1. Rings and ideals

1.1 Rings and ring homomorphisms

Definition 1 (Ring): A *ring* A is a set with two binary operations called addition and multiplication such that

1. A is an abelian group with respect to addition.
2. Multiplication is associative.
3. Multiplication is commutative, and distributive over addition.
4. There is a multiplicative identity.

Definition 2 (Ring homomorphism): A *ring homomorphism* is a map $f : A \to B$ such that

1. $f(a+b) = f(a) + f(b)$ for all $a, b \in A$ (that is f is a group homomorphism over the additive structure).
2. $f(ab) = f(a)f(b)$ for all $a, b \in A$.
3. $f(1) = 1$.

Definition 3 (Subring): A subset S of a ring A is a *subring* if S is additively and multiplicatively closed, and contains the multiplicative identity.

1.2 Ideals and quotient rings

Definition 4 (Ideal): An ideal $\mathfrak{a}$ of a ring A is an additive subgroup such that $A\mathfrak{a} \subseteq \mathfrak{a}$ (that is, $x \in A \wedge y \in \mathfrak{a} \Rightarrow xy \in \mathfrak{a}$).

The multiples ax of an element $x \in A$ form a *principal ideal* which we denote by (x). By convention, we denote (0) by 0.

Result 5: There is a one-to-one, order-preserving correspondence between the ideals $\mathfrak{b}$ of A which contain $\mathfrak{a}$, and the ideals $\overline{\mathfrak{b}}$ of $A/\mathfrak{a}$ given by $\mathfrak{b} = \varphi^{-1}\left(\overline{\mathfrak{b}}\right)$.

Proof.

□

Definition 6 (Kernel): The *kernel* of a ring homomorphism $f : A \to B$ is the pre-image of $0 \in B$; notatively $\ker(f) = f^{-1}(0)$.

Result 7: For any ring homomorphism $f : A \to B$, $\ker(f)$ is an ideal $\mathfrak{a}$ of A, $\operatorname{im}(f)$ is a subring C of B, and f induces a ring isomorphism $A/\mathfrak{a} \cong C$.

1.3 Zero divisors, nilpotent elements and units

Definition 8 (Zero divisor): An element $x \in A$ is a *zero divisor* if there exists an element $0 \neq y \in A$ such that $xy = 0$.

Definition 9 (Integral domain): A ring without zero divisors is called an *integral domain*.

Definition 10 (Nilpotent): An element $x \in A$ is *nilpotent* if $x^n = 0$ for some $n > 0$.

Definition 11 (Unit): An element $x \in A$ is a *unit* if there exists an element $y \in A$ such that $xy = 1$. If it exists, this y is unique, and denoted by x^{-1}.

Result 12: An element $x \in A$ is a unit if and only if $(x) = A$.

Proof. Let x be a unit, and $x^{-1} \in A$ it's multiplicative inverse. Then $1 = x^{-1}x \in (x)$, hence $(x) = A$. If $(x) = A$, $1 \in (x)$, and hence there exists an element $y \in A$ such that $yx = 1$. □

Definition 13 (Field): A field is a ring in which $0 \neq 1$ and every non-zero element is a unit.

Result 14: A field is an integral domain.

Proof. Let $x \in A$ be a unit, and suppose that it is also a zero divisor. Then, there exists an element $y \in A$ such that $xy = 0$. But $0 = x^{-1}0 = x^{-1}xy = 1y = y$. □

Result 15: Let A be a non-zero ring. The following are equivalent,

i) A is a field;
ii) the only ideals in A are (1) and 0;
iii) every homomorphism of A into a non-zero ring B is injective.

Proof. ($\mathrm{i} \iff \mathrm{ii}$) is a direct consequence of Result 12.

($\mathrm{ii} \iff \mathrm{iii}$): Let $\varphi : A \to B$ be a homomorphism. Then $\ker(\varphi)$ is an ideal by Result 7. If $\ker(\varphi) = 0$, φ is injective. If $\ker(\varphi) = A$, B is trivial. □

1.4 Prime and maximal ideals

Definition 16 (Prime ideal): An ideal $\mathfrak{p}$ is *prime* if $\mathfrak{p} \neq (1)$ and $xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p} \vee y \in \mathfrak{p}$.

Definition 17 (Maximal ideal): An ideal $\mathfrak{m}$ is *maximal* if there is no ideal $\mathfrak{a}$ such that $\mathfrak{m} \subset \mathfrak{a} \subset (1)$.

Result 18: Equivalent formulations of primality and maximality are,

$$\mathfrak{p} \text{ is prime} \iff A/\mathfrak{p} \text{ is an integral domain}$$
$$\mathfrak{m} \text{ is maximal} \iff A/\mathfrak{m} \text{ is a field.}$$

Result 19: Every ring has at least one maximal ideal.

Result 20: If $\mathfrak{a} \neq (1)$ is an ideal in A, there exists a maximal ideal of A containing $\mathfrak{a}$.

Proof. This is a direct consequence of Result 19. □

Result 21: Every non-unit of A is contained in a maximal ideal.

Proof. This is a direct consequence of Result 19 together with Result 12. □

Definition 22 (Local ring): A ring A with exactly one maximal ideal $\mathfrak{m}$ is called a *local ring*. A ring with a finite number of maximal ideals is called a *semi-local ring*.