---

Answer ten of the following twelve problems. If more than ten are answered, only the best ten count.

---

Warning: Some questions are copies of previous test questions, but others are modifications of previous test questions or new questions. Be sure to read every question carefully.

---

1. Define ring.

**Solution**:

A set $R$ with two binary operations + and $\cdot$ is a ring if the following are satisfied:

- $R$ is an abelian group with respect to +
- $\cdot$ is associative
- left distributive law: $c \cdot (a + b) = c \cdot a + c \cdot b$ for all $a, b, c$ in $R$
- right distributive law: $(a + b) \cdot c = a \cdot c + b \cdot c$ for all $a, b, c$ in $R$

Note that both distributive laws are required since $\cdot$ is not required to be commutative.

---

2. Define group.

**Solution**:

A set $G$ with an operation * satisfying:

a. * is associative
b. identity: $\exists\ e$ such that $\forall\ x \in G\ (\ e * x = x * e = x\ )$
c. inverses: $\forall\ x \in G\ \exists\ y \in G$ such that $y * x = x * y = e$

---

3. Given an equivalence relation $\sim$, prove that $a \sim b$ if and only if $[a] = [b]$

**Solution**:

($\Rightarrow$)

Assume $a \sim b$ and show $[a] = [b]$.

To show $[a] = [b]$, show $[a] \subseteq [b]$ and $[b] \subseteq [a]$.

Let $c \in [a]$. Then, $c \sim a$. Since $a \sim b$ and $\sim$ is transitive, this gives $c \sim b$ which implies that $c \in [b]$. Thus, $[a] \subseteq [b]$.

Similarly, let $c \in [b]$. Then, $c \sim b$. Since $a \sim b$ and $\sim$ is symmetric, $b \sim a$. Since $b \sim a$ and $\sim$ is transitive, this gives $c \sim a$ which implies that $c \in [a]$. Thus, $[b] \subseteq [a]$.

($\Leftarrow$)

Assume $[a] = [b]$ and show $a \sim b$.

Since $a \in [a]$ and $[a] = [b]$, $a \in [b]$ which implies that $a \sim b$.

---

4. A ring $R$ is called a Boolean ring if $a^2 = a$ for every element $a$ of $R$.
If $R$ is a Boolean ring and $a, b \in R$, prove that $(a + b)^2 = a^2 + b^2$ and that $(a + b)^3 = a^3 + b^3$ and that, in fact, for all integers $n > 0$, $(a + b)^n = a^n + b^n$.

**Solution**:

$$(a + b)^2 = a + b = a^2 + b^2$$

$$(a + b)^3 = (a + b)^2 (a + b) = (a + b) (a + b) = (a + b)^2 = a^2 + b^2$$
$$= aa + bb = a(a^2) + b(b^2) = a^3 + b^3$$

Now, finish by induction.

Assume that $(a + b)^n = a^n + b^n$ and $(a + b)^{n+1} = a^{n+1} + b^{n+1}$.

Show that $(a + b)^{n+2} = a^{n+2} + b^{n+2}$.

$$\begin{aligned}(a + b)^{n+2} &= (a + b)^n (a + b)^2 \\ &= (a + b)^n (a + b) \\ &= (a + b)^{n+1} \\ &= a^{n+1} + b^{n+1} \\ &= (a^n)a + (b^n)b \\ &= (a^n)a^2 + (b^n)b^2 \\ &= a^{n+2} + b^{n+2}.\end{aligned}$$

---

5. Use the Euclidean algorithm to write the greatest common divisor of 382 and 26 as a linear combination of 382 and 26.

**Solution**:

$382 = 14 \cdot 26 + 18$
$26 = 1 \cdot 18 + 8$
$18 = 2 \cdot 8 + 2$
$8 = 4 \cdot 2 + 0$

So, 2 is the gcd.

Working backwards gives:

$$\begin{aligned} 2 &= 18 - 2 \cdot 8 \\ &= 18 - 2 \cdot (26 - 18) \\ &= 3 \cdot 18 - 2 \cdot 26 \\ &= 3 \cdot (382 - 14 \cdot 26) - 2 \cdot 26 \\ &= 3 \cdot 382 - 44 \cdot 26 \end{aligned}$$

---

6. If $\theta : R \to S$ is a homomorphism of the ring $R$ into the ring $S$ and $a \in R$, prove that

$\theta (a^n) = \theta (a)^n$ for every positive integer $n$.

**Solution**:

Proof by induction:

Basis case:

For $n = 1$, this is obvious.

Induction case:

Assume $\theta (a^n) = \theta (a)^n$

Show $\theta (a^{n+1}) = \theta (a)^{n+1}$

$$\begin{aligned} \theta (a^{n+1}) &= \theta (a^n a) \\ &= \theta (a^n)\, \theta (a) \\ &= \theta (a)^n\, \theta (a) \\ &= \theta (a)^{n+1} \end{aligned}$$

---

7. Prove that $\mathbf{Z}_n$ is an integral domain if and only if $n$ is prime.

**Solution**:

($\Rightarrow$)

Indirect proof

Assume $n$ is not prime.

Show that $\mathbf{Z}_n$ is not an integral domain

If $n$ is not prime, then there are $a$ and $b$ with $1 < a, b < n$ and $ab = n$

Then, in $\mathbf{Z}_n$, $ab = 0$ with neither $a$ nor $b = 0$, so $\mathbf{Z}_n$ is not an integral domain

($\Leftarrow$)

Indirect proof

Assume $\mathbf{Z}_n$ is not an integral domain

Show that $n$ is not prime.

There are $a$ and $b$ in $\mathbf{Z}_n$ with $ab = 0$ and neither $a$ nor $b = 0$.

This means that $n \mid ab$ but $n$ does not divide $a$ and $n$ does not divide $b$.

This is impossible if $n$ is prime.

---

8. Factor the following polynomials into irreducible factors over the field $\mathbf{Z}_7$. Write the elements of $\mathbf{Z}_7$ as 0, 1, 2, 3, 4, 5, 6. [ Hints: They both factor over $\mathbf{Z}_7$ into different factors than over the real numbers. Recall that a polynomial of degree two or three factors if and only if it has a root.]

$f(x) = x^2 + 3$

$g(x) = x^3 + 2x^2 + 5x + 3$

**Solution**:

Factor $f(x)$

$f(x) = x^2 + 3 = 0$ for $x = 2$ or 5.

Thus, $x - 2$ and $x - 5$ are factors.

$f(x) = (x + 5)(x + 2)$

Factor $g(x)$

$g(x) = x^3 + 2x^2 + 5x + 3$

| $x$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| $g(x)$ | 3 | 4 | 1 | 0 | 0 | 0 | 6 |

$g(x) = (x + 4)(x + 3)(x + 2)$

---

9. Prove: If $K$ is a nonempty subset of a group $G$ so that for all $a, b \in K$, $ab^{-1} \in K$, then $K$ is a subgroup of $G$.

**Solution**:

Since $K$ is nonempty, we can pick an $k \in K$ and use it for both $a$ and $b$ in the given statement.

This gives $k\,k^{-1} \in K$. So, $e \in K$.

For any $k \in K$, $e\,k^{-1} \in K$. Thus $K$ contains inverses of all of its elements.

For all $a, b \in K$, $b^{-1} \in K$, so $a(b^{-1})^{-1} \in K$.

Thus, $K$ is closed under the group operation.

Since $K$ is a nonempty subset closed under the group operation and contains inverses of all of its elements, it is a subgroup of $G$.

---

10. Prove that if a commutative ring $R$ has a nonzero divisor of zero then $R$ cannot be an ordered ring.

**Solution**:

Let $a$ and $b$ be nonzero elements of $R$ with $ab = 0$.

Then, $a(-b) = 0$ and $(-a)b = 0$ and $(-a)(-b) = 0$.

Thus, any assignment of positive and negative to $a$ and $b$ makes the product of two positive elements zero which is not allowed in an ordered ring.

---

11. An element $a$ of a ring $R$ is said to be idempotent if $a^2 = a$. If $m$ and $n$ are relatively prime integers greater than 1, prove that the ring $\mathbf{Z}_{mn}$ has at least two idempotent elements other than 0 and 1. [ Hint: If $1 = mx + ny$, consider $mx$ and $ny$ as elements of $\mathbf{Z}_{mn}$ . ]

**Solution**:

If $m$ and $n$ are relatively prime integers greater than 1, then there are integers $x$ and $y$ with $1 = mx + ny$.

In $\mathbf{Z}_{mn}$, $(mx)^2 = mx(1 - ny) = mx - mnxy = mx$

In $\mathbf{Z}_{mn}$, $(ny)^2 = ny(1 - mx) = ny - mnxy = ny$

It is left to show that neither of these is 0 or 1 in $\mathbf{Z}_{mn}$.

If $mx = 0$, then $mn \mid mx$. This gives $n \mid x$ which would mean that $n$ is a factor of $mx + ny = 1$ which is

impossible. Similary, $ny$ cannot be 0.

If $mx = 1$, then $mn \mid mx - 1$. This gives $mn \mid ny$ and so $ny = 0$. This was shown above to be impossible.

---

12. Given a homomorphism $\theta$ from a group $G$ to a group $H$, we define $K$, the kernel of $\theta$, to be the set of all elements of $G$ that map to the identity in $H$.

That is, $K = \{ a \in G : \theta(a) = e_H \}$

Show (a) that $K$ is a subgroup of $G$ and (b) that $K$ also satisfies the property:

$\forall k \in K \; \forall a \in G \; (a^{-1} k a \in K)$

That is, for all $k$ in $K$ and all $a$ in $G$, the product $a^{-1} k a$ is in $K$.

**Solution**:

(a)

$K$ is nonempty since the identity in $G$ maps to the identity in $H$.

$K$ is closed under the group operation in $G$ since if $a$ and $b$ are in $K$,

$$\theta(ab) = \theta(a)\,\theta(b) = e_H e_H = e_H$$

$K$ contains inverses of all of its elements since if $a$ is in $K$,

$$\theta(a^{-1}) = \theta(a)^{-1} = (e_H)^{-1} = e_H$$

Since $K$ is a nonempty subset closed under the group operation and contains inverses of all of its elements, it is a subgroup of $G$.

(b)

Let $k \in K$ and $a \in G$.

$\theta(a^{-1} k a) = \theta(a^{-1})\,\theta(k)\,\theta(a) = \theta(a)^{-1} \quad e_H \quad \theta(a) = \theta(a)^{-1}\,\theta(a) = e_H$

Thus, $a^{-1} k a$ is in $K$.

---