \\ 0 & 1 & 11 \end{array}\right] \xrightarrow{R_1-R_2} \left[\begin{array}{cc|c} 1 & -1 & 4 \\ 0 & 1 & 11 \end{array}\right] \xrightarrow{R_2-2R_1} \left[\begin{array}{cc|c} 1 & -1 & 4 \\ -2 & 3 & 3 \end{array}\right] \xrightarrow{R_1-R_2} \left[\begin{array}{cc|c} 3 & -4 & 1 \\ -2 & 3 & 2 \end{array}\right] \implies$$

$$1 = 15(3) + 11(-4) \implies \boxed{m = 3, n = -4.}$$

Problem 2:

Distributivity and commutativity of multiplication in the commutative ring $\mathbb{Z}$ will be taken for granted.

(a)

Suppose that $b|a \iff a = bk$ for some $k \in \mathbb{Z} \implies ac = (bk)c = b(kc) \implies b|ac$.

(b)

Suppose that $b|a, c|b \iff a = bk_1$ and $b = ck_2$ for some $k_1, k_2 \in \mathbb{Z} \implies a = (ck_2)k_1 = c(k_2k_1) \implies c|a$.

(c)

Now suppose that $c|a, c|b \implies a = k_1c$ and $b = k_2c$ for some $k_1, k_2 \in \mathbb{Z}$. Then we may compute

$$\begin{aligned} ma + nb &= m(k_1c) + n(k_2c) \\ &= (mk_1)c + (nk_2)c \\ &= (mk_1 + nk_2)c, \end{aligned}$$

which shows that $c|(ma + nb)$ as desired.

Problem 3:

(a)

$(\mathbb{Z}_4,+)$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$(\mathbb{Z}_4,\cdot)$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

(b)

Elements at the top of columns are applied first, as in they are seen on the right when writing the composition.

$(S_3,\circ)$	()	(12)	(23)	(13)	(123)	(132)
()	()	(12)	(23)	(13)	(123)	(132)
(12)	(12)	()	(123)	(132)	(23)	(13)
(23)	(23)	(132)	()	(123)	(13)	(12)
(13)	(13)	(123)	(132)	()	(12)	(23)
(123)	(123)	(13)	(12)	(23)	(132)	()
(132)	(132)	(23)	(13)	(12)	()	(123)

Problem 4:

An element $[m]_n$ has multiplicative inverse if and only if there exists $j,k \in \mathbb{Z}$ such that $mj = nk+1 \implies 1 = m(j) + n(-k)$. In particular, the multiplicative inverse is $[j]_n$.

(a)

It is easy to see that $1 = 15 - 14 \implies \boxed{[14]_{15}^{-1} = [-1]_{15} = [14]_{15}.}$

(b)

$$\left[\begin{array}{cc|c}1 & 0 & 38\\ 0 & 1 & 83\end{array}\right] \xrightarrow{R_2-2R_1} \left[\begin{array}{cc|c}1 & 0 & 38\\ -2 & 1 & 7\end{array}\right] \xrightarrow{R_1-5R_2} \left[\begin{array}{cc|c}11 & -5 & 3\\ -2 & 1 & 7\end{array}\right] \xrightarrow{R_2-2R_1} \left[\begin{array}{cc|c}11 & -5 & 3\\ -24 & 11 & 1\end{array}\right] \implies$$

$$38(-24) = 83(-11) + 1 \implies \boxed{[38]_{83}^{-1} = [-24]_{83} = [59]_{83}.}$$

Problem 5:

(a)

By slightly abusing notation, let us define a map

$$f^{-1} : \left\{ \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & x-3 \end{array} \right. .$$

It is easy to see that $f(f^{-1}(x)) = f^{-1}(f(x)) = x$ so that $f \circ f^{-1} = f^{-1} \circ f = \mathbb{1}_{\mathbb{R}}$. By definition, this is an inverse function for f, so $\underline{f \text{ must be a bijection}}$.

(b)

The condition $f(x) = z$, which holds true for all $z \in \mathbb{C}$ precisely when f is surjective (there exists a suitable x), is equivalent to the condition $f(x) - z = 0$. Because z is a constant, $f(x) - z$ is again a polynomial with complex coefficients.

By the fact that $\mathbb{C}$ is algebraically closed, which is related to the fundamental theorem of algebra, there exist 2 (potentially identical) solutions x which satisfy the condition. Therefore, f is surjective. As for injectivity, note that $f(-2) = f(0) = 1$ even though $-2 \neq 0$, so f is not injective.

(c)

When dealing with functions on a fixed finite set, surjectivity results precisely when injectivity does as well, which can easily be argued by exhausting either codomain or domain elements. As such, it will suffice to show injectivity in order to establish that f is a bijection. Let $x, y \in \mathbb{Z}_5$ be arbitrary elements. Then we have

$$\begin{aligned} f(x) &= f(y) \\ [3x+8]_5 &= [3y+8]_5 \\ [3x]_5 &= [3y]_5 \\ [x]_5 &= [y]_5. \end{aligned}$$

This follows because of how addition and multiplication are defined within $\mathbb{Z}_n$. As a result, f is injective and thereby also bijective. If it is desired to show surjectivity separately, the simplest method is to map the domain through f and to record the resulting range (which will be $\mathbb{Z}_5$).

Problem 6:

The multiplication table shown for the operation $*$ has repeated elements in some rows and some columns. The cancellation property prohibits this behavior, so this magma lacks the cancellation property. Because this property is implied by the group axioms, the lack of it implies that $(\{a, b, c\}, *)$ is not a group.

On the other hand, $(\{a, b, c\}, \star)$ is a cyclic group of order 3, which can be shown by making the associations $a \mapsto 0$, $b \mapsto 1$, and $c \mapsto 2$. By translating the elements, we find that the multiplication table is precisely that for $\mathbb{Z}_3$. Therefore, $(\{a, b, c\}, \star)$ is a group.

Problem 7:

(a)

Similar to problem 6, we associate $(\mathbb{Z}, *)$ to a well known group, namely $(\mathbb{Z}, +)$ by the rule $[n]_* \mapsto [n+1]_+$. In particular, this "weird" multiplication has identity -1, generator 0, and inverse $a^{-1} = (-a-2)$—as opposed to identity 0, generator 1, and inverse $a^{-1} = -a$ in $(\mathbb{Z}, +)$. Therefore, $(\mathbb{Z}, *)$ is an infinite cyclic group, thereby also abelian since cyclic groups are always abelian.

(b)

Let $a, b \in \mathbb{Q}$ be distinct rationals. Note that

$$a \star -1 = a - 1 - a = -1 = b - 1 - b = b \star -1$$

even though $a \neq b$. Therefore, the cancellation property is violated, implying that $(\mathbb{Q}, \star)$ cannot be a group.

(c)

We now consider $\underline{(\mathbb{Q}\setminus\{-1\},\star)\text{, which satisfies the (abelian) group axioms}}$ as demonstrated below.

- Associativity: Let $a, b, c \in \mathbb{Q}$ be arbitrary rationals all not equal to -1. By making heavy use of the associativity of addition, we find that

  $$(a\star b)\star c = (a+b+ab)+c+(a+b+ab)c = a+b+ab+c+ac+bc+abc = a+(b+c+bc)+a(b+c+bc) = a\star(b\star c).$$

- Identity: Let $a \in \mathbb{Q}$ be an arbitrary rational ($a \neq -1$). Then

  $$a \star 0 = a + (0) + a(0) = a,$$

  so $\underline{0 \text{ is the identity}}$ since the choice of a is arbitrary.

- Inverses: Again let $a \in \mathbb{Q}$ be an arbitrary rational ($a \neq -1$). With help from the distributive property, we find that

  $$a \star \frac{-a}{a+1} = a + \frac{-a}{a+1} + \frac{-a^2}{a+1} = a + \frac{-a(a+1)}{a+1} = a + (-a) = 0 \Longrightarrow \boxed{a^{-1} = \frac{-a}{a+1}.}$$

- Abelian: Let $a, b \in \mathbb{Q}$ be arbitrary ($a, b \neq -1$). Utilizing the commutativity of both addition and multiplication, we compute

  $$a \star b = a + b + ab = b + a + ba = b \star a,$$

  which shows that $\underline{(\mathbb{Q},\star)\text{ is abelian}}$.

Problem 8:

Let $a, b \in G$ be arbitrary elements. Because all elements of G have order 2, $a = a^{-1}$ for all $a \in G$. With this, computing the product $(ab)^2$ gives the desired result:

$$(ab)^2 = abab = e \Longrightarrow ab = b^{-1}a^{-1} = ba.$$

The $\underline{\text{converse is not true}}$. For example, $\mathbb{Z}$ is commutative but $1 + 1 = 2 \neq 1$.