I. RING THEORY
First review before Midterm 1

1. Definition, and Examples

Definition 1.1. A non-empty set \( R \) is called a ring if there are two binary operations "\(+\)" and "\(\cdot\)" defined in \( R \) such that:

(i) \((R, +)\) is an abelian group,
(ii) \((R, \cdot)\) is a semigroup,
and the following distributive laws must be satisfied:
(iii) \((a + b)c = ac + bc\) and \(c(a + b) = ca + cb\) for \(\forall a, b, c \in R\).

In addition, if there is an element \( e \in R \) such that \( ea = ae = a \) for \(\forall a \in R\), then \( R \) is called a ring with identity. In this case, \( e \) is the identity of \( R \). We always denote the identity of a ring (if it exists) by the number 1.

Definition 1.2. Let \( R \) be a ring. If \( ab = ba \) for all \( a, b \in R \), then \( R \) is called a commutative rings.

Remarks 1.3. (1) There are rings in which there exist nonzero elements \( a, b \) with \( ab = 0 \). To see this consider the \( 2 \times 2 \) matrix ring \( M_2(\mathbb{R}) \) over the real number field \( \mathbb{R} \); or the ring \( \mathbb{Z}_m \) where \( m \) is not a prime number (for example \( m = 4, 6, 8, 9, \ldots \)).

(2) For \( n > 1 \), the ring \( M_n(\mathbb{R}) \) is never commutative.

Remark 1.4. If a ring \( R \) has an identity 1, then the \( n \times n \) matrix ring \( M_n(R) \) over \( R \) has also an identity, and this is the matrix \((a_{ij})\) where \( a_{ii} = 1 \) (1 \( \leq i \leq n \)) and \( a_{ij} = 0 \) for all \( i \neq j \).

Remark 1.5. For any element \( a \) of a ring \( R \), and any positive integers \( m, n \),
\( a^m = a \cdot a \cdots a \) (\( m \) times), \( a^m \cdot a^n = a^{m+n} \), \( (a^m)^n = a^{mn} \). In general, the negative power of an element in a ring does not exist, unless that element has a multiplicative inverse.

Definition 1.6. (i) Let \( R \) be a ring, and \( a \in R \). Then \( a \) is called a nilpotent element of \( R \) if there is a positive integer \( m \) such that \( a^m = 0 \).
(ii) A ring \( R \) is called a nil ring if every element of \( R \) is nilpotent.
(iii) A ring \( R \) is called a nilpotent ring if \( R^k = 0 \) for some positive integer \( k \).

Remark 1.7. (a) A ring with identity is never nil or nilpotent, because the identity is not nilpotent.
(b) There are nil rings that are not nilpotent.

**Definition 1.8.** An element $f$ of a ring $R$ is called an idempotent element (or an idempotent) if $f^2 = f$.

2. Subrings

**Definition 2.1.** Let $A$ be a non-empty subset of a ring $R$. Then $A$ is called a subring of $R$ if the following two conditions are satisfied:

1. For all $a, b \in A$, $a - b \in A$;
2. For all $a, b \in A$, $ab \in A$.

**Example 2.2.** Let $R$ be a commutative ring, and $N$ be the set of all nilpotent elements of $R$. Then $N$ is a subring of $R$.

**Remarks 2.3.** (1) The statement in Example 2.2 is no more correct if $R$ is not commutative. For example, let $R = M_2(\mathbb{R})$, the $2 \times 2$ matrix ring over $\mathbb{R}$. We know that for example, for $\alpha = \begin{bmatrix} 0 & 2 \\ 0 & 0 \end{bmatrix}$ and $\beta = \begin{bmatrix} 0 & 0 \\ -4 & 0 \end{bmatrix}$, then $\alpha$ and $\beta$ are in $N$ (= the set of all nilpotent elements of $R$). But $\alpha - \beta = \begin{bmatrix} 0 & 2 \\ 4 & 0 \end{bmatrix}$ is not nilpotent (prove it?), and hence not in $N$.

(2) In general, for a ring $R$ with $R^2 \neq 0$ and for $n > 1$, any $n \times n$ matrix ring over $R$ is never commutative.

**Example 2.4.** Any subgroup of $(\mathbb{Z}, +)$ is a subring of the ring $\mathbb{Z}$. Moreover, for any positive integer $m$, any additive subgroup of $\mathbb{Z}_m$ is a subring of the ring $\mathbb{Z}_m$.

**Remark 2.5.** In contrast to Example 2.4, there are rings $R$ in which not any additive group of $(R, +)$ is a subring of the ring $R$. To see that, we take the ring $R = M_2(\mathbb{R})$ and let $A = \{ \begin{bmatrix} 0 & a \\ b & 0 \end{bmatrix} | a, b \in \mathbb{R} \}$. Then $(A, +)$ is a subgroup of $(R, +)$ (prove this!), but $A$ is not a subring of $R$, because, for example, if we take an element $\alpha = \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix} \in A$, then $\alpha^2 \not\in A$. (Check this!)

**Definitions 2.6.** (1) Let $R$ be a ring. If there is a positive integer $m$ such that $mR = 0$, then the smallest number among such positive integers is defined to be the characteristic of the ring $R$.

(2) If for all positive integers $m$, $mR$ is non-zero, then we say that the characteristic of $R$ is ZERO.

**Example 2.7.** The characteristic of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ is 0. But for any $n > 1$, the characteristic of $\mathbb{Z}_n$ is $n$, because $n$ is the smallest positive integer for which $n\mathbb{Z}_n = \overline{0}$.
3. Ideals

Definition 3.1. Let $A$ be a non-empty subset of a ring $R$. Then $A$ is called an ideal of $R$ if the following two conditions are satisfied:

1. For all $a, b \in A$, $a - b \in A$;
2. For all $a \in A$, and all $r \in R$, $ra \in A$ and $ar \in A$.

Examples 3.2. (1) The set $N$ of all nilpotent elements in a commutative ring $R$ is an ideal of $R$ (prove it!).

(2) Any subgroup of $(\mathbb{Z}, +)$ is an ideal of the ring $\mathbb{Z}$. Moreover, for any positive integer $m$, any additive subgroup of $\mathbb{Z}_m$ is an ideal of the ring $\mathbb{Z}_m$.

(3) Let $R = M_2(\mathbb{R})$ and let $A = \left\{ \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix} | a \in \mathbb{R} \right\}$. Then $A$ is a subring of $R$ (check it), but $A$ is not an ideal of $R$. To see this take $\alpha = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \in A$ and $\beta = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \in R$, then $\alpha \beta = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \notin A$.

Definitions 3.3. (1) Let $R$ be a ring with identity 1. Then an element $u \in R$ is called a unit of $R$, if there exists an element $v \in R$ such that $uv = vu = 1$.

(2) A ring $R$ with identity 1 is called a DIVISION RING if every nonzero element of $R$ is a unit of $R$. A commutative division ring is said to be a FIELD.

(3) A field $P$ is called a prime field, if $P$ has exactly two subfield: $(0)$ and $P$ itself.

Remarks 3.4. (1) Any matrix $\alpha \in M_n(\mathbb{R})$ with $\det(\alpha) \neq 0$ is a unit of $M_n(\mathbb{R})$.

(2) Let $R$ be a ring with identity 1, and let $A$ be an ideal of $R$. Then $A = R$ if and only if $A$ contains a unit of $R$ (prove it!).

(3) Any division ring has exactly two distinct ideals, namely $(0)$ and $R$ itself.

(4) But a ring with exactly two distinct ideals is not necessarily a division ring. To see that take $R = M_2(\mathbb{R})$. This matrix ring has exactly two distinct ideals but is not a division ring (prove it!).

(5) Let $R$ be a commutative ring with $R^2 \neq 0$. Then $R$ is a field $\iff$ $R$ has exactly two distinct ideals.

(6) Let $R$ be a commutative ring. Then $R$ is either a field, or a ring with $p$ elements ($p$ a prime number) and $R^2 = 0 \iff R$ has exactly two distinct ideals.

(7) Let $R$ be a division ring. Then for each positive integer $m$, either $mR = R$, or $mR = 0$ (prove it!). This implies that the characteristic of a division ring is either zero or a prime number.
(7a) If the characteristic of the division ring $R$ is 0, then $R$ contains a prime field $K$ that is isomorphic to the field $\mathbb{Q}$.

(7b) If the characteristic of the division ring $R$ is a prime number $p$, then $R$ contains a prime field $K$ with $K \cong \mathbb{Z}_p$.

From this we get the following theorem.

**Theorem 3.5.** Every division ring $R$ contains a prime field $K$ such that either $K \cong \mathbb{Q}$ or $K \cong \mathbb{Z}_p$.

### 4. Homomorphisms of Rings

**Definitions 4.1.** (1) Let $\varphi : R \to S$ be a map from a ring $R$ into a ring $S$. Then $\varphi$ is called a (ring) homomorphism if the following two conditions are satisfied:

(a) $\varphi(a + b) = \varphi(a) + \varphi(b)$, $\forall a, b \in R$;

(b) $\varphi(ab) = \varphi(a)\varphi(b)$, $\forall a, b \in R$.

(2) The subset $\{x \in R | \varphi(x) = 0\}$ is called the kernel of $\varphi$, and is denoted by $\text{Ker}(\varphi)$.

(3) We set $\text{Im}(\varphi) = \varphi(R)$, the image of $R$ by $\varphi$.

(4) The homomorphism $\varphi$ is called an epimorphism (or an onto homomorphism) if $\varphi(R) = S$.

(5) $\varphi$ is a monomorphism if $\varphi$ is 1-1.

(6) $\varphi$ is called an isomorphism if $\varphi$ is 1-1 and onto. In this case, we say that $R$ is isomorphic to $S$, and denote this situation by $R \cong S$.

**Property 4.2.** Let $\varphi : R \to S$ be a homomorphism then:

(1) $\text{Ker}(\varphi)$ is an ideal of $R$, and $\text{Im}(\varphi)$ is a subring of $S$. Moreover $\text{Im}(\varphi)$ is called the homomorphic image of $R$ under $\varphi$.

(2) It holds $\text{Im}(\varphi) \cong R/\text{Ker}(\varphi)$.

(3) From (2) we see that there is an 1-1 correspondence between the set of ideals of a ring $R$ and the homomorphic images of $R$. Precisely: Let $A \subseteq R$ be an ideal, then the map $f : x \mapsto x + A$ for all $x \in R$ is a homomorphism of $R$ onto $R/A$ (prove it!). Conversely, if $g$ is a homomorphism of the ring $R$, then $g$ determines an ideal of $R$, namely $\text{Ker}(g)$, and $g(R) \cong R/\text{Ker}(g)$.

(4) If $A$ is an ideal and $B$ is a subring of $R$. Then the image of $B$ in $R/A$ is $(B + A)/A$. As rings we have $(B + A)/A \cong B/(B \cap A)$.

(5) If $A$, $B$ are ideals of $R$ with $A \subseteq B$, then $(R/A)/(B/A) \cong R/B$. 


Example 4.3. (1) Every division ring has only two distinct homomorphic images.

(2) Every homomorphic image of $\mathbb{Z}$ has the form $\mathbb{Z}_m$ where $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ ($m = 0, 1, \ldots$).

(3) Let $f : \mathbb{Z} \to \mathbb{Z}$ be a homomorphism, then either $f(x) = 0$ for all $x \in \mathbb{Z}$, or $f(x) = x$ for all $x \in \mathbb{Z}$ (prove it!). This means there are exactly two distinct homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}$.

(4) For $\mathbb{Z}_m$, the number of distinct divisors of $m = \text{the number of distinct ideals of } \mathbb{Z}_m = \text{the number of distinct homomorphic images of } \mathbb{Z}_m$. (Prove it!)

5. Direct sums

Let $X$ and $Y$ be subsets of a ring $R$. Then the sum $X + Y$ and the product $XY$ are defined as follows:

$$X + Y = \{x + y \mid \forall x \in X, \forall y \in Y\}; \quad XY = \{\sum_{finite} x_iy_i \mid x_i \in X, \; y_i \in Y\}.$$

Definitions 5.1. Let $R$ be a ring containing ideals $A_1, A_2, \ldots, A_n$. Then we say that $R$ is a direct sum of $A_1, A_2, \ldots, A_n$, and denote this by $R = A_1 \oplus \cdots \oplus A_n$, or $R = \bigoplus_{i=1}^n A_i$, if the following two conditions are satisfied:

1. $R = A_1 + \cdots + A_n$.
2. $A_i \cap (A_1 + \cdots + A_{i-1} + A_{i+1} + \cdots + A_n) = 0$ for $i = 1, 2, \ldots, n$.

Property 5.2. (1) Let $A$, $B$ be ideals in a ring $R$. Then $AB \subseteq A \cap B$. In addition, if $A \cap B = 0$, then $AB = BA = 0$.

(2) If $R = A_1 \oplus \cdots \oplus A_n$, then every element $a \in R$ has a unique representation as the sum $a = \sum_{i=1}^n a_i$ where each $a_i \in A_i$.

(3) For $R = A_1 \oplus \cdots \oplus A_n$ denote by $\pi_i$ the projection of $R$ onto $A_i$, where for each $a \in R$, $a = \sum_{i=1}^n a_i$ ($a_i \in A_i$) we set $\pi_i(a) = a_i$. Because of the uniqueness of the representation of $a$ (see (3)), $\pi$ is a map. Then $\pi_i$ is a homomorphism (of $R$ onto $A_i$) (why?). It is easy to see that $\text{Ker}(\pi) = \bigoplus_{j=1, j\neq i}^n A_j$. Thus $R/(\bigoplus_{j=1, j\neq i}^n A_j) \cong A_i$.

(4) If $R$ has an identity 1 and $R = A_1 \oplus \cdots \oplus A_n$, then $1 = \sum_{i=1}^n e_i$ where $e_i$ is the identity of $A_i$. Moreover, in this case if $C$ is an ideal of $R$, then $C = \bigoplus_{i=1}^n (A_i \cap C)$.

(5) Under the assumptions of (5) we obtain $R/C \cong \bigoplus_{i=1}^n [A_i/(A_i \cap C)]$.

(6) For a ring $S$, we denote by $M_k(S)$ the ring of all $k \times k$ matrices over $S$. If $R = A_1 \oplus \cdots \oplus A_n$, then $M_k(R) = M_k(A_1) \oplus \cdots \oplus M_k(A_n)$ (prove it!). Similarly it holds for the polynomial ring over $R$, i.e., we have $R[x] = A_1[x] \oplus \cdots \oplus A_n[x]$.

(7) If $R = A_1 \oplus \cdots \oplus A_n$, then $R/A_i \cong \bigoplus_{j=1, j\neq i}^n A_j$. 
(8) For the ring \( \mathbb{Z}_m \) it is easy to see a decomposition of \( \mathbb{Z}_m \). Namely, \( m = p_1^{m_1} \cdots p_k^{m_k} \) where the \( p_i \)'s are distinct primes and each \( m_i \) is a positive integer, then \( \mathbb{Z}_m \cong \bigoplus_{i=1}^{k} \mathbb{Z}_{p_i^{m_i}} \).

For example if \( m = 6 \), then since \( 6 = 2 \cdot 3 \), we have \( \mathbb{Z}_6 = \{0, 3\} \oplus \{\overline{0}, \overline{3}\} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3 \).

6. Maximal and Prime Ideals

Definitions 6.1. (1) Let \( M \) be a proper ideal of a ring \( R \). Then \( M \) is called a maximal ideal of \( R \) if for any ideal \( A \) of \( R \), \( M \subseteq A \subseteq R \) implies either \( A = M \) or \( A = R \).

(2) An ideal \( P \) of a ring \( R \) is called a prime ideal of \( R \) if for any ideals \( A \), \( B \) of \( R \), the relation \( AB \subseteq P \) implies either \( A \subseteq P \) or \( B \subseteq P \).

(3) A ring \( R \) is called a prime ring if \( (0) \) is a prime ideal of \( R \).

Property 6.2. (1) Let \( R \) be a ring with identity. Then every maximal ideal of \( R \) is prime. But the converse is not true in general, i.e., there are prime ideals of \( R \) that are not maximal.

(2) If \( R \) is a commutative ring with identity and \( M \) is a maximal ideal of \( R \), then \( R/M \) is a field.

(3) For any prime number \( p \), \( p\mathbb{Z} \) is a maximal ideal of \( \mathbb{Z} \). Every nonzero prime ideal of \( \mathbb{Z} \) has the form \( p\mathbb{Z} \) for some prime number \( p \). Notice that \( (0) \) is also a prime ideal of \( \mathbb{Z} \).

(4) Let \( K \) be a field, and \( K[x] \) be the polynomial ring over \( K \).

(4a) A non-constant polynomial \( f(x) \in K[x] \) is defined to be irreducible if whenever \( f(x) = f_1(x)f_2(x) \), (\( f_i(x) \in K[x] \)) then either \( f_1(x) \in K \) or \( f_2(x) \in K \).

(4b) Every ideal \( A \) of \( K[x] \) is principal, i.e., \( A \) is generated by an element of \( K[x] \). \( A \) is a maximal ideal of \( K[x] \) if and only if \( A = f(x)K[x] \) for some irreducible polynomial \( f(x) \in K[x] \).

(4c) From (2) and (4b) it follows that \( K[x]/(g(x)) \) is a field if and only if \( g(x) \) is an irreducible polynomial in \( K[x] \). In particular, \( \mathbb{R}[x]/(x^2 + 1) \) is a field, and it can be shown that \( \mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C} \). One can find many factor rings of \( \mathbb{R}[x] \) that are fields. For example \( \mathbb{R}[x]/(x^2 + x + 1) \), or \( \mathbb{R}[x]/(x^2 - x + 1) \) are also fields (why?).

(5) Let \( K \) be a field, and let \( f(x) \in K[x] \). An element \( \alpha \in K \) (or \( \alpha \) is in some larger field \( L \) containing \( K \)) is called a root of \( f(x) \) if \( f(\alpha) = 0 \). A field \( K \) is called algebraically closed, if every non-constant polynomial of \( K[x] \) has a root in \( K \).

(6) We know that every non-constant polynomial of \( \mathbb{C}[x] \) has all roots in \( \mathbb{C} \). Hence every irreducible polynomial of \( \mathbb{C}[x] \) has degree 1, i.e., in \( \mathbb{C}[x] \) only polynomials of the form \( ax + b \) (\( a, b \in \mathbb{C}, \ a \neq 0 \)) are irreducible. Hence \( \mathbb{C} \) is an algebraically closed field.
(7) Division algorithm in $K[x]$ where $K$ is a field: Let $f(x), g(x) \in K[x]$ such that $\deg(g(x)) \geq 1$. Then there exist $k(x), r(x) \in K[x]$ such that

$$f(x) = k(x)g(x) + r(x),$$

where either $r(x) = 0$ or $0 \leq \deg(r(x)) < \deg(g(x))$. Using this one can prove, for example, (4b) easily.

(8) There are some criteria of finding out the irreducibility of some types of polynomials in $\mathbb{Q}[x]$. However we don’t discuss these here.

Next part will be on Module Theory!