§ 6 Rings and Fields

Introduction to Rings and Fields

Definition 6.1

A ring is a set R equipped with binary operations $+$ and $\cdot$ (usually called addition and multiplication) that satisfy

R1) $(R,+)$ is an abelian group.

R2) Multiplication $\cdot$ is associative.

R3) (Distributive Law) For all $a,b,c\in R$, $a\cdot(b+c)=a\cdot b+a\cdot c$ and $(a+b)\cdot c=a\cdot c+b\cdot c$.

Remark: The additive identity is usually denoted by 0.

Example 6.1

$\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$ with usual additions and multiplications are rings

$R=\{e\}$ with $e+e=e$ and $e\cdot e=e$ is a ring, called trivial ring.

$M_{n\times n}(\mathbb{R})$ is a ring.

$n\mathbb{Z}=\{na\cdot a\in\mathbb{Z}\}$ is a ring

$\mathbb{Z}_n=\mathbb{Z}/n\mathbb{Z}$ is a ring.

$\mathbb{R}[x]$ = set of all polynomials with real coefficients is a ring.

Example 6.2

Let $R_1,R_2,\cdots,R_n$ be rings. Then $R=R_1\times R_2\times\cdots\times R_n$ is a ring with

$(a_1,a_2,\cdots,a_n)+(b_1,b_2,\cdots,b_n)=(a_1+b_1,a_2+b_2,\cdots,a_n+b_n)$ and

$(a_1,a_2,\cdots,a_n)\cdot(b_1,b_2,\cdots,b_n)=(a_1\cdot b_1,a_2\cdot b_2,\cdots,a_n\cdot b_n)$ where $a_i,b_i\in R_i$.

Notations:

If R is a ring and $a\in R$,

the additive inverse of a is denoted by $-a$.

$\underbrace{a+a+\cdots+a}_{n}$ is denoted by na.

Caution: n is a positive integer, which may not be an element of R.

If n is a negative integer, na means $(-a)+(-a)+\cdots+(-a)$.

If n is zero, $0a=0$

integer additive identity in R

Proposition 6.1

If R is a ring with additive identity 0, then for any $a, b \in R$, we have

1) $0 \cdot a = a \cdot 0 = 0$

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

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

Definition 6.2

Let R and R' be rings.

A function $\phi : R \to R'$ is said to be a ring homomorphism from R to R' if for all $a, b \in R$

1) $\phi(a+b) = \phi(a) + \phi(b)$

2) $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$

In particular, if ϕ is bijective, ϕ is said to be a ring isomorphism.

Proposition 6.2

If $\gcd(r,s) = 1$, $\phi : \mathbb{Z}_{rs} \longrightarrow \mathbb{Z}_r \times \mathbb{Z}_s$ defined by $\phi(n) = n(1,1)$ is a ring isomorphism.

Definition 6.3

A ring in which the multiplication is commutative is a commutative ring

A ring with a multiplicative identity is a ring with unity.

Definition 6.4

Let R be a ring with unity $1 \neq 0$. An element u in R is a unit if it has a multiplicative inverse.

If every nonzero element of R is a unit, then R is a division ring.

A field is a commutative division ring.

Idea: Multiplication of a field is commutative and we can "perform division" on a field by defining a/b by ab^{-1} if $b \neq 0$.

Caution: For example, in $M_{m \times n}(\mathbb{R})$, the additive and multiplicative identity are the zero matrix and identity matrix (but not real numbers 0 and 1).

Sometimes, it may be more convenient to write down every condition as the following:

A field F is a set equipped with binary operations $+$ and $\cdot$ with such that

(A1) (Commutative law) $a+b=b+a$ for all $a,b\in F$.

(A2) (Associative law) $(a+b)+c=a+(b+c)$ for all $a,b,c\in F$

(A3) (Existence of 0) there exists $0\in F$ such that $a+0=0+a$ for all $a\in F$

(A4) (Existence of additive inverse) for all $a\in F$, there exists $b\in F$ such that $a+b=b+a=0$.

(M1) (Commutative law) $a\cdot b=b\cdot a$ for all $a,b\in F$.

(M2) (Associative law) $(a\cdot b)\cdot c=a\cdot(b\cdot c)$ for all $a,b,c\in F$

(M3) (Existence of 1) there exists $1\in F\setminus\{0\}$ such that $a\cdot 1=1\cdot a$ for all $a\in F$.

(M4) (Existence of multiplicative inverse) for all $a\in F\setminus\{0\}$, there exists $b\in F$ such that

$$a\cdot b=b\cdot a=1$$

(D) (Distributive law) $a\cdot(b+c)=a\cdot b+a\cdot c$ and $(b+c)\cdot a=b\cdot a+c\cdot a$ for all $a,b,c\in F$.

Definition 6.5

If a and b are nonzero element of a ring R such that $ab=0$, then a and b are called divisors of 0.

An integral domain D is a commutative ring with unity $1\neq 0$ and containing no divisors of 0

Proposition 6.3

Every field is an integral domain.

proof:

By definition, a field is a commutative division ring and hence a commutative ring with unity $1\neq 0$. Therefore, it suffices to show that a field has no divisors of 0.

Let F be a field and let $a,b\in F$ such that $a\cdot b=0$.

If $a=0$, it is done!

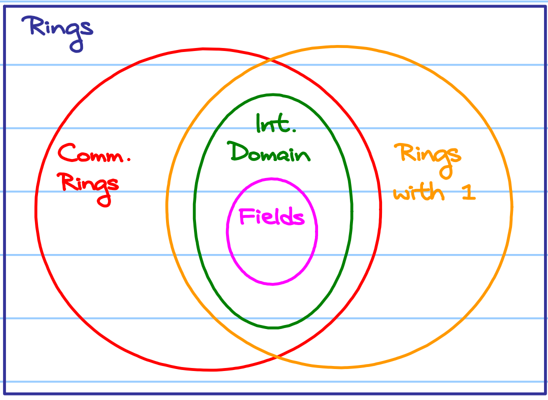
If $a\neq 0$, a^{-1} exists and $a^{-1}\cdot(a\cdot b)=a^{-1}\cdot 0$

$$(a^{-1}\cdot a)\cdot b=0 \qquad \text{(R2 and prop. 6.1)}$$

$$1\cdot b=0$$

$$b=0$$

$\therefore$ There is no divisor.



Exercise 6.1

Verify the following:

	$\mathbb{Z}$	$n\mathbb{Z}$ $(n>1)$	$\mathbb{Z}_n$ $(n:$ NOT $\text{prime})$	$\mathbb{Z}_p$ $(p:\text{prime})$	$M_{n\times n}(\mathbb{R})$	$GL_n(\mathbb{R})$	$\mathbb{Q}$
Commutative Ring	✓	✓	✓	✓			✓
Ring with Unity	✓		✓	✓	✓	✓	✓
Division Ring				✓		✓	✓
Integral Domain	✓			✓		✓	✓
Field				✓			✓

To check if $\mathbb{Z}_p$ is a field (where p is a prime), the only nontrivial part is proving the existence of multiplicative inverse.

Let $[n] \in \mathbb{Z}_p$, for $1 \leq n \leq p-1$.

Since $\gcd(n,p)=1$, there exists $r,s \in \mathbb{Z}$ such that $nr+ps=1$.

Then $nr \equiv 1 \pmod p$, i.e. $[n]^{-1}=[r]$.

Definition 6.6

Let R be a ring. If there exists a positive integer n such that $na=0$ for all $a \in R$, then the least such positive integer is said to be the characteristic of the ring R. If no such positive integer exists, then R is said to be of characteristic 0.

Example 6.3

$\mathbb{Z}_n$ is of characteristic n.

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are of characteristic 0.

Proposition 6.4

Let R be a ring with unity.

1) If $n \cdot 1 \neq 0$ for all $n \in \mathbb{Z}^+$, then R has characteristic 0.

2) If n is the least positive integer such that $n \cdot 1 = 0$, then R has characteristic n.

Remark: To find the characterist of R, it suffices to look at 1.

proof:

1) trivial.

2) Let $a \in R$

$na = a + a + \cdots + a = a(1+1+\cdots+1) = a\cdot(n\cdot 1) = a \cdot 0 = 0$

$\therefore$ characteristic of $R \leq n$

However, if characteristic of $R < n$, it contradicts to the fact that n is the least positive integer such that $n \cdot 1 = 0$.

$\therefore$ characteristic of $R = n$

Ideals and Factor Rings

Definition 6.7

Let N be a subset of a ring R. N is said to be an ideal of R if

1) N is a subgroup of $(R,+)$.

2) $aN = \{a \cdot x : x \in N\} \subseteq N$ and $bN = \{x \cdot b : x \in N\} \subseteq N$

Remark: If R is a commutative ring, we have $aN = Na$.

Example 6.4

Let $n \in \mathbb{Z}$. Then, $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

Exercise 6.1

Prove that every ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z}$

Example 6.5

Let $p(x) \in \mathbb{R}[x]$ and let $\langle p(x) \rangle = \{p(x)q(x) : q(x) \in \mathbb{R}[x]\}$

Then $\langle p(x) \rangle$ is an ideal of $\mathbb{R}[x]$.

Proposition 6.5

Let R be a ring with unity and let N be an ideal of R

$N=R$ if and only if $1\in N$.

proof:

"$\Rightarrow$" Trivial.

"$\Leftarrow$" Clearly $N\subseteq R$. To show $N=R$, it suffices to show $R\subseteq N$.

Let $a\in R$. Note that $aN\subseteq N$ and $1\in N$, so $a=a\cdot 1\in N$ and $R\subseteq N$.

Recall: Let R be a ring and let N be an ideal of R.

We can define a relation $\sim$ on R such that $a\sim b$ if $a-b\in N$ and

in fact $\sim$ is an equivalence relation.

Let $a\in R$, the equivalence class of a is $a+N=\{a+x : x\in N\}$

(left cosets of N in the additive group $(R,+)$,

in fact $a+N=N+a$, since $(R,+)$ is an abelian group.)

Then, the set of all equivalence classes is denoted by R/N (instead of $R/\sim$).

Proposition 6.6

R/N is ring with addition and multiplication defined by

$(a+N)+(b+N):=(a+b)+N$ and $(a+N)\cdot(b+N)=(a\cdot b)+N$.

R/N is called factor ring or quotient ring of R by N.

Example 6.6

$\mathbb{R}[x]/\langle x^2+1\rangle = \{g(x)+\langle x^2+1\rangle : g(x)\in\mathbb{R}[x]\}$ (Recall: $g(x)+\langle x^2+1\rangle = \{g(x)+(x^2+1)q(x) : q(x)\in\mathbb{R}[x]\}$)

$= \{r(x)+\langle x^2+1\rangle : r(x)=a_0+a_1x,\ a_0,a_1\in\mathbb{R}\}$

why?

By division algorithm, for any $g(x)\in\mathbb{R}[x]$, there exist unique $q(x)$, $r(x)=a_0+a_1x$ such that

$g(x)=(x^2+1)q(x)+r(x)$. Therefore, $g(x)\equiv r(x) \pmod{x^2+1}$

$g(x)+\langle x^2+1\rangle = r(x)+\langle x^2+1\rangle$ (Just an analogue to $\mathbb{Z}/n\mathbb{Z}$)

Idea: Given a commutative ring R and an ideal N.

Will we get a "better" ring by taking quotient, i.e. R/N?

Example 6.7

$\mathbb{Z}$ is an integral domain and $n\mathbb{Z}$ is an ideal.

Consider the factor ring $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$.

If $n=0$, $\mathbb{Z}_n$ is isomorphic to $\mathbb{Z}$ (still an integral domain).

If $n=p$ which is a prime, $\mathbb{Z}_p$ is a field (better!)

If $n=6$, $\mathbb{Z}_6$ is not an integral domain as $[2]\cdot[3]=[6]=[0]$ (worse!).

Example 6.8

The ring $\mathbb{Z}\times\mathbb{Z}$ is not an integral domain as $(1,0)\cdot(0,1)=(0,0)$.

Check: $N=\{(0,n): n\in\mathbb{Z}\}$ is an ideal of $\mathbb{Z}\times\mathbb{Z}$

$\mathbb{Z}\times\mathbb{Z}/N = \{(a,b)+N : (a,b)\in\mathbb{Z}\times\mathbb{Z}\}$

$= \{(a,0)+N : a\in\mathbb{Z}\}$

which is isomorphic to $\mathbb{Z}$ (an integral domain, better!)

Definition 6.8

A prime ideal of a ring R is a proper ideal P such that for all $a,b\in R$,

if $ab\in P$, then either $a\in P$ or $b\in P$.

A maximal ideal of a ring R is a proper ideal M such that there exists no ideal N such that $M\subsetneq N\subsetneq R$.

Example 6.9

Let p be a prime. Then $p\mathbb{Z}$ is a proper ideal of $\mathbb{Z}$.

Suppose $a,b\in\mathbb{Z}$ such that $ab\in p\mathbb{Z}$.

We have $p\mid ab \Rightarrow p\mid a$ or $p\mid b \Rightarrow a\in p\mathbb{Z}$ or $b\in p\mathbb{Z}$.

$\therefore$ $p\mathbb{Z}$ is a prime ideal

Let N be an ideal such that $p\mathbb{Z}\subsetneq N\subseteq R$.

Then there exists $m\in N$ such that $m\notin p\mathbb{Z}$.

$\gcd(m,p)=1$ and so $1=mr+ps$ for some $r,s\in\mathbb{Z}$.

Since $m,p\in N$, $1\in N$ which implies $N=R$.

Therefore, there exists no ideal N of R such that $p\mathbb{Z}\subsetneq N\subsetneq R$.

$\therefore$ $p\mathbb{Z}$ is a maximal ideal.

Exercise 6.2

Show that $N = \{(0,n) : n \in \mathbb{Z}\}$ is a prime ideal, but not a maximal ideal of $\mathbb{Z} \times \mathbb{Z}$.

Proposition 6.7

Let R be a commutative ring with unity and let N be a proper ideal of R.

R/N is an integral domain if and only if N is a prime ideal.

R/N is a field if and only if N is a maximal ideal.

Remark: This gives us a way to construct fields.

Corollary 6.1

A maximal ideal of a commutative ring with unity is a prime ideal.

proof:

N is a maximal ideal $\Rightarrow$ R/N is a field

$\Rightarrow$ R/N is an integral domain

$\Rightarrow$ N is a prime ideal

Example 6.10

If p is a prime, $p\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$.

Therefore, $\mathbb{Z}/p\mathbb{Z}$ is a field.

Example 6.11

Think: Why $\langle x^2+1 \rangle$ is a maximal ideal?

Then, $\mathbb{R}[x]/\langle x^2+1 \rangle$ is a field

Brief discussion: Let $F = \mathbb{R}[x]/\langle x^2+1 \rangle$.

$\mathbb{R}$ can be regarded as a subfield of F by $a \mapsto (a+0x)+\langle x^2+1 \rangle$

Therefore, $f(x) = x^2+1 \in \mathbb{R}[x]$ can be regarded as an element in $F[x]$.

($f(x) = (1+\langle x^2+1 \rangle)\,x^2 + (1+\langle x^2+1 \rangle) \in F[x]$)

Note that we cannot find a real number x_0 such that $f(x_0) = 0$, but

$f(x+\langle x^2+1 \rangle) = (1+\langle x^2+1 \rangle)(x+\langle x^2+1 \rangle)^2 + (1+\langle x^2+1 \rangle) = (x^2+1)+\langle x^2+1 \rangle = 0+\langle x^2+1 \rangle$.

i.e. we extend $\mathbb{R}$ to a field F such that $x^2+1=0$ has a solution!

In fact, $\mathbb{C} := \mathbb{R}[x]/\langle x^2+1 \rangle$ and $a_0+a_1 i$ means $(a_0+a_1 x)+\langle x^2+1 \rangle$