6. Introduction to Rings

6.1 Definition of Rings

A ring $(R, +, \cdot)$ is a set R with two law of compositions $+$ and $\cdot$, called addition and multiplication respectively, that satisfy:

1. $(R, +)$ forms an abelian group
2. "$\cdot$" is associative and there is a multiplicative identity $1 \in R$ s.t. $1 \cdot r = r \cdot 1 = r, \forall r \in R$
3. (Distributive Law) For any $a, b, c \in R$:

   $(a + b)c = ac + bc$, $c(a + b) = ca + cb$

If the multiplication of a ring is commutative, it is a commutative ring. The subject to study commutative rings is Commutative Algebra, which is the algebraic foundation of Algebraic Geometry.

Notation. In a ring, the additive identity is usually denoted by 0 and the multiplicative identity is usually denoted by 1.

Examples:

1. $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$
2. $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$, $\bar{a} + \bar{b} = \overline{a + b}$, $\bar{a}\bar{b} = \overline{ab}$
3. $M_{n \times n}(\mathbb{R})$, the set of $n \times n$ real matrices is a non-commutative ring with addition and multiplication of matrices.
4. $C(\mathbb{R})$, the set of all continous functions $\mathbb{R} \to \mathbb{R}$, with $(f + g)(x) = f(x) + g(x)$, $(fg)(x) = f(x)g(x)$.
5. The zero ring $R = \{0\}$, $0 + 0 = 0$, $0 \cdot 0 = 0$.

Prop. R is a ring. $0 = 1 \iff R = \{0\}$.

Pf. If $R = \{0\}$, it is obvious since $1 \in R = \{0\}$.

If $0 = 1$ in R, then $\forall r \in R$, $r = 1 \cdot r = 0 \cdot r = 0$.

Prop. R is a ring. Then:

1. $0 \cdot a = a \cdot 0 = 0$
2. $-a = (-1) \cdot a$
3. $-(ab) = (-a)b = a(-b)$

Pf. $0 \cdot a + a = 0 \cdot a + 1 \cdot a = (0 + 1) \cdot a = 1 \cdot a = a \to 0 \cdot a = 0$

$(-1) \cdot a + a = (-1) \cdot a + 1 \cdot a = (-1 + 1) \cdot a = 0 \cdot a = 0$

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

In general, not every element in a ring has an multiplication inverse.

R is a ring. $u \in R$ is a unit if it has an multiplication inverse $u^{-1} \in R$ such that $uu^{-1} = 1$.

Prop. The set of units of a ring R form a group with respect to multiplication, denoted by $R^{\times}$, called the group of units of R.

e.g. $(\mathbb{Z}, +, \cdot)$. $\mathbb{Z}^{\times} = \{\pm 1\}$.

e.g. $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$. $\mathbb{Z}^{\times} = \{\overline{a} : \gcd(\overline{a}, n) = 1\}$.

R is a ring, $x, y \in R$. We say x is associated to y if there exists $u \in R^{\times}$ such that $x = uy$.

Prop. R is a ring."$x \sim y$ if x is associated to y" is an equivalence relation on R.

A field is a ring R with $R^{\times} = R \setminus \{0\}$, i.e., all the nonzero elements are units.

e.g. $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ where p is a prime

6.2 Polynomial Rings

The polynomial ring $R[x]$ is the set of all polynomials with coefficients in R, with

addition: $(\sum a_i x^i) + (\sum b_i x^i) = \sum (a_i + b_i) x^i$

multiplication: $(\sum a_i x^i)(\sum b_i x^i) = \sum_k (\sum_{i+j=k} a_i b_j) x^k$

A polynomial is monic if its leading coefficient is 1.

The degree of a polynomial is the biggest power of x with nonzero coefficient.

Prop. (Division Algorithm) If $f(x) \in R[x]$ is a monic polynomial, then for any $g(x) \in R[x]$, $\exists! q(x) \in R[x]$, $r(x) \in R[x]$ such that $g(x) = q(x)f(x) + r(x)$, with $\deg(r) < \deg(f)$.

A ring R is called an integral domain if $ab = 0 \to a = 0/b = 0$. (i.e., $\forall a, b \in R, a \neq 0, b \neq 0$, then $ab \neq 0$.)

Prop. If R is an integral domain. Then $(R[x])^{\times} = R^{\times}$.

Cor. If R is an integral domain, $p(x), q(x) \in R[x] - \{0\}$, then $\deg(pq) = \deg(p) + \deg(q)$.

6.3 Ring Homomorphisms

A ring homomorphism $f : R \to R'$ is a map from a ring R to a ring R' such that

1. $\forall a, b \in R$, $f(a + b) = f(a) + f(b)$
2. $\forall a, b \in R$, $f(ab) = f(a)f(b)$
3. $f(1) = 1'$

Remark. (3) is to avoid the situation $f(r) = 0\ \forall r \in R$.

e.g. $f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $f(k) = \overline{k}$ is a ring homomorphism.

$f(a + b) = \overline{a + b} = \overline{a} + \overline{b} = f(a) + f(b)$, $f(ab) = \overline{ab} = \overline{a}\overline{b} = f(a)f(b)$, $f(1) = \overline{1}$

R is a ring. $r_0 \in R$. Define

$E_{r_0} : R[x] \to R$

$p(x) \mapsto p(r_0)$

E_{r_0}, called the evalutation map, is a ring homomorphism.

Prop. (Substituion Principle) $f : R \to R'$ is a ring homomorphism. $r'_0 \in R'$. Then there exists unique ring homomorphism $F : R[x] \to R'$ satisfying $F|_R = f$ and $F(x) = r'_0$.

The kernel of a ring homomorphism $f : R \to R'$ is $\ker(f) = \{r \in R | f(r) = 0'\}$.

e.g. $f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $f(k) = \bar{k}$. $\ker(f) = n\mathbb{Z}$.

6.4 Ideals

A nonempty subset I of a ring R is an ideal if:

1. $\forall a, b \in I$, $a + b \in I$
2. $\forall \alpha \in I, \forall r \in R$, $\alpha r \in I$

Prop. The kernel of a ring homomorphism $f : R \to R'$ is an ideal of R.

Prop. If I is an ideal of a ring R, then I is a subgroup of R with respect to addition.

Examples:

1. $\{0\}$ is an ideal of R, R is an ideal of R.
2. By the above Prop, an ideal of $\mathbb{Z}$ is necessarily a subgroup of $(\mathbb{Z}, +)$, so the candidates are $n\mathbb{Z}$. For each of $n \in \mathbb{N}$, $n\mathbb{Z}$ satisfies definition of an ideal.
3. $R = R[x]$. Ideal $I = \{p \in R | p(0) = 0\}$.

Prop. R is a ring. I is an ideal of R. Then the following are equivalent:

1. $I = R$
2. $1 \in I$
3. $I \cap R^\times \neq \emptyset$

An ideal I of R is proper if $I \neq \{0\}$ and $I \neq R$.

Prop. R is a ring. $a \in R$. Then a is a proper ideal $\iff$ $a \notin R^\times \cup \{0\}$.

Cor. A nonzero ring ($R \neq \{0\}$) is a field $\iff$ it has no proper ideal.

A ring R is called an integral domain if for any $a, b \in R \setminus \{0\}$, $ab \neq 0$.

An integral domain is called a Principle Ideal Domain (PID) if all of its ideals are principal.

e.g. The ring of integers $\mathbb{Z}$ is a PID.

Prop. R is an integral domain. Then $R[x]$ is PID $\iff$ R is a field.

6.5 Quotient Rings

R is a ring and I is an ideal of R, the quotient ring R/I is the set of cosets of I in R, whose elements are $r + I$ $(r \in R)$, with addition: $(r_1+I)+(r_2+I)=(r_1+r_2)+I$

multiplication: $(r_1+I)(r_2+I)=r_1r_2+I$

e.g. $R=\mathbb{Z}$, $I=n\mathbb{Z}$, $R/I=\mathbb{Z}/n\mathbb{Z}$

A ring isomorphism is a bijective ring homomorphism.

R is isomorphic to R' if $\exists f: R\to R'$ a ring isomorphism. We write $R\cong R'$.

First Isomorphism Theorem for Rings. $f: R\to R'$ is a surjective ring homomorphism. $I=\ker(f)$. Then there exists a unique ring isomorphism $F: R/I\to R'$ such that $f=F\circ\pi$.

Example: $f:\mathbb{R}[x]\to\mathbb{C}$ is a ring homomorphism

$$p(x)\mapsto p(i)$$

f is surjective since $\forall a+bi\in\mathbb{C}$, $f(a+bx)=a+bi$.

$\ker(f)=x^2+1$

By the first isomorphism theorem, $\mathbb{R}[x]/(x^2+1)\cong\mathbb{C}$

An ideal I in R $(I\neq R)$ is maximal if for any ideal J of R that $I\subseteq J$, either $J=I$ or $J=R$.

Prop. R is a ring and I is an ideal. Then I is a maximal ideal $\iff$ R/I is a field.

Pf. If I is maximal, then for any $x\neq I$,

$I\subsetneq I+(x)=R$, so $1\in R=I+(x)\to 1=a+rx$ for some $a\in I, r\in R$

$\to(r+I)(x+I)=(1-a)+I=1+a\to x+I$ is invertible

If I is not maximal, then $\exists J: I\subsetneq J\subsetneq R$.

It follows J/I is a proper ideal in R/I. So R/I cannot be a field.

F is a field. A polynomial $p(x)\in F[x]$ is irreducible if it's not a prodect of two non-constant polynomials in $F(x)$.

Prop. $p(x)\in F[x]$ is irreducible $\iff$ $(p(x))$ is maximal.

Pf. If $p(x)$ is not irreducible, $p(x)=q(x)r(x)$, $\deg q\geq 1$, $\deg r\geq 1$,

then $(p(x))\subsetneq(r(x))\subsetneq F[x]$, so $(p(x))$ is not maximal.

If $(p(x))$ not maximal, $\exists J$ s.t. $(p(x))\subsetneq J\subsetneq F[x]$

$F[x]$ is PID, so $J=(m(x))$. $J\neq F[x]\to\deg m\geq 1$.

$p(x)\in(p(x))\subseteq(m(x))$, so $p(x)=m(x)g(x)$ and $\deg g\geq 1$, otherwise $(p(x))=(m(x))$, so $p(x)$ is not irreducible.

Cor. $F[x]/(p(x))$ is a field $\iff$ $p(x)$ is an irreducible polynomial.

e.g. $\mathbb{R}[x]/(x^2+1)$ is a field since x^2+1 is irreducible in $\mathbb{R}[x]$.

$\mathbb{R}[x]/(x^2-1)$ is not a field since $x^2-1=(x-1)(x+1)$.

Actually, $\mathbb{R}[x]/(x^2-1)$ is not an integral domain since $(x-1+I)(x+1+I)=(x-1)(x+1)+I=(x^2-1)+I=0+I$.

$F \subseteq E$ are fields. $\gamma \in E$. We say γ is algebraic over F is $\exists p(x) \in F$ such that $p(\gamma) = 0$.

If $F \subseteq E$. $\gamma \in E$ is algebraic. The nonzero monic polynomial $m(x) \in F[x]$ of least degree satisfying $m(\gamma) = 0$ is the minimal polynomial of γ.

Prop. The minimal polynomial $m(x)$ of an algebraic γ over F is irreducible in $F[x]$.