Homework 4

Tejas Patel

17 October, 2025

1

1.1 a

$\mathbb{Z}, +$ is an abelian group. It is closed on integers over addition. The neutral element is 0, and the additive inverse is always part of $\mathbb{Z}$. For $x \in \mathbb{Z}$, the additive inverse is $-x$. For $x, y \in \mathbb{Z}$, $x + y = y + x$, making it commutative

1.2 b

$2\mathbb{Z}$ is the set of all evens.
Prove it is closed on addition: $\exists k, l \in \mathbb{Z}\ 2k + 2l = 2(k + l)$. Since $k, l \in \mathbb{Z}$ and $\mathbb{Z}$ is closed on addition, $2\mathbb{Z}$ is also closed on addition
The Neutral Elements and Additive Inverses remain the same from part (a) at 0, and $-x$. $x, y \in \mathbb{Z}$, $2x + 2y = 2y + 2x$, making it commutative and by definition, an Abelian group

1.3 c

$(\mathbb{Q}^{\times}, \cdot)$ is an abelian group under multiplication. It is closed over multiplication, where for $p \in \mathbb{Q} : p = \dfrac{m}{n}$ the inverse of a general element is $\dfrac{n}{m}$ and the identity element is 1. It is also commutative as $\dfrac{p}{q} * \dfrac{r}{s} = \dfrac{pr}{qs} = \dfrac{r}{s} * \dfrac{p}{q}$

2

2.1 a

$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$
$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e$
Since both expressions are equivalent to the neutral element, $(b^{-1}a^{-1})$ is equivalent to $(ab)^{-1}$

2.2 b

By definition $aa^{-1} = e = a^{-1}a$ since a^{-1} is the inverse on both sides of the equation when multiplied to a, that means $a = a^{-1}$ and $(a^{-1})^{-1} = a$

3

$6x + 15y = 3(2x + 5y) : x, y \in \mathbb{Z}$ meaning $\bigcup \forall x \forall y : 2x + 5y = \mathbb{Z}$ hence $3(2x + 5y) = 3\mathbb{Z}$

4

4.1 a

$(\mathbb{Z}, +)$ is an abelian group, it is associative and commutative over addition, 0 is the neutral element, and every $a \in \mathbb{Z}$ has an additive inverse $-a$.
Multiplication is associative and commutative and has identity 1.
Distributive laws hold: $a(b+c) = ab+ac$ and $(a+b)c = ac+bc$ for all $a, b, c \in \mathbb{Z}$. Hence $\mathbb{Z}$ is a commutative ring with identity 1.

4.2 b

$u \in \mathbb{Z}$ is a unit if $\exists v \in \mathbb{Z}$ with $uv = 1$. If $uv = 1$, then $u \mid 1$, so $|u| \leq 1$, hence $u = \pm 1$. Conversely, $1 \cdot 1 = 1$ and $(-1) \cdot (-1) = 1$. Thus the group of units is $U(\mathbb{Z}) = \{\pm 1\}$.

4.3 c

Suppose $ab = 0 \;\; a, b \in \mathbb{Z}$. If $a \neq 0$ and $b \neq 0$, then $|a| \geq 1$ and $|b| \geq 1$, so $|ab| = |a||b| \geq 1$ a contradiction to $ab = 0$. Hence $a = 0$ or $b = 0$. Therefore $\mathbb{Z}$ has no nonzero zero divisors.
Combining (a) and (c), $\mathbb{Z}$ is a commutative ring with 1 and without zero divisors, so $\mathbb{Z}$ is an integral domain.

5

5.1 a

$\bar{7} + \bar{9} = 16 \bmod 12 \;\; = 4$ and $\bar{11} + \bar{4} = 15 \bmod 12 \;\; = 3$

5.2 b

The identity element is 0 over addition, and the inverse element is $\bar{12 - k}$

5.3 c

If $a \equiv a'$ and $b \equiv b'$ both mod 12, then $ab - a'b' = a(b - b') + a'(b - b')$ is divisible by 12
Multiplicative identity is $\bar{1} \Rightarrow \bar{1} * \bar{k} = \bar{k}$

6

6.1 a

$p(x) + q(x) = 2x^3 + x^2 - 2x + 6$ and $p(x)q(x) = 2x^5 + 2x^4 - x^3 + 2x^2 + 2x + 5$

6.2 b

Define $\mathrm{ev}_2 : \mathbb{Z}[x] \to \mathbb{Z}$ by $\mathrm{ev}_2(f) = f(2)$. Then $\mathrm{ev}_2(p) = 15$ and $\mathrm{ev}_2(q) = 7$. $\forall f, g \in \mathbb{Z}[x]$, $\mathrm{ev}_2(f+g) = (f+g)(2) = f(2) + g(2) = \mathrm{ev}_2(f) + \mathrm{ev}_2(g), \quad \mathrm{ev}_2(fg) = (fg)(2) = f(2)g(2) = \mathrm{ev}_2(f)\,\mathrm{ev}_2(g)$.
Hence ev_2 is a ring homomorphism.

7

7.1 a

$\mathbb{Z}$ is not a field because it is not commutative across multiplication.

7.2 b

$\mathbb{Q}$ is a field. It has commutativity on addition, a inverted is $-a$ and on multiplication $a^{-1} = \dfrac{1}{a}$ where $a \in \mathbb{Q}$. It also follows the distributive property on both addition and multiplication

7.3 c

$\mathbb{R}$ is a field. It has commutativity on addition, $a^{-1} = -a$ and on multiplication $a^{-1} = \dfrac{1}{a}$ where $a \in \mathbb{R}$. It also follows the distributive property on both addition and multiplication

7.4 d

$(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ is a field, since for any $\overline{k} \neq \overline{0}$ we have $\gcd(k,p) = 1$ and hence $\exists a, b \in \mathbb{Z}$ with $ak + bp = 1$, so $ak \equiv 1 \pmod{p}$ and $\overline{a}$ is the inverse of $\overline{k}$.

7.5 e

Not a field
Assuming F is a field, take $a \equiv b \pmod{10}$
If $a = 5, b = 2$, $\bar{a} \cdot \bar{b} = \bar{0}$
$1 \cdot b = (a^{-1} \cdot a)b = a^{-1}(a \cdot b) = a^{-1} \cdot 0 = 0$
Making $b = 0$, a contradiction

8

8.1 a

No. The roots of $f(x) = 2 - x^2$ are $\pm\sqrt{2}$, which are both known to be irrational numbers.

8.2 b

Yes. The roots of $f(x) = 2 - x^2$ being $\pm\sqrt{2}$ are irrational but are part of the domain of real numbers.

9

For $a \in \mathbb{R}$ define $T_a : \mathbb{R} \to \mathbb{R}$ by $T_a(x) = x + a$. Let $\mathscr{T} = \{T_a : a \in \mathbb{R}\}$ with composition.
$(T_a \circ T_b)(x) = T_a(x + b) = x + b + a = x + (a + b) = T_{a+b}(x)$, so $T_a \circ T_b = T_{a+b}$.
The identity is T_0 since $T_0(x) = x$.
The inverse of T_a is T_{-a} because $T_a \circ T_{-a} = T_{a+(-a)} = T_0 = \mathrm{id}$ and $T_{-a} \circ T_a = T_{-a+a} = T_0$.
Therefore $(\mathscr{T}, \circ)$ is an abelian group and isomorphic to $(\mathbb{R}, +)$ via $a \mapsto T_a$.

10

$\circ$	0°	90°	180°	270°
0°	0°	90°	180°	270°
90°	90°	180°	270°	0°
180°	180°	270°	0°	90°
270°	270°	0°	90°	180°

10.1 b

It is closed on rotation, as the table shows. The identity element is 0° and is associative
Inverses are $0^\circ \Leftrightarrow 0^\circ, 90^\circ \Leftrightarrow 270^\circ, 180^\circ \Leftrightarrow 180^\circ, 270^\circ \Leftrightarrow 90^\circ$
It is commutative based on the Cayley Table

11

11.1 b

For any base b we have $c(c(b)) = b$. If $w = b_1 b_2 \cdots b_n$ is a string then
$c \circ c\,(w) = c\big(c(b_1) \cdots c(b_n)\big) = b_1 \cdots b_n = w$
So $c \circ c = \mathrm{id}$. Hence G is a group with identity id, inverse of c equal to c, and it has two elements so it is abelian. Thus $G \cong C_2$.

11.2 b

Since $c = c^{-1}$, the inverse does the same operation as c: it complements each base, for example $c^{-1}(\mathrm{ATCG}) = \mathrm{TAGC}$.