Exam Corrections.

1. Redo question(s) that you missed (on a separate piece of paper)
2. Explain mode.
3. Make another example question like it — solve it, showing you understand.

If all this is correct, I will give ½ of the points back.

Rings — a set R with two operations $(+, \cdot)$ s.t.
- R is an abelian group under $+$.
- multiplication is associative.
- The set R is closed under multiplication
- $\forall a, b, c \in R$, $a \cdot (b+c) = a \cdot b + a \cdot c$ and $(b+c) \cdot a = b \cdot a + c \cdot a$.

"Commutative ring" means multiplication is commutative.

Example: $M_2(2\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in 2\mathbb{Z} \right\}$.

↑ Note: Not commutative, since

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 4 \\ 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 4 \\ 0 & 0 \end{pmatrix}.$$

↑ ↑

Note $M_2(2\mathbb{Z})$ has zero divisors, ie. elements A, B s.t. $AB = 0$.

Note also, $M_2(2\mathbb{Z})$ does not have a multiplicative identity (called unity or 1).
ie. $M_2(2\mathbb{Z})$ is not a "ring with unity" = "ring with 1".

If mult. is commutative for a ring R, we say R is a commutative ring.

If R contains an element 1, i.e. s.t. $1 \cdot u = u \ \forall u \in R$, then we say R is a ring with unity.

Often, we will restrict our attention to commutative rings with unity.

Examples Commutative Rings with unity:

$\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}, \mathbb{Z}_n, \mathbb{Z}_n \times \mathbb{Z}_k$ (operations component-wise; unity: $(1,1)$)

$C(\mathbb{R}) = \{$Continuous $\mathbb{R}$-valued functions on $\mathbb{R}\}$

$\mathcal{F}(\mathbb{R}) = \{$functions $f: \mathbb{R} \to \mathbb{R}\}$ ↑ pointwise addition & mult.

unity: $u(x) = 1 \ \forall x$.

$R[x] = \{$polynomials with coefficients in a ring $R\}$

1 ↗ this is in place as long as $1 \in R$ is a unity.

Commutating rings without unity

$R = m\mathbb{Z}$ $m \in \mathbb{Z}$, $|m| \neq 1$.

$\{0\}$

$(m\mathbb{Z})[x]$ $\{$functions $: \mathbb{R} \to m\mathbb{Z}.\}$.

A subring $S \subseteq$ a ring R is a ring inside of R that uses the same operations as R

If R is a ring with unity, then $a \in R$ is called a unit

if a^{-1} exists, ie $\exists b \in R$ s.t. $a \cdot b = 1$.

Note 1 is always a unit.

Given R, a ring with unity, let $R^\times = \{$ units $u \in R\}$.
Then $R^\times$ is a group under multiplication.

subring $2\mathbb{Z} \subseteq \mathbb{Z}$.

$\mathbb{Z}[x] \subseteq \mathbb{R}[x]$.

Consider $R = \mathbb{Z}_{10}$.

Then $R^\times = \{1, 3, 7, 9\}$ $\quad |\mathbb{Z}_n^\times| = \phi(n)$

$3^{-1} = 7 \quad 9^{-1} = 9$ $\quad \phi(n)$

in general $(\mathbb{Z}_n)^\times = \{$ integers $[u] \in \mathbb{Z}_n$ s.t. $(u, n) = 1\}$.

Pf. If GCD $(u, n) = 1$, $\exists\ ru + sn = 1$ for $r, s \in \mathbb{Z}$.

$\Rightarrow ru \equiv 1 \bmod n$.

If GCD $(u, n) \neq 1$

$p = $ GCD (u, n) $\quad p \neq 0, 1$

$u = kp$

$n = lp$ $\quad (k, l) = 1$

If $ru = 1$, then

$rkp \equiv 1 \bmod n$

$\Rightarrow rkp - an = 1$ for some $a \in \mathbb{Z}$.

$\Rightarrow (p, n) = 1$, a contradiction. ☐

If R is a commutative ring with 1,

$R^\times$ is an abelian group.

Note: $\{1, 3, 7, 9\} = (\mathbb{Z}_{10})^\times = \{1, 3, 3^3, 3^2\} \cong \mathbb{Z}_4$. both 3 & 7 are generators.

Consequences of defns of Ring:

✡ $0 \cdot a = 0 \quad \forall a \in R$

Proof: $(0+0)\cdot a = 0 \cdot a$

$\|$

$0\cdot a + 0\cdot a = 0\cdot a$

$0\cdot a + (0\cdot a) + -(0\cdot a) = 0\cdot a + -(0\cdot a)$

$0\cdot a + 0 = 0$

$0\cdot a = 0$. ☑

✡ $-(a\cdot b) = (-a)\cdot b = a\cdot(-b)$

⋮

The characteristic of a ring: the least positive integer p, if it exists, such that

$p \cdot a = 0 \quad \forall a \in R$. (Note: always a prime number).

If no such p exists, we say R has characteristic 0. if R is an integral domain.)

A commutative ring with 1 with no zero divisors is called an integral domain.

$\mathbb{Z}_{10}$ is a comm. ring with 1.

characteristic: 10.

integral domain? No. Proof: $2 \cdot 5 = 0$.

$\mathbb{Z}_p$ for p prime: $pa = 0 \ \forall a \in \mathbb{Z}_p$.

p is the characteristic.

A comm. ring with 1 with all nonzero elements units is a field.