Rings, ideals, and quotient rings

Definition A ring R (环) is a set together with two binary operations $+$ and $\cdot$, satisfying

(1) $(R,+)$ is an abelian group (with 0 the additive unit)

(2) $\cdot$ is associative i.e. $(a\cdot b)\cdot c = a\cdot(b\cdot c)$ $\forall\, a,b,c\in R$

(3) the distributive law holds in R : for all $a,b,c\in R$,

$$(a+b)\cdot c = a\cdot c + b\cdot c, \text{ and } a\cdot(b+c) = a\cdot b + a\cdot c$$

(4) R is unital (含单位元), i.e. $\exists$ an element $1_R\in R$, $1_R\neq 0_R$ ← important assumptions for this course.

s.t. $1_R\cdot a = a\cdot 1_R = a$ $\forall a\in R$.

- Say a ring R is commutative (交换环) if $a\cdot b = b\cdot a$ for all $a,b\in R$.

Definition A ring is called a division ring (可除环) or a skew field, if every nonzero element $a\in R$ has a multiplicative inverse

A commutative division ring is called a field (域)

Examples ① $\mathbb{Z}$, $\mathbb{Z}_n$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, ⋯

② $\mathbb{Z}[\frac{1}{N}] := \left\{\frac{a}{N^r}\in\mathbb{Q}\,;\, a\in\mathbb{Z},\, r\in\mathbb{Z}_{\geq 0}\right\}$ is a subring of $\mathbb{Q}$

③ If R is a ring, $R[x] = \left\{\sum_{n\geq 0} a_n x^n\,;\, a_n\in R\right\}$ is a ring

or more generally, $R[x_1,\cdots,x_n]$ (Often, we require R to be commutative)

④ If R is a ring, then $\mathrm{Mat}_n(R)$ is a ring

⑤ $\mathbb{H} = \{a+bi+cj+dk\,;\, a,b,c,d\in\mathbb{R}\}$ Hamiltonian quaternion (四元数)

multiplication: $i^2=j^2=k^2=-1$, $ij=-ji=k$, $jk=-kj=i$, $ki=-ik=j$.

Conjugate: $\overline{a+bi+cj+dk} := a-bi-cj-dk$, note $\overline{zw} = \bar{w}\cdot\bar{z}$.

$Nm(z) = z\bar{z} = a^2+b^2+c^2+d^2 \in \mathbb{R}_{\geq 0}$

So if $z \neq 0$, $z^{-1} := \bar{z}/Nm(z)$, So $\mathbb{H}$ is a division ring.

(In the construction above, we can replace $\mathbb{R}$ by $\mathbb{Q}$.)

⑥ Group ring (群环)

Let R be a (commutative) ring and G a (finite) group, say $G = \{\overset{e}{g_1}, \cdots, g_n\}$

Define $R[G] := \{a_1 g_1 + \cdots + a_n g_n \; ; \; a_i \in R\}$

$= \{\sum_{g \in G} a_g g \text{ finite sum}, \; a_g \in R\}$

multiplication : $\left(\sum_{g\in G} a_g g\right)\left(\sum_{h\in G} b_h h\right) := \sum_{g,h\in G} a_g b_h gh$

$1_{R[G]} = 1_R \cdot e_G$

Example : $G = Z_n = \langle \sigma \mid \sigma^n = 1 \rangle$

$R[G] = \{a_0 + a_1\sigma + \cdots + a_{n-1}\sigma^{n-1} \; ; \; a_i \in R\}$

satisfying $\sigma^n = 1$

$G = \mathbb{Z} = \langle \sigma \rangle$

$R[G] = R[x^{\pm 1}] = \{\sum_{n\in\mathbb{Z}} a_n x^n \; ; \; a_n \in R\}$

Definition Let R and S be rings

(1) A ring homomorphism (环同态) is a map $\varphi : R \to S$ satisfying

(a) $\varphi(a+b) = \varphi(a) + \varphi(b)$ for all $a, b \in R$ $\Rightarrow \varphi(0_R) = 0_S$.

(b) $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in R$

(c) $\varphi(1_R) = 1_S$ ← we will always assume this

(2) The kernel of φ is $\ker \varphi = \varphi^{-1}(0_S)$

φ is injective $\iff \ker\varphi = \{0_R\}$

(3) φ is an <u>isomorphism</u> if moreover φ is bijective.

<u>Example</u>: ① $\mathbb{Z} \xrightarrow{\varphi} Z_n$

② If R is a <u>commutative</u> ring, $\forall r \in R$

$$\phi_r : R[x] \longrightarrow R \qquad \text{Needs } R \text{ to be commutative!}$$
$$f(x) \longmapsto f(r)$$

<u>Definition</u> Let R be a ring.

(1) $0 \neq a \in R$ is called a <u>zero-divisor</u> (零因子) if $\exists\, 0 \neq b \in R$ s.t. either $ab = 0$ or $ba = 0$

(2) $u \in R$ is called a <u>unit</u> in R (可逆元) if $\exists\, v \in R$ s.t. $uv = vu = 1$

The set of units in R is $R^\times$. It is a group under multiplication.

- A <u>commutative</u> ring R containing no zero-divisor is called an <u>integral domain</u> (整环)

<u>Examples</u>: ① $Z_n^\times = \{ a \bmod n \mid \gcd(a,n) = 1 \}$

zero-divisors in $Z_n = \{ a \bmod n \mid \gcd(a,n) \neq 1,\ a \neq 0 \}$

② If R is an integral domain, so is $R[x]$

b/c $f(x) = a_m x^m + \cdots$, $g(x) = b_n x^n + \cdots$ $\quad a_m, b_n \neq 0$

$$\Rightarrow f(x)g(x) = \underbrace{a_m b_n}_{\neq 0} x^{m+n}$$

<u>Lemma</u>. A finite integral domain R is a field

Proof: <u>NTS</u> $\forall a \neq 0$ in R, a has a multiplicative inverse.

Consider $m_a : R \longrightarrow R$ is a homomorphism of additive groups

$x \longmapsto ax$

$\ker m_a = \{x \in R \mid ax = 0\} = \{0\}$

$\Rightarrow m_a$ is injective $\Rightarrow$ bijective

Then $a^{-1} := m_a^{-1}(1)$ is the inverse of a $\square$

Fraction field : R an integral domain

Define the fraction field (分式域) to be $\mathrm{Frac}(R) = \left\{ (a,b) \in R \times (R \setminus \{0\}) \right\} \Big/ (a,b) \sim (c,d)$ iff $ad = bc$

((a,b) written as $\frac{a}{b}$)

$\mathrm{Frac}(R)$ is a field.

Example : $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$, $\mathrm{Frac}(k[x]) = k(x)$

Question: Analogues of normal subgroups for rings?

Definition A subset $I \subseteq R$ is called a left ideal (左理想)

if (1) $\forall a, b \in I$, $a - b \in I$ (so I is a subgroup of $(R,+)$)

(2) $\forall a \in I$, $x \in R$, $xa \in I$

Say I is a right ideal if (2) is replaced by $ax \in I$.

Say I is an ideal (or a two-sided ideal) (双边理想)

if it is a left ideal and a right ideal.

(For commutative rings, left ideals = right ideals = two-sided ideals)

- An ideal is (usually) not a ring as $1_R \notin I$ $(1_R \in I \Rightarrow I = R)$

Definition Let R be a ring and I a two-sided proper ideal, i.e. $I \neq R$ (so the R/I is not the "zero ring")

Define the quotient ring (商环) $R/I := \{x+I \mid x \in R\}$ (quotient as additive groups)

$$(x+I)+(y+I) = x+y+I+I = (x+y)+I$$

$$(x+I)\cdot(y+I) = xy+I$$

Check: multiplication is well-defined:

if $x' = x+a$, $y' = y+b$ for $a, b \in I$

then $x'y'+I = (x+a)(y+b)+I = xy + xb + ay + ab + I$ (all in I)

There is a natural surjective quotient homomorphism

$$\pi : R \twoheadrightarrow R/I$$

$$x \longmapsto x+I =: \bar{x} \qquad \text{with } \ker(\pi) = I$$

Isomorphism Theorems

1st Thm. If $\varphi : R \to S$ is a homomorphism of rings,

then $\ker\varphi$ is a two-sided ideal and $\varphi(R)$ is a subring of S

Moreover φ induces an isomorphism $R/\ker\varphi \xrightarrow{\sim} \varphi(R)$

$$x+\ker\varphi \longmapsto \varphi(x)$$

4th Thm Let I be a proper ideal of R. Then there is a 1-1 correspondence

$$\{\text{left/right/two-sided ideals } J \supseteq I\} \longleftrightarrow \{\text{left/right/two-sided ideals } \bar{J} \text{ of } R/I\}$$

$$J \longmapsto J/I$$

$$\pi^{-1}(\bar{J}) \longmapsto \bar{J} \qquad \pi : R \to R/I$$

preserving orders, sums, intersections, quotients $((R/I)/(J/I) \simeq R/J)$, ...

Notation. Let R be a commutative ring, and let $(a_j)_{j\in J} \subseteq R$ be a subset

Define $(a_j ; j\in J) := \left\{ \sum_{j\in J} x_j a_j \text{ , each } x_j \in R \text{ and all but finitely many } x_j \text{ is zero} \right\} \subseteq R$

It is the ideal generated by a_J

It is the minimal ideal that contains all of $a_j ; j\in J$

Examples (1) $R = \mathbb{Z}$ $(4,6) = \{4x+6y ; x,y\in\mathbb{Z}\} = 2\mathbb{Z} = (2)$.

So $(a_1, \cdots, a_s) = (\gcd(a_1, \cdots, a_s))$ ← to be continued next lecture :)

(2) $\varphi : \mathbb{Z} \longrightarrow Z_n$ $\ker\varphi = n\mathbb{Z} = (n)$.

$a \longmapsto a \bmod n$ So $Z_n \simeq \mathbb{Z}/n\mathbb{Z}$

(3) R commutative $a\in R$ $\rightsquigarrow$ $\phi_a : R[x] \longrightarrow R$

$f(x) \longmapsto f(a)$

$\ker\phi_a = \{f(x)\in R[x], f(a)=0\} = (x-a)$ $\quad \forall f(x)\in R[x]$

↑ b/c can always write $f(x) = g(x)(x-a) + f(a)$

So $R[x]/(x-a) \simeq R$

(4) $R[G]$ group ring $\phi : R[G] \longrightarrow R$

$\sum_{g\in G} a_g g \longmapsto \sum_{g\in G} a_g$

$\ker\phi = (g-1 ; g\in G)$ called the augmentation ideal of $R[G]$ ← a very important ideal for group rings.

↑ means e_G

(5) $R = R_1 \times R_2$ direct product of rings

Then $R_1 \times \{0\}$ and $\{0\} \times R_2$ are ideals

Note: $R_1 \longrightarrow R_1 \times R_2$ does not take 1_{R_1} to $1_{R_1\times R_2}$

$a \longmapsto (a,0)$ so NOT a homomorphism in our convention!

Operations on ideal Let I, J be (two-sided) ideals of a ring R

(1) Define $I+J = \{ a+b \mid a \in I, b \in J \}$ sum of ideals

(2) The product of ideals $IJ = \{$ finite sums of elements ab for $a \in I, b \in J \}$

Caveat: In general, not all elements of IJ can be written as a pure product ab for $a \in I, b \in J$

E.g. $R = \mathbb{Z}[x]$, $I = (2,x) = \{ f(x) \in \mathbb{Z}[x] \mid f(0) = 2 \}$

$x^2+4 \in I^2$ but can't be written in the form of ab for $a, b \in (2,x)$

In practice: if R is commutative and $I = (a_1, \cdots, a_s)$, $J = (b_1, \cdots, b_t)$

then $I+J = (a_1, \cdots, a_s, b_1, \cdots, b_t)$, $IJ = (a_i b_j \; ; \; i=1,\cdots,s, j=1,\cdots,t)$

Meaning of quotient ring: imposing relations among generators

VERY IMPORTANT!

E.g. k field, $k[x,y,z] / (x-y^2, y-z^3) \simeq k[z]$

$$x^2y = (x-y^2+y^2)^2 y = (x-y^2)* + y^4 \cdot y = (x-y^2)* + (y-z^3+z^3)^5$$
$$= (x-y^2)* + (y-z^3)* + z^{15}$$

That means: in the quotient, $x = y^2$, $y = z^3$

Example: $\phi_i : \mathbb{R}[x] \longrightarrow \mathbb{C}$

$f(x) \longmapsto f(i)$ $\ker \phi_i = (x^2+1)$ ← prototype for field extns

describing $\mathbb{C}$ in terms of $\mathbb{R}$

So $\mathbb{R}[x]/(x^2+1) \simeq \mathbb{C}$

imposing a relation that $x^2 = -1$

- Let $f: R \to S$ be a ring homomorphism
  - $b \subseteq S$ an ideal $\Rightarrow f^{-1}(b)$ is an ideal
  - $a \subseteq R$ an ideal $\rightsquigarrow$