Lecture 1: Rings

29 August 2020
16:45

Def^n: A ring $(R, +, \cdot)$: R set, $+, \cdot : R \times R \to R$ binary operations satisfying the following axioms

1) $(R, +)$ is a commutative group (with 0_R the additive identity)
2) $a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall\, a, b, c \in R$
3) (i) $a \cdot (b + c) = a \cdot b + a \cdot c$ "
   (ii) $(b + c) \cdot a = b \cdot a + c \cdot a$ "

(*) R is said to be a ring with identity/unity if $\exists\, 1_R \in R$ s.t. $a \cdot 1_R = 1_R \cdot a = a \quad \forall\, a \in R$.

(*) R is said to be commutative if $\forall\, a, b \in R$
$a \cdot b = b \cdot a$.

Examples: 1) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $M_{n \times n}(\mathbb{R})$ (Math)

($\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$: Fields)

A comm ring

(**) R is said to be a field if $(R \setminus \{0_R\}, \cdot)$ is a group.

2) $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ is a ring.

3) $R = \{0\}$, the zero ring.

⊛ Ring homomorphism :

A function/map $\varphi : R_1 \to R_2$ is said to be a ring homomorphism if φ behaves well with respect to the two binary operators.

i.e. $$\varphi(a+b) = \varphi(a) + \varphi(b)$$
$$\varphi(ab) = \varphi(a) \cdot \varphi(b)$$
$\forall\, a, b \in R_1$.

Example: 1) $\varphi : \mathbb{Z} \longrightarrow \mathbb{Q}$ is a ring homo.
$n \longmapsto n$

$\omega : \mathbb{Z} \longrightarrow \mathbb{Q}$ Is this a ring homo? No!
$n \longmapsto -n$

$\omega_1 : \mathbb{Z} \longrightarrow \mathbb{Q}$ Is this a ring homo?
$n \longmapsto 2n$ $\varphi(nm) = 2nm \neq \varphi(n)\varphi(m)$

⊛ Let R_1, R_2 be two rings with unity.
Then a ring homo. $\varphi : R_1 \longrightarrow R_2$ is additionally required to send 1_{R_1} to 1_{R_2}
i.e. $\varphi(1_{R_1}) = 1_{R_2}$ $n \mapsto (n,0)$, $\mathbb{Z} \to \mathbb{Z}^2 = \{(a,b) \mid a,b \in \mathbb{Z}\}$, $(a_1,b_1)+(a_2,b_2) = (a_1+b_1, a_2+b_2)$

⊛ Note that $\varphi(0_{R_1}) = 0_{R_2}$ ($\because$ φ is a group homo $(R_1,+) \to (R_2,+)$)

⊛ R is a ring with unity (1) then
$-a = -1 \cdot a \quad \forall\, a \in R$.

Pf: $(a + -1 \cdot a) = (1 \cdot a + -1 \cdot a)$
$= (1 + -1) \cdot a$
$= 0 \cdot a = 0$
$\Rightarrow -a = -1 \cdot a$

In general $\det(A+B) \neq \det(A) + \det(B)$

⊛ $M_{n\times n}(\mathbb{R}) \xrightarrow{\det} \mathbb{R}$; Is this a ring homomorphism?

Defn: Let R be a ring with unity. An element $u \in R$ is said to be a unit if $\exists\, u' \in R$ s.t. $u \cdot u' = u' \cdot u = 1_R$.

Ex: 1) Units in $\mathbb{Z}$? $1, -1$ 2) $(\mathbb{Z}/n\mathbb{Z})^\times = \{[a] \mid (a,n) = 1\}$
Euler no $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$

Example: The set of all continuous function from $[0,1] \longrightarrow \mathbb{R}$. $\mathcal{C}[0,1]$ is a ring: $(f+g)(x) = f(x) + g(x)$, $\cdot$ by multiplication.

$\varphi_{1/5}: \mathcal{C}[0,1] \longrightarrow \mathbb{R}$ is

$f \longmapsto f(1/5)$

ring homo.

$\mathcal{C}[0,1]$ is a ring with unity.

$\underline{1}(x) = 1 \quad \forall\, x \in [0,1]$

$(f \cdot \underline{1})(x) = f(x) \cdot \underline{1} = f(x)$

Def^n: A ring homo $\varphi: R_1 \to R_2$ is said to be an injective ring homo / a monomorphism if φ is injective.

By φ is an epimorphism if φ is surjective and

φ is an isomorphism if φ is bijective.

(*) φ is an isomorphism $\Rightarrow$ $\psi := \varphi^{-1}: R_2 \to R_1$ is a homomorphism. And in this scenario R_1 is said to be isomorphic to R_2.

exercise

(*) Let $\varphi: R_1 \to R_2$ be a ring homomorphism Then $\mathrm{Im}(\varphi)$ is a subring of R_2 and $\ker(\varphi)$ is an ideal of R_1. $\mathrm{Im}(\varphi) = \{\varphi(r) \mid r \in R_1\}$ $\{r \in R_1 \mid \varphi(r) = 0\}$

Def^n: Let $(R,+,\cdot)$ be a ring and $R_1 \subseteq R$. We say R_1 is a subring of R if $(R_1,+,\cdot)$ is ring.

i.e. $\forall a,b \in R_1$, $a+b \in R_1$, $a\cdot b \in R_1$ and $-a \in R_1$.

Ex: $\mathbb{Z}$ is a subring of $\mathbb{Q}$. $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

$2\mathbb{Z} \subseteq \mathbb{Z}$ is subring
$\Uparrow$ is not a ring with unity

(*) In $\mathbb{Z}^2$, the set $\{(n,0) \mid n \in \mathbb{Z}\} = R_1$ is a subring

$1_{R_1} \neq (1,1) = 1_{\mathbb{Z}^2}$

(*) $1_R \in R_1 \Rightarrow 1_{R_1} = 1_R$

Def^n: Let R be a (commutative) ring with unity. A subset $I \subseteq R$ is said to be an ideal of R if

(1) $\forall a, b \in I$, $a+b \in I$

(2) $\forall a \in I$ & $\forall r \in R$, $ra \in I$. ← left ideal

(2') $\forall a \in I$ & $\forall r \in R$, $ar \in I$ ← right ideal

Prop: Kernel of a ring homo. is an ideal.

Pf: $\varphi : R_1 \to R_2$ be a ring homo.

$a, b \in \ker(\varphi)$ then $\varphi(a+b) = \varphi(a) + \varphi(b) = 0$

$r \in R_1$ & $a \in \ker\varphi \Rightarrow \varphi(ra) = \varphi(r)\varphi(a) = 0$ ∎

Example: Ideals of $\mathbb{Q}$

1) $\{0\} \subseteq \mathbb{Q}$ is an ideal

zero ideal → $\{0\}$ is always an ideal in any ring

2) $\mathbb{Q}$ is an ideal of $\mathbb{Q}$

R is always an ideal of any ring R.

(*) These are all the ideals of $\mathbb{Q}$.

Pf: $I \subseteq \mathbb{Q}$ be a nonzero ideal. $\Rightarrow \exists a \neq 0$ s.t. $a \in I$ ($a \in \mathbb{Q}$)

Let $b \in \mathbb{Q}$ then $\frac{b}{a} \in \mathbb{Q}$ & $\frac{b}{a}\cdot a = b \in I \Rightarrow I = \mathbb{Q}$.

(**) Let $(F, +, \cdot)$ be a field then the only ideals of F are (0) & F.

Pf: I nonzero ideal F, let $a \neq 0 \in I$ then $a^{-1} \in F$. Let $b \in F$ then $ba^{-1} \in F \Rightarrow ba^{-1} \cdot a \in I$ (b'') ∎

Ex: In $\mathbb{Z}$, what are the ideals?

(0), $\mathbb{Z}$, $n\mathbb{Z}$

Text books: 1) Dummit & Foote

2) M. Artin

3) S. Lang

Lecture 2:
02 September 2020
18:10

(*) Let R be a (comm) ring with unity.
Recall an ideal I of R is subset s.t. $\forall a,b \in I$ $a+b \in I$ and $\forall r \in R$ & $a \in I$, $ra \in I$.
A subring R_1 of R is a subset s.t. $\forall a,b \in R_1$, $a-b$ & ab are in R_1.

Examples: 1) $\mathbb{Z}[\sqrt{2}] = \{a+b\sqrt{2} \mid a,b \in \mathbb{Z}\}$ is a subring of $\mathbb{R}$
$(a+b\sqrt{2})(c+d\sqrt{2}) = ac+2bd+(ad+bc)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$.

2) $\mathbb{Z}[\frac{1}{2}] \subseteq \mathbb{Q}$ smallest subring of $\mathbb{Q}$ containing $\mathbb{Z}$ & $\frac{1}{2}$.
$\mathbb{Z}[\frac{1}{2}] = \{\frac{a}{2^n} \mid a \in \mathbb{Z}, n \geq 0, n \in \mathbb{Z}\} := R$

Pf: $R \supseteq \mathbb{Z}[\frac{1}{2}]$ ✓
Let $\alpha \in R$ then $\alpha = \frac{a}{2^n}$ for some $a \in \mathbb{Z}$ & $n \geq 0$.
$\Rightarrow \alpha = a \cdot (\frac{1}{2})^n \in \mathbb{Z}[\frac{1}{2}] \Rightarrow R \subseteq \mathbb{Z}[\frac{1}{2}]$.

3) $\mathbb{Z}[\pi] \subseteq \mathbb{R}$; $\mathbb{Z}[\pi] = \{a_0+a_1\pi+a_2\pi^2+\dots+a_n\pi^n \mid n \geq 0, a_0,\dots,a_n \in \mathbb{Z}\}$

(*) $\mathbb{Z}[i] \subseteq \mathbb{C}$ is similar to $\mathbb{Z}[\sqrt{2}]$, i.e. $\mathbb{Z}[i] = \{a+bi \mid a,b \in \mathbb{Z}\}$. Are they isomorphic?

(*) A map $\varphi: (R_1,+,\cdot) \to (R_2,\oplus,\odot)$ is said to be a ring homo. if
$\varphi(a+b) = \varphi(a) \oplus \varphi(b)$
$\varphi(a \cdot b) = \varphi(a) \odot \varphi(b)$

$\varphi: \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[$
$\varphi(\sqrt{2}) = ?$
$\varphi(\sqrt{2})\varphi(\sqrt{2}) = \varphi(2) = 2\varphi(1) =$
$\Rightarrow \varphi(\sqrt{2}) = \sqrt{2}$ or $-\sqrt{2}$

(*) Intersection of subrings of a ring is a subring.

Pf: Let R be ring & $\{R_\alpha \mid \alpha \in \Omega\}$ be a collection of subrings of R. Ω an indexing set.
Let $R_0 = \bigcap_{\alpha \in \Omega} R_\alpha$. Then R_0 is a subring
R_0 is an additive subgroup of R.
$a,b \in R_0 \Rightarrow a,b \in R_\alpha \ \forall \alpha \in \Omega \Rightarrow ab \in R_0$
$\Rightarrow a \cdot b \in R_\alpha$ "

Polynomial ring

Let $(R,+,\cdot)$ be a (commutative) ring with unity.

The polynomial ring $R[x]$ over R consists of polynomials with coefficients in R with polynomial addition and multiplication as the binary operators.

A typical element of $R[x]$ is

$$a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + a_0$$

where a_i's are in R.

Formally $R[x] := \{ a : \mathbb{Z}_{\geq 0} \to R \mid$ for some $n \geq 0$, $a(i) = 0 \ \forall\ i > n \}$. For $a, b \in R[x]$

$$(a \oplus b)(n) = a(n) + b(n) \quad \text{for } n \in \mathbb{Z}_{\geq 0}$$

$$(a \odot b)(n) = \sum_{i=0}^{n} a(i) \cdot b(n-i) \quad \text{for } n \in \mathbb{Z}_{\geq 0}$$

Prop: $(R[x], \oplus, \odot)$ is a ring with unity. If R is commutative then so is $R[x]$.

(*) $a \in R[x]$ is denoted as

$$a(n)x^n + a(n-1)x^{n-1} + \dots + a(0)$$

where $n = \max\{ i \mid a(i) \neq 0 \}$ is called the degree of a.

Pf: $(R[x], \oplus)$ is an abelian group.

- $a \in R[x]$ then $b(n) := -a(n)$ $\forall n \in \mathbb{Z}_{\geq 0}$
  $b \in R[x]$ & $a \oplus b = 0$ ← the zero function.
  where $0(i) = 0_R$ · check 0 function is the additive identity
- $\oplus$ is assoc

- $\odot$ is assoc
- Distributive laws
- $1_{R[x]}(0) = 1$, $1_{R[x]}(n) = 0$ $\forall n \geq 1$.
  then $1_{R[x]}$ is the unity of $R[x]$

- R is comm $\Rightarrow$ $R[x]$ is comm

$a, b, c \in R[x]$, $n \geq 0$

$$((a \odot b) \odot c)(n) = \sum_{i=0}^{n} (a \odot b)(i) \cdot c(n-i)$$

$$= \sum_{i=0}^{n} \sum_{j=0}^{i} a(j) \cdot b(i-j) \cdot c(n-i)$$

$$a \odot (b \odot c)(n) = \sum_{i=0}^{n} a(i) \cdot (b \odot c)(n-i)$$

$$= \sum_{i=0}^{n} \sum_{j=0}^{n-i} a(i) \cdot b(j) \cdot c(n-i-j)$$

set $k = i + j \Rightarrow j = k - i$

$$= \sum_{i=0}^{n} \sum_{k=i}^{n} a(i)\, b(k-i)\, c(n-k)$$

$$= \sum_{0 \leq i \leq k \leq n} a(i)\, b(k-i)\, c(n-k)$$

$$= \sum_{0 \leq j \leq i \leq n} a(j)\, b(i-j)\, c(n-i)$$

(*) The map $R \xrightarrow{i} R[x]$ which sends

$a \mapsto f_a$ where f_a: $n \mapsto 0$ $n \geq 1$, $0 \mapsto a$

is an injective ring homo.

Pf: i is an injective function is clear.

Since $f_a = f_b \Rightarrow f_a(0) = f_b(0)$, i.e. $a = b$

$$i(a+b) = f_{a+b}$$

$$f_{a+b}(n) = \begin{cases} 0 = f_a(n) + f_b(n) & \text{if } n > 0 \\ a+b = f_a(0) + f_b(0) & \text{if } n = 0 \end{cases}$$

$$f_{a+b}(n) = f_a(n) + f_b(n) \quad \forall n \in \mathbb{Z}_{\geq 0}$$

$$\Rightarrow f_{a+b} = f_a \oplus f_b$$

$$i(ab) = f_{ab}$$

$$i(a)\, i(b) = f_a \odot f_b$$

$$f_a \odot f_b(n) = \sum_{i=0}^{n} f_a(i) f_b(n-i) = \begin{cases} 0 & n > 0 \\ ab & n = 0 \end{cases} = f_{ab}$$

Hence i is ring homo.

Lecture 3: More on polynomial rings and ideals

03 September 2020
14:36

(#1) R a ring with unity then $R[x]$ consisting of polynomials with coefficient in R with addition and multiplication is a ring. We will denote elements of $R[x]$ as $a_n x^n + a_{n-1}x^{n-1} + \dots + a_0$ instead of a function $a: \mathbb{Z}_{\geq 0} \to R$ with $a(i) = \begin{cases} a_i & i \leq n \\ 0 & \text{o.w.} \end{cases}$

Also $R \longrightarrow R[x]$, $a \longmapsto a$ is an injective ring homo.

So R is a subring of $R[x]$. Also if R is comm then $R[x]$ is comm ring.

Ex $\mathbb{Z}[\pi] \subseteq \mathbb{R}$ subring.

Claim: $\mathbb{Z}[x]$ the poly ring is isom to $\mathbb{Z}[\pi]$

Pf: $\varphi: \mathbb{Z}[x] \longrightarrow \mathbb{Z}[\pi]$

$a_n x^n + a_{n-1}x^{n-1} + \dots + a_0 \longmapsto a_n \pi^n + a_{n-1}\pi^{n-1} + \dots + a_0$

$\varphi(f(x)) = f(\pi)$

$\varphi(f+g) = (f+g)(\pi) = f(\pi) + g(\pi) = \varphi(f) + \varphi(g)$

$\varphi(fg) = \varphi(f)\varphi(g)$ (!!!) $\varphi(n) = n \ \forall n \in \mathbb{Z}$. So φ is a homomorphism

φ is clearly surjective.

"φ is injective" is a consequence of a deep result which says that "π is not a root of any nonzero polynomial with integer coefficient."

$\varphi(f) = \varphi(g) \Rightarrow \varphi(f-g) = 0$

$\Rightarrow (f-g)(\pi) = 0$

$\Rightarrow f - g = 0$

$\Rightarrow f = g$.

Hence φ is injective. So φ is an isom.

So now we have more ways of constructing new rings.

$(\mathbb{Z}[X])[Y]$ $(\cong \mathbb{Z}[X,Y])$

More generally, R a ring then the poly ring in n-variable $R[X_1, \dots, X_n] := (((R[X_1])[X_2])\dots)[X_n]$

$R_0 := R$, $R_{i+1} = R_i[X]$ $i \geq 0$ then

$R[X_1, \dots, X_n] := R_n$

⊛ Ideals in a ring.

⊛ R a comm ring with unity. Let $\{I_\alpha \mid \alpha \in \Omega\}$ be a collection of ideals in R. Then $I = \bigcap_{\alpha \in \Omega} I_\alpha$ is an ideal.

Pf: Same as subring

Let $a \in I$ & $r \in R$

$a \in I_\alpha \ \forall \alpha \in \Omega \Rightarrow ra \in I_\alpha \ \forall \alpha \in \Omega$

$\Rightarrow ra \in \bigcap_{\alpha \in \Omega} I_\alpha = I$

⊛ What about $I_1 \cup I_2$ if I_1, I_2 are ideals in R? Is it an ideal?

Ex In $\mathbb{Z}$ $2\mathbb{Z}$, $3\mathbb{Z}$ ideals in $\mathbb{Z}$

$2\mathbb{Z}$ = {even integers}, $3\mathbb{Z}$ = {integers which are multiple of 3}

$S = 2\mathbb{Z} \cup 3\mathbb{Z}$ $1 \notin S$ but $3, -2 \in S$

$\Rightarrow 3 + (-2) \notin S$

(*) Let I_1, I_2 be ideals of a ring R then

$I_1 + I_2 :=$ the ideal generated by I_1 and I_2

i.e. the smallest ideal containing I_1 & I_2

(*) Let $S \subseteq R$ be a subset of a ring R (comm ring with unity) then $\langle S \rangle$ denotes the ideal generated by S, i.e. smallest ideal containing S

$$\langle S \rangle := \bigcap \{ I \mid I \text{ ideal of } R, S \subseteq I \}$$

Prop: Let $S \subseteq R$ be a subset of a ring R then

$$\langle S \rangle = \left\{ r_1 a_1 + r_2 a_2 + \cdots + r_n a_n \;\middle|\; \begin{array}{l} n \geq 1, a_1, \ldots, a_n \in S \\ \& \; r_1, \ldots, r_n \in R \end{array} \right\}$$

Pf: Let $T = RHS$

Clearly $T \subseteq \langle S \rangle$ ($\because r_i a_i \in \langle S \rangle$ & $\sum_{i=1}^{n} r_i a_i \in \langle S \rangle$)

$S \subseteq T$. So enough to show T is an ideal.

T is clearly closed under addition

Let $\sum_{i=1}^{n} r_i a_i \in T$ & $r \in R$ then

$$r\left(\sum_{i=1}^{n} r_i a_i\right) = \sum_{i=1}^{n} (r r_i) a_i \in T$$

($r r_i$ are in R; these are in S)

So T is an ideal. Hence $\langle S \rangle \subseteq T$. ∎

(*) Let I_1, I_2 be ideals of R. Then

$$I_1 + I_2 = \{ a + b \mid a \in I_1 \;\&\; b \in I_2 \}$$

$$= I$$

Pf: RHS $\subseteq I_1 + I_2$ i.e. $T \subseteq I_1 + I_2$

Note $T \supseteq I_1 \cup I_2$ ✓

Let $a+b \in T$ & $a'+b' \in T$

i.e. $a, a' \in I_1$ & $b, b' \in I_2$

$a+b+a'+b' = \underbrace{(a+a')}_{\uparrow I_1} + \underbrace{(b+b')}_{\uparrow I_2} \in T$

Let $r \in R$, $a+b \in T$ $a \in I_1$ & $b \in I_2$

$\Rightarrow r(a+b) = \underbrace{ra}_{\uparrow I_1} + \underbrace{rb}_{\uparrow I_2} \in T$

Hence T is an ideal $\Rightarrow T = I_1 + I_2$

Ex: In $\mathbb{Z}$, Compute $2\mathbb{Z} + 3\mathbb{Z}$? $\mathbb{Z}$

In $\mathbb{Z}[x]$ " $2\mathbb{Z}[x] + x\mathbb{Z}[x]$?

$= \{ f(x) \in \mathbb{Z}[x] \mid f(0) \text{ is even} \} = T$

$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in T$

a_0 is even

$f(x) = x(a_n x^{n-1} + a_{n-1} x^{n-2} + \cdots + a_1) + a_0$

$f(x) \in 2\mathbb{Z}[x] + x\mathbb{Z}[x] \Rightarrow T \subseteq 2\mathbb{Z}[x] + x\mathbb{Z}[x]$

$f(x) = 2g(x) + xh(x)$ for some $g(x), h(x) \in \mathbb{Z}[x]$

$= 2b_0 + xh_1(x)$ $\quad g(x) = b_m x^m + \cdots + b_1 x + b_0$

$\Rightarrow f(x) \in T$. where $h_1(x) = h(x) + b_m x^{m-1} + \cdots + b_2 x + b_1 \in \mathbb{Z}[x]$

$\Rightarrow 2\mathbb{Z}[x] + x\mathbb{Z}[x] \subseteq T$. Hence equality

Lecture 4: Group ring, nilpotents, zero divisors

06 September 2020
15:51

(*) Let $R=\mathbb{Z}[X]$, $I_1=2\mathbb{Z}[X]$, $I_2=X\mathbb{Z}[X]$

$I_1+I_2=\{f(X)\in R \mid f(0) \text{ is even}\} \doteq T$

$f(X)=X^3+3X^2+2$

$I_1 \ni (2)+(X^3+3X^2) \in I_2$

$I_1 \ni (2+4X)+(X^3+3X^2-4X) \in I_2$.

$T \subseteq I_1+I_2$ ✓

$f \in I_1+I_2$ then $f=2g+Xh$ for some $g,h\in R$

Let $g=b_m X^m+b_{m-1}X^{m-1}+\dots+b_1X+b_0$, $b_i\in\mathbb{Z}$

then $f=2b_0+Xh_1$ for some $h_1\in R$

"or simply $f(0)=2g(0)$ is even"

(*) Def^n Group ring: Let $(R,+,\cdot)$ be a ring (comm) with unity and G be a group.

The group ring $R[G]=\{r_1g_1+r_2g_2+\dots+r_ng_n \mid r_i\in R \,\&\, g_i\in G, n\geq 1\}$ (formal sum)

More precisely, $R[G]=\{f:G\to R \mid f(g)=0 \text{ for all but finitely many } g\in G\}$

$f \leftrightarrow \sum_{g\in G} f(g)g$

Given $a,b\in R[G]$, $(a\oplus b)(g)=a(g)+b(g)$

$(a\circ b)(g)=\sum_{h\in G} a(h)b(h^{-1}g)\in R$

Explicitly $(r_1g_1+r_2g_2+r_3g_3)\cdot(s_1h_1+s_2h_2)=r_1s_1g_1h_1+r_1s_2g_1h_2+r_2s_1g_2h_1+r_2s_2g_2h_2+r_3s_1g_3h_1+r_3s_2g_3h_2$ then combine same terms

$g,g'\in G$, $1g,1g'\in R[G]$, $1gg'\in R[G]$

Check $(R[G],\oplus,\circ)$ is a ring with unity. (Exc.)

$0_{R[G]}$ is the zero function.

$1_{R[G]} = ?\ 1_e$ where $e\in G$ is identity.

$1_{R[G]}$ is the multiplicative identity of $R[G]$.

$(a\cdot 1_{R[G]})(g)=\sum_{h\in G} a(h)1(h^{-1}g) = a(g)1(g^{-1}g)+0 = a(g)$

$\Rightarrow 1_{R[G]}$ is the unity of $R[G]$.

Example: $R = \mathbb{Z}$, 1) $G = \{e\}$ then $R[G] \cong R$

2) $G = \{e, g, g^2\}$ a group of order 3.

$\mathbb{Z}[G] = \{ae + bg + cg^2 \mid a, b, c \in \mathbb{Z}\} \not\cong \mathbb{Z}^3$ $(\pm 1, \pm 1, \pm 1)$

$1 \cdot g \in (\mathbb{Z}[G])^\times$ $\because (1 \cdot g)^3 = 1 \cdot e$

3) $G = S_3 = \{e, (1\,2\,3), (1\,2), (3\,2\,1), (1\,3), (2\,3)\}$

$(1\,2\,3) = \sigma$, $(1\,2) = \tau$, $(3\,2\,1) = \sigma^2$, $(1\,3) = \sigma\tau$, $(2\,3) = \tau\sigma$

?

$$\mathbb{Z}[G] \cong \frac{\mathbb{Z}[x]}{(x^3 - 1)}$$

$\mathbb{Z}[S_3]$ is not commutative

Def^n: Let R be a ring with unity.
An element $a \in R$ is said to be a zero divisor if $\exists\, b \in R$, $b \neq 0$ s.t. $ab = 0$.
An element $c \in R$ is called nilpotent if $\exists\, n \geq 1$, $n \in \mathbb{N}$ s.t. $c^n = 0$.

Example 1) $R = \mathbb{Z}$, zero divisor: 0
nilpotent: 0

2) $\mathbb{Z}/12\mathbb{Z}$, zero divisor: $2, 4, 6, 3, 9, 8, 10, 0$
nilpotent: $0, 6$

3) $\mathbb{Z}[G]$, $G = \{e, g, g^2\}$
zero divisor: 0, $(e-g)(e+g+g^2)$
$= e+g+g^2-g-g^2-g^3$
$= 0$

4) $M_{n\times n}(\mathbb{R})$, zero divisor: Any singular matrix A

$$A \cdot \operatorname{adj}(A) = \det(A)\, I = 0$$

$$A : \mathbb{R}^n \xrightarrow{A\cdot} \mathbb{R}^n$$

$$0 \neq v \in \ker(A) = \operatorname{Null}(A)$$

$$B = [v \mid 0 \mid 0 \mid \cdots \mid 0] \neq 0$$

$$AB = 0$$

(*) If $a \in R$ is not a zero divisor then it is called a non zero divisor in R.

(*) Let R be a nonzero ring with unity. Then units are nonzero divisors

Pf: Let $u \in R$ be a unit. If

$$ub = 0 \text{ in } R$$

$$\Rightarrow u^{-1}ub = u^{-1}0$$

$$\Rightarrow b = 0$$

□

(*) Nilpotents are zero divisors.

Lecture 5: Reduced ring, integral domains; quotient rings.

09 September 2020
12:22

Recall: $a \in R$ is a zero divisor if $ab = 0$ for some $b \in R$, $b \neq 0$.

$a \in R$ is nilpotent if $a^n = 0$ for some $n \geq 1$.

Def^n: Let R be a nonzero comm ring with unity. It is said to be **reduced** if it does not contain nonzero nilpotents.

Def^n: A ring R is said to be an **integral domain** if it is a nonzero comm ring with unity and it does not contain any nonzero zero divisors, i.e. every nonzero element of R is a nonzerodivisor.

(*) Let R be a comm ring with unity, $a \in R$ be a nonzero divisor then

$ab = ac \Rightarrow b = c$ (cancellation property holds)

In particular if R is an integral domain then

$ab = ac \Rightarrow a = 0$ or $b = c$.

Pf: $ab = ac \Rightarrow a(b-c) = 0$

$\Rightarrow (b-c) = 0$ ($\because a$ is a nonzerodivisor)

$\Rightarrow b = c$

If R is an int domain

$ab = ac$ & $a \neq 0 \Rightarrow b = c$. ▨

Examples: 1) $\mathbb{Z}$ ← Integral domain

2) $\mathbb{Z}/n\mathbb{Z}$ ← • For n prime $\mathbb{Z}/n$ is an int. domain

• n not a prime then $\mathbb{Z}/n\mathbb{Z}$ is not an int domain.

• (Exc) $\mathbb{Z}/n\mathbb{Z}$ is reduced iff $p^2 \nmid n$ for any prime p.

3) $\mathbb{Z}[X]$ ← Integral domains.

4) $\mathbb{Q}[X]$ ↙

5) valuation ring ← Int domain

6) $\mathbb{Z}^2$ ← $(1,0)$ is a zerodivisor ($\because (1,0)(0,1) = (0,0)$)

$(a,b)^n = (a^n, b^n) \Rightarrow \{(a,b) \neq 0 \Rightarrow (a,b)^n \neq 0\}$

7) $\mathcal{C}([0,1])$ ← $\mathbb{R}$-valued cont. functions on $[0,1]$.

(*) Integral domains are reduced rings.

(*) R an int domain and $R_1 \subseteq R$ subring. Then R_1 is an int domain.

• Let $f \in \mathcal{C}([0,1])$ $\quad f^n \equiv 0$

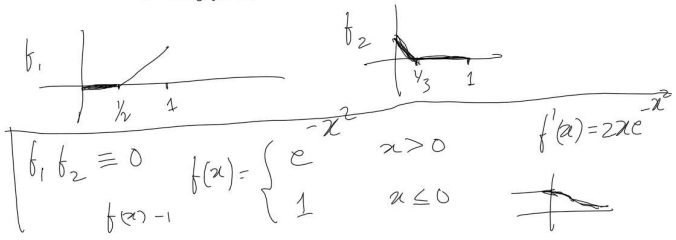
$\Rightarrow (f(x))^n = 0 \quad \forall x$

$\Rightarrow f(x) = 0 \quad \forall x$

$\Rightarrow f \equiv 0$

$\Rightarrow \mathcal{C}([0,1])$ is reduced.

•



Def/Prop: Let R be a comm ring with unity and I be an ideal of R. Then R/I with usual addition $(a+I)\oplus(b+I) = (a+b)+I$ and the multiplication given by

$$(a+I)\odot(b+I) := (ab+I)$$

makes $(R/I, \oplus, \odot)$ into a ring. Moreover the map $q: R \longrightarrow R/I$, $a \longmapsto a+I$ is a surjective ring homomorphism.

The ring R/I is called the quotient of R by the ideal I and $q: R \to R/I$ is called the quotient map.

Pf:

Claim: $(a+I)\odot(b+I) := (ab+I)$ is well-defined.

Pf: $a+I = a'+I$ & $b+I = b'+I$

$\Rightarrow a-a' \in I$ & $b-b' \in I$

$(a-a')b + a'(b-b') \in I$

$\Rightarrow ab - a'b + a'b - a'b' \in I$

$\Rightarrow ab - a'b' \in I$

$\Rightarrow ab + I = a'b' + I$

Assoc (Easy exc.)

Distributive law: $(a+I)\odot(b+I \oplus c+I)$

$= (a+I)\odot((b+c)+I)$

$= a(b+c)+I$

$= (ab+ac)+I$ (by Dist axiom in R)

$= (ab+I)\oplus(ac+I)$

$= [(a+I)\odot(b+I)]\oplus[(a+I)\odot(c+I)]$

Check $1\oplus I$ is the multiplicative identity.

Ill'y check other axioms.

$q: R \longrightarrow R/I$, $a \longmapsto a+I$ ($= \bar{a}$ notation!)

q is a group homo (Group theory)

$q(ab) = ab+I = (a+I)\odot(b+I) = q(a)\odot q(b)$ ∎

Example 1) $\mathbb{Z} \xrightarrow{n\mapsto[n]} \mathbb{Z}/n\mathbb{Z}$ ← ideal is $R=\mathbb{Z}$, $I=n\mathbb{Z}$

2) $q: \mathbb{Q}[x] \longrightarrow \dfrac{\mathbb{Q}[x]}{(x^2-2)\mathbb{Q}[x]} \cong \mathbb{Q}[\sqrt{2}] \subseteq \mathbb{R}$ ← int domain

3) $q: \mathbb{R}[x] \longrightarrow \dfrac{\mathbb{R}[x]}{(x^2-2)\mathbb{R}[x]} \cong \dfrac{\mathbb{R}[x]}{(x-\sqrt{2})(x+\sqrt{2})}$

4) $q: \mathbb{Z}[x] \longrightarrow \dfrac{\mathbb{Z}[x]}{(x^2-2)\mathbb{Z}[x]} \cong \mathbb{Z}[\sqrt{2}]$

5) $\dfrac{\mathbb{Z}[x]}{(2, x^2-2)\mathbb{Z}[x]} \cong \dfrac{\mathbb{Z}/2\mathbb{Z}[x]}{\langle x^2 \rangle}$ Next class

6) $\dfrac{\mathbb{Z}[x]}{(5, x^2-2)\mathbb{Z}[x]} \cong \dfrac{\mathbb{Z}/5\mathbb{Z}[x]}{(x^2-2)}$ ← Int domain

$\varphi: \mathbb{Q}[x] \to \mathbb{Q}[\sqrt{2}]$, $f(x) \mapsto f(\sqrt{2})$

φ is a ring homo (Check!)

$\ker(\varphi) \ni x^2-2$ (= $g(x)$)

$g(\sqrt{2}) = 0$

$(x^2-2)\mathbb{Q}[x] \subseteq \ker(\varphi)$

Let $f(x) \in \mathbb{Q}[x]$ & $f(x) \in \ker(\varphi)$

$f(x) = g(x)q(x) + r(x)$ ← Remainder thm

$\deg(r(x)) \le 1$

$0 = f(\sqrt{2}) \Rightarrow r(\sqrt{2}) = 0 \Rightarrow r(x) = 0$ $\Rightarrow f(x) \in (x^2-2)\mathbb{Q}[x]$

$\Rightarrow \ker(\varphi) = (x^2-2)\mathbb{Q}[x]$

$\overset{1^{st}\text{ isom}}{\Rightarrow} \dfrac{\mathbb{Q}[x]}{(x^2-2)\mathbb{Q}[x]} \cong \mathbb{Q}[\sqrt{2}]$

(*) Every ideal is a kernel of a ring homo. This follows from the fact that $\ker(q) = I$.

Pf: Let $a \in I$

$q(a) = a + I = 0 + I$

$\Rightarrow a \in \ker(q)$

$a \in \ker(q) \Rightarrow q(a) = 0 + I$

$\Rightarrow a + I = 0 + I$

$\Rightarrow a \in I$.

(*) $\dfrac{\mathbb{R}[x]}{(x^2-2)\mathbb{R}[x]}$ is not an integral domain ($(x^2-2)\mathbb{R}[x] \in I$ say)

$x - \sqrt{2} \in \mathbb{R}[x]$

$q(x-\sqrt{2}) = \overline{x-\sqrt{2}} = (x-\sqrt{2}) + I \neq 0 + I$

$q(x+\sqrt{2}) = \overline{x+\sqrt{2}} = (x+\sqrt{2}) + I \neq 0 + I$

$\big((x-\sqrt{2}) + I\big) \cdot \big((x+\sqrt{2}) + I\big) = (x-\sqrt{2})(x+\sqrt{2}) + I$

$= x^2 - 2 + I = 0 + I$

Lecture 6: Isomorphism theorems

10 September 2020
15:27

- R an integral domain, $S \subseteq R$ subring (containing 1_R) then S is an int domain.
- R/I has a ring structure. $q: R \to R/I$ the quot. ring homo. **surjective.**
- In R/I, $a+I = q(a) = \bar{a}$, hence $\overline{a+b} = \bar{a}+\bar{b}$ & $\overline{ab} = \bar{a}\bar{b}$

Prop: Let R be an integral domain then $R[X]$ is an integral domain.
Hence $R[x_1,..,x_n]$ is also an " " .

Pf: Let $f(x), g(x) \in R[X]$ be nonzero elements then

$f(x) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_0$ for some $a_i \in R$, $a_n \neq 0$

$g(x) = b_m X^m + b_{m-1} X^{m-1} + \dots + b_0$ for some $b_i \in R$, $b_m \neq 0$

Then $f(x)g(x) = a_n b_m X^{n+m} + \dots + a_0 b_0$

R int domain $\Rightarrow a_n b_m \neq 0 \Rightarrow f(x)g(x) \neq 0$. ∎

(*) $R[X]$ int domain $\Rightarrow R$ is an int domain.

(*) Ideals in R/I.

Eg: $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $a\mathbb{Z}/n\mathbb{Z}$ where $a|n$
$\{b\mathbb{Z} \mid b|n\}$ ← ideals of $\mathbb{Z}$ containing $n\mathbb{Z}$

Prop: Ideals of R/I are in bijection with ideals of R containing I.
The bijection is given by: $J \subseteq R$ ideal containing I then
$q(J) = J/I \subseteq R/I$ is an ideal of R/I. Here $q: R \to R/I$ is the quotient map.
$W \subseteq R/I$ be an ideal then $q^{-1}(W)$ is an ideal of R containing I.

Pf: J/I is closed under addition ✓
Let $r+I \in R/I$ & $a+I \in J/I$ then $a \in J$
$\Rightarrow ra \in J \Rightarrow ra+I \in J/I \Rightarrow (r+I)(a+I) \in J/I$
Hence J/I is an ideal of R/I.
Also $q^{-1}(W)$ is an ideal of R for W an ideal of R/I and $I \subseteq q^{-1}(W)$ ✓ clear ($I = q^{-1}(0)$)

Lemma: $\varphi: A \to B$ be a ring homo of comm rings with unity and $J \subseteq B$ be an ideal of B then $\varphi^{-1}(J)$ is an ideal of A.

Pf: $a_1, a_2 \in \varphi^{-1}(J) \Rightarrow \varphi(a_1), \varphi(a_2) \in J \Rightarrow \varphi(a_1+a_2) \in J$
$\Rightarrow a_1 + a_2 \in \varphi^{-1}(J)$.
$r \in A$ & $a \in \varphi^{-1}(J) \Rightarrow \varphi(a) \in J \Rightarrow \varphi(r)\varphi(a) \in J$ ($\varphi(r) \in B$, J is an ideal of B)
φ is a ring homo $\Rightarrow \varphi(ra) \in J \Rightarrow ra \in \varphi^{-1}(J) \Rightarrow \varphi^{-1}(J)$ is an ideal of A.

- $I \subseteq J \subseteq R$ ideal then $q^{-1}(J/I) = J$ ($a \in q^{-1}(J/I) \Leftrightarrow a+I \in J/I \Leftrightarrow a \in J$)
- $W \subseteq R/I$ be an ideal of R/I then $q^{-1}(W)/I = W$
  $a+I \in W \Leftrightarrow a \in q^{-1}(W) \Leftrightarrow a+I \in q^{-1}(W)/I$

∎

(R) $\varphi: A \to B$ ring homo, $\psi: B \to C$ " " then $\psi \circ \varphi: A \to C$ is a ring homo.

$\psi \circ \varphi(a_1 a_2) = \psi(\varphi(a_1)\varphi(a_2)) = \psi(\varphi(a_1))\,\psi(\varphi(a_2))$

Isomorphism theorems

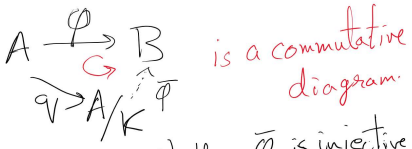
First isom thm: Let $\varphi: A \to B$ be a surjective ring homo. Then the induced map

$$\bar{\varphi}: A/\ker\varphi \longrightarrow B \quad \text{is an isomorphism.}$$
$$\bar{a} \longmapsto \varphi(a)$$

($\bar{a} = a + \ker\varphi$)

Prop: Let $\varphi: A \to B$ be a ring homo. (be an A-ideal) and $K \subseteq \ker(\varphi)$. Then there exist a ring homo

$$\bar{\varphi}: A/K \longrightarrow B \quad \text{s.t. } \bar{\varphi} \circ q = \varphi$$



is a commutative diagram.

In particular, if $K = \ker(\varphi)$ then $\bar{\varphi}$ is injective

Pf: $\bar{\varphi}: A/K \longrightarrow B$ is well-defined
$\bar{a} \longmapsto \varphi(a)$

($\bar{a} = a + K$)

Let $\bar{a} = \bar{b}$ for $a, b \in A \Rightarrow a - b \in K \subseteq \ker\varphi$

$\Rightarrow \varphi(a-b) = 0$ in B

$\Rightarrow \varphi(a) = \varphi(b)$ in B. Hence $\bar{\varphi}$ is well-defined

$\bar{\varphi}$ is a ring homo:

$\bar{\varphi}(\bar{a}+\bar{b}) = \bar{\varphi}(\overline{a+b}) = \varphi(a+b) = \varphi(a)+\varphi(b)$ (φ is a ring homo)

$\bar{\varphi}(\bar{a}) + \bar{\varphi}(\bar{b}) = \varphi(a) + \varphi(b)$

Ill'y $\bar{\varphi}(\bar{a}\bar{b}) = \bar{\varphi}(\overline{ab}) = \varphi(ab) = \varphi(a)\varphi(b) = \bar{\varphi}(\bar{a})\bar{\varphi}(\bar{b})$

For $a \in A$

$\bar{\varphi} \circ q(a) = \bar{\varphi}(\bar{a}) = \varphi(a)$ ($q: A \to A/K$)

$\Rightarrow \bar{\varphi} \circ q = \varphi$

Now if $K = \ker(\varphi)$ and $\bar{a} \in A/K$ be s.t. $\bar{\varphi}(\bar{a}) = 0$ in B then

$\varphi(a) = 0$. Hence $a \in K = \ker(\varphi)$

$\Rightarrow \bar{a} = 0$ in A/K.

Hence $\ker(\bar{\varphi}) = 0$; i.e. $\bar{\varphi}$ is injective. ∎

Pf of 1st isom thm:

By prop. $\bar{\varphi} : A/\ker\varphi \longrightarrow B$ is an injective ring homo. But φ is surjective & $\bar{\varphi} \circ q = \varphi \Rightarrow \bar{\varphi}$ is surjective

Hence $\bar{\varphi}$ is an isomorphism.

Second isom thm: Let R be a comm ring with unity.

Let $S \subseteq R$ be a subring & I be an R-ideal. Then

$S+I$ is subring of R, $S \cap I$ is an S-ideal and

$$S+I/I \cong S/S\cap I \quad \text{as rings.}$$

Pf: $\alpha, \alpha' \in S+I$

$\Rightarrow \alpha = r+a$ for some $r \in S$ & $a \in I$

$\alpha' = r'+a'$ " " $r' \in S$ & $a' \in I$

$\Rightarrow \alpha+\alpha' = \underbrace{(r+r')}_{\in S} + \underbrace{(a+a')}_{\in I} \in S+I$

& $\alpha \cdot \alpha' = (r+a)(r'+a') = \underbrace{rr'}_{\in S} + \underbrace{a(r'+a') + ra'}_{\in I} \in S+I$

$S \cap I = i^{-1}(I)$ where $i : S \hookrightarrow R$ is the inclusion map.

Hence $S \cap I$ is an S-ideal. (By Lemma)

Let $S \xhookrightarrow{i} S+I \xrightarrow{q} S+I/I$

$\varphi = q \circ i$. Then φ is a ring homo. $\alpha \in S+I/I \Rightarrow$

$(r+a)+I = \alpha = \overline{r+a}$ for some $r \in S$ & $a \in I$

$\Rightarrow \alpha = \bar{r}$ $(\because r+a-r = a \in I)$

$\Rightarrow \alpha = \varphi(r)$

Hence φ is surj

Claim: $\ker(\varphi) = S \cap I$

$x \in \ker(\varphi) \Rightarrow \varphi(x) = 0$ & $x \in S$

$\Rightarrow x + I = 0$ in $S+I/I$ & $x \in S$

$\Rightarrow x \in I \cap S$.

$x \in S \cap I \Rightarrow \varphi(x) = 0$ $(\because I = \ker(\varphi))$

Hence by 1st isom thm

$S/S \cap I \cong S+I/I$ ∎

Ex $\dfrac{\mathbb{Z}[x]}{(2, x^2-2)\mathbb{Z}[x]} \cong \dfrac{\mathbb{Z}/2\mathbb{Z}[Y]}{(Y^2)}$

$I = (2, x^2-2) \subseteq \mathbb{Z}[x] = R$

$J = (x^2-2) \subseteq I$

$K = (2) \subseteq I$

R/K

$R/I \cong \dfrac{R/K}{I/K}$

$\dfrac{\mathbb{Z}[x]}{(2, x^2-2)} \cong \dfrac{\mathbb{Z}[x]/(2)}{I/K}$

$\mathbb{Z}[x] \xrightarrow{\varphi} \mathbb{Z}/2\mathbb{Z}[x]$

$f \longmapsto f \pmod 2$

$\ker(\varphi) = (2) = 2\mathbb{Z}[x]$

$\cong \dfrac{\mathbb{Z}/2\mathbb{Z}[x]}{(x^2-\bar{2})} \cong \dfrac{\mathbb{Z}/2\mathbb{Z}[x]}{(x^2)}$

Lecture 7:Third Isomorphism theorem, prime and maximal ideals.

First isom thm: $\varphi : A \to B$ be a surj ring homo then the induced map $A/\ker(\varphi) \longrightarrow B$ is an isomorphism.

second isom thm: R a comm ring with unity. $S \subseteq R$ subring I an R-ideal. Then

$$S/S\cap I \cong S+I/I$$

$$s + S\cap I \longmapsto s + I \quad \text{for } s \in S$$

Third isom thm: Let R be a comm ring with unity. $I \subseteq J$ be ideals of R. Then

$$R/J \cong \frac{R/I}{J/I}$$

$(R/I, +)$ $(R, +)$ $(R$

Pf: Note that J/I is an ideal of R/I.

Let $\varphi : R/I \longrightarrow R/J$ be the ring homo

$$a+I \longmapsto a+J$$

Note φ is well-defined. $(a+J = a'+I \Rightarrow a-a' \in I \subseteq J \Rightarrow a+J = a'+J$

$$\varphi((a+I)\cdot(a'+I)) = \varphi(aa'+I) = aa'+J = (a+J)\cdot(a'+J) = \varphi(a+I)\,\varphi(a'+I)$$

(R/I on the left, R/J on the right)

φ is surjective ✓

Claim: $\ker(\varphi) = J/I$

$$a+I \in \ker\varphi \iff \varphi(a+I) = 0 \text{ in } R/J$$
$$\iff a+J = 0 \text{ in } R/J$$
$$\iff a \in J \iff a+I \in J/I$$

Hence by 1st isom thm

$$R/I \,/\, J/I \cong R/J$$

∎

Notation: R a ring $a, b \in R$ then the ideal $(a,b)R$ is also denoted by (a,b) if it clear from the context to which ring this ideal belongs.

Example: $\dfrac{\mathbb{Z}[x]}{(n)} \cong \mathbb{Z}/(n)[x]$

((n) ↖ $n\mathbb{Z}[x]$; (n) ↖ $n\mathbb{Z}$)

$\varphi : \mathbb{Z}[x] \longrightarrow \mathbb{Z}/n\mathbb{Z}[x]$

$f \longmapsto f \pmod n$

" $a_m x^m + a_{m-1}x^{m-1} + \dots + a_0 \longmapsto [a_m]_n x^m + [a_{m-1}]_n x^{m-1} + \dots + [a_0]_n$

$\varphi(f+g) = (f+g) \pmod n = f \pmod n + g \pmod n$

$= \varphi(f) + \varphi(g)$ | φ is a ring homo & surj is clear.

III by $\varphi(fg) = \varphi(f)\varphi(g)$ |

$\ker \varphi = \{ f \in \mathbb{Z}[x] \mid f \pmod n = 0 \text{ in } \mathbb{Z}/n\mathbb{Z}[x] \}$

$= \{ f \in \mathbb{Z}[x] \mid n \mid f(x) \} = n\mathbb{Z}[x]$

So $\dfrac{\mathbb{Z}[x]}{n\mathbb{Z}[x]} \cong \mathbb{Z}/n\mathbb{Z}[x]$

Examples: $\dfrac{\mathbb{Z}[x]}{(5, x^2-2)} \cong \dfrac{\mathbb{Z}/5\mathbb{Z}[x]}{(x^2 - [2]_5)}$

$= \mathbb{Z}[x]$

$I = 5\mathbb{Z}[x]$, $J = (5, x^2-2)\mathbb{Z}[x]$

$R/J \cong R/I \,/\, J/I$

" $\dfrac{\mathbb{Z}[x]}{(5, x^2-2)}$ " $\dfrac{\mathbb{Z}[x]}{5\mathbb{Z}[x]} \Big/ \dfrac{(5, x^2-2)\mathbb{Z}[x]}{5\mathbb{Z}[x]}$

$\mathbb{Z}/5\mathbb{Z}[x] \Big/ (x^2 - [2]_5)\,\mathbb{Z}/5\mathbb{Z}[x]$ "

$\dfrac{\mathbb{Z}/5\mathbb{Z}[x]}{(x^2 - [2]_5)}$

(*) $\dfrac{\mathbb{Z}[x]}{(2, x^2-2)} \cong \dfrac{\mathbb{Z}/2\mathbb{Z}[x]}{(x^2)}$ ↖ not reduced

Def^n: Prime ideals: Let R be a comm ring with unity. An ideal P of R is said to be a prime ideal if $P \subsetneq R$ and $ab \in P$ for some $a, b \in R \Rightarrow a \in P$ or $b \in P$.

Example: In $\mathbb{Z}$, $n\mathbb{Z}$ is prime ideal iff n is a prime number or $n = 0$.

Pf: (0) is prime ideal ($\because ab = 0 \Rightarrow a = 0$ or $b = 0$; $\mathbb{Z}$ is an int domain)

$n \neq 0$: n a prime. Let $ab \in n\mathbb{Z} \Leftrightarrow n \mid ab$

$\xrightarrow{n \text{ a prime}}$ $n \mid a$ or $n \mid b \Leftrightarrow a \in n\mathbb{Z}$ or $b \in n\mathbb{Z}$ $\Rightarrow n\mathbb{Z}$ is a prime ideal

$n\mathbb{Z}$ a prime ideal. Let $n \mid ab \Leftrightarrow ab \in n\mathbb{Z}$

$\Rightarrow a \in n\mathbb{Z}$ or $b \in n\mathbb{Z} \Leftrightarrow n \mid a$ or $n \mid b$ $\Rightarrow n$ is prime ∎

⊛ R is an int domain $\Leftrightarrow (0)$ is a prime ideal of R.

Prop: Let R be a comm ring with unity and $I \subseteq R$ be an ideal. The ring R/I is an integral domain iff I is a prime ideal.

Pf: Note that $R/I = 0$ iff $I = R$.

R/I is an int domain $\Leftrightarrow I \neq R$ & for $\alpha, \beta \in R/I$

$\alpha\beta = 0 \Rightarrow \alpha = 0$ or $\beta = 0$

$\Updownarrow$

$I \subsetneq R$ & for $a, b \in R$ $\quad I \neq R$ & $\alpha = \bar{a}$ & $\beta = \bar{b}$

$ab \in I \Rightarrow a \in I$ or $b \in I$ $\Leftrightarrow$ for some $a, b \in R$

$\Updownarrow$ $\quad \bar{a}\bar{b} = \bar{a}\bar{b} = 0 \Rightarrow \bar{a} = 0$ or $\bar{b} = 0$ in R/I

I is a prime ideal of R.

Ex 1) $p\mathbb{Z}[x]$ is a prime ideal of $\mathbb{Z}[x]$ if p is a prime. ($\because \mathbb{Z}[x]/p\mathbb{Z}[x] \cong \mathbb{Z}/p\mathbb{Z}[x]$; $\mathbb{Z}/p\mathbb{Z}$ int domain)

2) $\mathbb{Q}[x]/(x^2-2) \cong \mathbb{Q}[\sqrt{2}] \Rightarrow (x^2-2)$ in $\mathbb{Q}[x]$ is a prime ideal.

3) In $\mathbb{Z}[x]$, $(x-n)$ is a prime ideal for $n \in \mathbb{Z}$.

4) $6\mathbb{Z}$ is not a prime ideal of $\mathbb{Z}$

Def^n: Maximal ideals: Let R be comm ring with unity. An ideal m of R is called a maximal ideal if m is maximal among proper ideals of R, i.e. $m \subseteq I \subseteq R$, I an ideal then

$$I = m \text{ or } I = R.$$

Prop: Let R be a nonzero comm ring with unity then R contains a maximal ideal.

Ex: In $\mathbb{Z}$, let p be a prime number then $p\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$.

$$p\mathbb{Z} \subseteq I \subseteq \mathbb{Z}$$

$n \in I \setminus p\mathbb{Z} \Rightarrow (n, p) = 1$ ($\because$ only factors of p are 1 & p)

$\Rightarrow \exists a, b \in \mathbb{Z}$

$an + bp = 1 \in I$

$\Rightarrow I = \mathbb{Z}$

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

If n is not a prime then $n\mathbb{Z}$ is not maximal

$n = pq$ where $|p|, |q| > 1$

$n\mathbb{Z} \subseteq p\mathbb{Z} \subseteq \mathbb{Z}$; Hence $n\mathbb{Z}$ is not maximal.

Lecture 8: Maximal ideals.

16 September 2020
23:12

Let R be a comm ring with unity. Recall:

1) $I \subsetneq R$ is a prime ideal if $I \neq R$, $ab \in I \Rightarrow a \in I$ or $b \in I$.

2) $I \subsetneq R$ is a prime ideal $\Leftrightarrow$ R/I is an integral domain.

3) $m \subsetneq R$ is a maximal ideal if $\nexists$ any ideal $m \subsetneq I \subsetneq R$

Observation: $I \subseteq R$ an ideal. $I = R$ iff $1_R \in I$.

Prop: Let R be comm ring with unity and I be an R-ideal.
Then I is a maximal ideal iff R/I is a field.

Lemma: Let R be a comm ring with unity. Then R is a field iff the only ideals in R are 0 and R.

Pf: ($\Rightarrow$): Let $I \subseteq R$ be an ideal. $I \neq (0) \Rightarrow$
$\exists\, a \in I$ & $a \neq 0 \Rightarrow 1 = a^{-1}a \in I \Rightarrow I = R$.
(Since R is a field $a^{-1} \in R$)

($\Leftarrow$): Let $a \in R$ & $a \neq 0$ then $aR \neq 0 \Rightarrow$
$aR = R \Rightarrow \exists\, b \in R$ s.t. $ab = 1_R$
Hence R is a field.

Proof of the proposition: $I \subseteq R$ is maximal ideal
$\Leftrightarrow$ the only ideals in R/I are the 0 ideal & R/I.
(∵ ideals in R/I are in bijection with ideals of R containing I. and I being maximal the two such ideals are I & R whose images under $\varphi: R \to R/I$ are 0 R/I-ideal and R/I.)
$\overset{\text{Lemma}}{\Leftrightarrow}$ R/I is a field.

Cor: R a comm ring with unity & $I \subseteq R$ a maximal ideal then I is a prime ideal of R.

Pf: I is a maximal ideal of $R \underset{\text{(*) Prop}}{\Rightarrow} R/I$ is a field $\overset{\text{obvious}}{\Rightarrow} R/I$ is an int domain $\underset{(2)}{\Rightarrow} I$ is a prime ideal.

Another proof of the cor: Let $I \subseteq R$ be a maximal ideal. Then $I \neq R$. Let $ab \in I$ for $a, b \in R$.

$Ra + I$ is an R-ideal containing I.

By maximality of I, $Ra + I = I \Rightarrow a \in I$

or $Ra + I = R$

$\Downarrow$

$\exists r \in R$ & $x \in I$ s.t.

$ra + x = 1$

$\Rightarrow rab + xb = b \Rightarrow b \in I$.

($rab \in I$ $\because ab \in I$, $xb \in I$ $\because x \in I$) ∎

Converse is not true: $(0) \subseteq \mathbb{Z}$ is a prime ideal but not maximal.

Question: Is every nonzero prime ideal of a ~~ring~~ integral dom R maximal?

$\mathbb{Z}[X]$ Ex: $(2) = 2\mathbb{Z}[X]$, (X) in $\mathbb{Z}[X]$

$(2) = I$

$$\frac{\mathbb{Z}[X]}{(2)} \cong \mathbb{Z}/(2)\,[X]$$

(Last time) $\sum_{i=0}^{n} a_i X^i$, $\sum_{i=0}^{m} b_i X^i$

$I = X\mathbb{Z}[X]$, let $f(X)g(X) \in I \Rightarrow$

$f(X)g(X) = X h(X)$

$f(0)g(0) = 0 \Rightarrow f(0) = 0$ or $g(0) = 0$

$a_0 = 0$, $b_0 = 0$

$\Downarrow$

$f(X) = X\left(\sum_{i=1}^{n} a_i X^{i-1}\right) \in I$, $g(X) \in I$

$\{f \in \mathbb{Z}[X] \mid f(0) \text{ even}\} = (2, X)$

$I \subsetneq (2, X) \subsetneq \mathbb{Z}[X]$

Or check $\frac{\mathbb{Z}[X]}{(X)} \cong \mathbb{Z}$

$$\frac{\mathbb{Z}[X]}{(2, X)} \cong \mathbb{Z}/(2)$$

Thm: Every nonzero comm ring with unity R contains a maximal ideal.

Zorn's lemma: Let $(\Omega, \leq)$ be a nonempty partially ordered set. Assume that every chain in Ω has an upper bound in Ω then Ω has a maximal element.

partially ordered means $\leq$ relation is reflexive
anti-symmetric
$(a \leq b \ \& \ b \leq a \Rightarrow a = b)$
and transitive.

A chain C in Ω is a totally ordered subset
i.e. $\forall a, b \in C \quad a \leq b$ or $b \leq a$.

C has an upper bound in Ω means $\exists$ $m \in \Omega$ s.t. $\forall a \in C \quad a \leq m$.

m is a maximal element of Ω means
if $m \leq a$ for some $a \in \Omega$ then $a = m$.

Zorn's lemma is equivalent to Axiom of choice

AC: Let I be a set and $\{A_\alpha\}_{\alpha \in I}$ be a collection of set.
Then $\exists$ a set A s.t. A contains exactly one element from each A_α $\forall \alpha \in I$.

Pf of the thm: Let R be a nonzero comm ring with unity. Let $\Omega = \{I \subseteq R \mid I \text{ is a proper } R\text{-ideal}\}$.

Then $\Omega \neq \phi$. Ω is a partially ordered by inclusion. R is not the zero ring. $I \leq I'$ if $I \subseteq I'$

Let $C = \{I_\alpha\}_{\alpha \in J}$ be a chain in Ω. J is an indexing set

Let $I = \bigcup_{\alpha \in J} I_\alpha$. Claim: I is proper R-ideal.

Pf: Let $a, b \in I$ then $a \in I_{\alpha_0}$ & $b \in I_{\beta_0}$ for some $\alpha_0, \beta_0 \in J$. Since $\{I_\alpha\}_{\alpha \in J}$ is totally ordered

$I_{\alpha_0} \subseteq I_{\beta_0}$ or $I_{\beta_0} \subseteq I_{\alpha_0} \Rightarrow a, b \in I_{\beta_0}$ or I_{α_0}

$\Rightarrow a+b \in I_\alpha$ or I_β for any $r \in R$

& ra

$\Rightarrow a+b$ & $ra \in I$ " " $r \in R$

$\Rightarrow I$ is an R-ideal

If $I = R \Rightarrow 1 \in I \Rightarrow 1 \in I_\alpha$ for some $\alpha \in J$

$\Rightarrow I_\alpha = R$, which contradicts $I_\alpha \in \Omega$.

Hence the claim. i.e. $I \in \Omega$ and I is an upper bound of $\{I_\alpha\}_{\alpha \in J}$.

Hence by Zorn's lemma Ω has a maximal element say M. Then M is a maximal ideal of R by definition.

$\blacksquare$

Lecture 9: Jacobson radical, nil radical

21 September 2020
13:33

Quiz 1: Elements of quotient rings, equivalence classes, etc.

$k[X]$, k a field, $I = (X-20) = \{f(X)(X-20) \mid f(X) \in k[X]\}$

$k[X]/I$ its elements are not elements of $k[X]$

$g(X) + f(X)(X-20) \in k[X]/I$ Doesn't make sense

$g(X)+I,\ f(X)+I \subseteq k[X]/I$ $\quad f(X) \sim g(X)$ if $f(X)-g(X) \in I$

$f(X), g(X) \in k[X]$

$k[X]/I \cong k$ $\quad \varphi : k[X] \to k$, $f \mapsto f(20)$

$\ker(\varphi) = (X-20)k[X] = I$

$n \in k[X]$

$n \pmod{X-20} \in k[X]/(X-20)$

$\bar{\varphi} : k[X]/I \to k$

$k[X]/(X-20) \cong k \neq k[X]/(X)$

$R = \mathbb{Z}[X]/(X-1, X^2)$ $\quad I = (X-1, X^2) = \mathbb{Z}[X]$

$\varphi \downarrow \mathbb{Z}$

$X(X-1) - X^2 \in I$

$-X \in I \Rightarrow -X + \underbrace{X-1}_{=1} \in I$

$0_R = X^2 + (X-1, X^2) = \overline{X^2} = q(X^2)$

where $q : \mathbb{Z}[X] \to \frac{\mathbb{Z}[X]}{(X-1, X^2)}$

$\bar{X} = q(X) = X + (X-1, X^2)$

$0 = \varphi(0_R) = \varphi(\bar{X}^2) = \varphi(\bar{X}\bar{X}) = \varphi(\bar{X})\varphi(\bar{X})$

$\Rightarrow \varphi(\bar{X}) = 0$ $\quad \varphi(1_R) = 0_R$ $\quad 1_R = 1 + (X-1, X^2) = X + (X-1, X^2) = \bar{X}$

Last time: We talked about maximal ideals.

$\mathbb{Z}[X]$ (X) is prime but not maximal

(2) " " " " "

Comm ring with unity

① I, J ideals of R then $IJ = \{a_1b_1 + \dots + a_nb_n \mid a_i \in I, b_i \in J\}$ $n \geq 1$, $1 \leq i \leq n$

② $IJ \subseteq I \cap J$. Does equality hold?

Note: IJ is an ideal. $(IJ, +)$ is a group.

$r \in R$ & $x \in IJ$ then $x = a_1b_1 + \dots + a_nb_n$, $a_i \in I$ & $b_i \in J$

$\Rightarrow rx = (ra_1)b_1 + \dots + (ra_n)b_n \in IJ$

② $IJ \subseteq I \cap J$ (all $a_ib_i \in I$ & $\in J$), then $ab \in I \cap J \Rightarrow IJ \subseteq I \cap J$.

$IJ \stackrel{?}{=} I \cap J$: Eg: $I = 2\mathbb{Z}$, $J = 2\mathbb{Z}$ $\quad I \cap J = 2\mathbb{Z}$, $IJ = 4\mathbb{Z}$

$I = 4\mathbb{Z}$, $J = 6\mathbb{Z}$ $\quad I \cap J = 12\mathbb{Z}$ $\quad IJ = 24\mathbb{Z}$

Jacobson radical: Let R be a nonzero comm ring with identity. The Jacobson radical of R is defined to be intersection of all maximal ideals of R.

$$J(R) := \bigcap_{\substack{m \text{ maximal} \\ \text{ideal of } R}} m$$

Nil radical: $nil(R) := \{x \in R \mid x^n = 0\}$
$= $ set of nilpotents of R

(*)1) $nil(R)$ is an ideal of R.

$x, y \in nil(R)$ & $r \in R$
$x^n = 0$ & $y^m = 0$ for some $n, m \geq 1$
$(rx)^n = 0$
$r^n x^n$

(*)2 $nil(R) \subseteq Jac(R)$

(*)3 $x \in Jac(R) \iff 1 + ax$ is a unit for all $a \in R$

↳ $(x+y)^{n+m} = x^{n+m} + * x^{n+m-1} y + \ldots + * x^n y^m + * x^{n-1} y^n + \ldots$ (Binomial coeff)
$= 0$
$\Rightarrow x + y \in nil(R)$.

(*)2 $x \in nil(R) \Rightarrow x^n = 0 \in m$ for m any maximal ideal
$\Rightarrow x \in m$ ($\because m$ is a prime ideal, $x^n = x \cdot x^{n-1} \in m$)

(In general P a prime ideal $a_1 \cdots a_n \in P$ then $a_1 \in P$ or $a_2 \in P$ or $\ldots$ or $a_n \in P$)

$\Rightarrow x \in \bigcap_{\substack{m \text{ max ideal} \\ \text{of } R}} m \Rightarrow nil(R) \subseteq Jac(R)$

In fact, $nil(R) \subseteq \bigcap_{P \text{ prime ideals of } R} P$

⊗ $\text{nil}(R) = \bigcap_{P \text{ a prime ideals of } R} P$

Pf: $x \in \text{nil}(R) \Rightarrow x^n = 0$ for some n

$\Rightarrow x^n \in P$ for all prime ideal P.

$\Rightarrow x \in P \ \forall P$ prime ideal of R

$\Rightarrow x \in \bigcap_{P \text{ a prime ideal of } R} P$

$\text{nil}(R) \subseteq \bigcap_{P \text{ prime ideal of } R} P$

$x \in \bigcap_{P \text{ prime ideal of } R} P$. WTS $x^n = 0$ for some n.

Suppose not

Let $S = \{1, x, x^2, x^3, \dots\}$ then $0 \notin S$

$\Omega = \{ I \subseteq R \mid I \text{ ideal s.t. } I \cap S = \phi \}$

Since $0 \notin S$ we have $\Omega \neq \phi$ $(\because (0) \in \Omega)$

Ω is a partially ordered set under inclusion

Let $\mathcal{C}$ be a chain in Ω.

Claim: Let $I_{\mathcal{C}} = \bigcup_{I \in \mathcal{C}} I$. Then $I_{\mathcal{C}}$ is an ideal

Moreover $S \cap I_{\mathcal{C}} = \phi$.

$x, y \in I_{\mathcal{C}} \Rightarrow x \in I_1, y \in I_2, I_1, I_2 \in \mathcal{C}$

$\mathcal{C}$ a chain $\Rightarrow I_1 \subseteq I_2$ or $I_2 \subseteq I_1$

$\Rightarrow x + y \in I_{\mathcal{C}}$ & $rx \in I_{\mathcal{C}}$ $\forall r \in R$.

$\Rightarrow I_{\mathcal{C}}$ is an ideal.

Also $S \cap I = \phi \ \forall I \in \mathcal{C}$

$\Rightarrow S \cap (\bigcup_{I \in \mathcal{C}} I) = \phi \Rightarrow S \cap I_{\mathcal{C}} = \phi$.

Hence by Zorn's lemma Ω has a maximal element m. caution $\not\Rightarrow (\because I \in \Omega \Rightarrow I \subseteq m)$

$\Rightarrow I \in \Omega$ & $m \subseteq I \Rightarrow m = I$

Claim: m is a prime ideal of R.

Claim $\Rightarrow x \notin m$ (a prime ideal), contradicting $x \in P$ (P prime in R)

Pf of claim: Let

$ab \in m$ for $a, b \in R$. WTS $a \in m$ or $b \in m$

If $a \notin m$ & $b \notin m$ then

$aR+m \supsetneq m$ & $bR+m \supsetneq m \Rightarrow aR+m \in \Omega$ & $bR+m \in \Omega$

Hence $x^n \in aR+m$ for some n & $x^k \in bR+m$

for some k.

$\Rightarrow x^n = r_1 a + y_1$ & $x^k = r_2 b + y_2$ for some $r_1, r_2 \in R$, $y_1, y_2 \in m$

$x^{n+k} = x^n x^k = (r_1 a + y_1)(r_2 b + y_2)$

$= \underbrace{r_1 r_2 ab}_{\in m} + \underbrace{y_1(r_2 b + y_2) + r_1 a y_2}_{\in m} \in m$

Contradicting $m \cap S = \phi$.

Hence $a \in m$ or $b \in m$. Hence the claim.

∎

(#3) $x \in \mathrm{Jac}(R)$ iff $1+ax$ is unit in R $\forall a \in R$.

($\Rightarrow$): $ax \in \mathrm{Jac}(R)$

(#1) Let R be a nonzero comm ring with unity. Let $I \subsetneq R$ ideal. Then $\exists$ a maximal ideal m of R containing I.

[Follows: Let $\overline{m}$ be a maximal ideal of R/I (this exist since R/I is a nonzero)

$m = q^{-1}(\overline{m})$ where $q: R \to R/I$

then $m \supseteq I$ & m is a max ideal of R (: ideals in R/I are in bijection with ideals of R containing I)

$R/m \cong R/I \,/\, m/I$ ← field

Note $m/I = \overline{m}$]

Lecture 10: Product of rings

23 September 2020
14:37

Recall: R comm ring with unity.

$\mathrm{Jac}(R) = \bigcap_{m \text{ maximal ideals of } R} m$ (Jacobson radical)

$\mathrm{nil}(R) = \sqrt{(0)} = \{x \in R \mid x^n = 0 \text{ for } n \geq 1\}$ is an ideal. ←

(*) $\mathrm{nil}(R) = \bigcap_{P \text{ prime ideals in } R} P$ (Nil radical of R)

(*) Let R be a comm ring with unity $I \subsetneq R$ be a proper ideal (i.e. $I \neq R$). Then $\exists$ a maximal ideal m of R s.t. $I \subseteq m$.

(**) $x \in \mathrm{Jac}(R) \iff 1+ax$ is a unit in R $\forall a \in R$.

Pf: ($\Rightarrow$): $x \in \mathrm{Jac}(R)$, suppose $1+ax$ is not a unit in R for some $a \in R$. Then $I = (1+ax)R \subsetneq R$. Hence $\exists$ m maximal ideal of R containing I. In particular $1+ax \in m$. But $ax \in m$ (as $x \in m$). Hence $1 \in m$ contradicting m is a maximal ideal.

($\Leftarrow$): $1+ax$ is a unit $\forall a \in R$. Let m be a maximal ideal of R. If $x \notin m$ then $Rx + m = R \Rightarrow$ $\exists y \in m$ and $a \in R$ s.t. $-ax + y = 1 \Rightarrow 1+ax = y \in m$ contradicting $1+ax$ is a unit. Hence x belongs to every maximal ideal, i.e. $x \in \mathrm{Jac}(R)$.

Examples:

Ring R	$\mathbb{Z}$	$\mathbb{Q}$ or any field	$\mathbb{Q}[X]$	$\mathbb{Z}[X]$
$\mathrm{Jac}(R)$	0	0	0	0
$\mathrm{nil}(R)$	0	0	0	0

(*) $p\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$ if p is a prime

→ $n \in \mathbb{Z}$ $n = p_1^{a_1} \cdots p_k^{a_k}$ then $n \in p_i\mathbb{Z}$

(*) Maximal ideal of $\mathbb{Q}[x]$, (x), $(x-a)$ $a \in \mathbb{Q}$.

$f(x) \in \mathbb{Q}[x]$, if $f(x) \in \mathrm{Jac}(\mathbb{Q}[x])$

$\Rightarrow$ $f(a) = 0$ $\forall a \in \mathbb{Q} \Rightarrow f(x) = 0$

$2 \in \mathbb{Q}[x]$ then $2^{-1} = \frac{1}{2} \in \mathbb{Q}[x] \Rightarrow (2, \ldots) = \mathbb{Q}[x]$

(*) Maximal ideal of $\mathbb{Z}[x]$, $(2, X)$, $(p, X-a)$ p prime & $a \in \mathbb{Z}$

Let R be a comm ring with unity and I be a proper R-ideal, i.e. $I \subsetneq R$.

Which ideal in R corresponds to $nil(R/I)$?

i.e. $q: R \to R/I$, What is $q^{-1}(nil(R/I))$?

$\sqrt{I} := q^{-1}(nil(R/I)) = \{r \in R \mid r^n \in I \text{ for some } n \geq 1\}$

$rad(I)$

$nil(R/I) = \{r+I \in R/I \mid r^n \in I \text{ for some } n \geq 1\}$

Example) $R = \mathbb{Z}$, $I = 12\mathbb{Z}$

$\sqrt{I} = 6\mathbb{Z}$, $Jac(R/I) = ?$ $6\mathbb{Z}/12\mathbb{Z}$

$nil(\mathbb{Z}/12\mathbb{Z}) = \{\bar{0}, \bar{6}\}$ $= \{\bar{0}, \bar{6}\}$

⊛ $\sqrt{I} = \bigcap P$, P prime in R & $I \subseteq P$ Exc

⊛ What is an example of a ring R s.t. $Jac(R) \supsetneq nil(R)$? valuation rings

Def^n / Prop:

Product of rings: Let $R_1, R_2, \dots, R_n$ be comm rings with unity then $R_1 \times R_2 \times \cdots \times R_n$ with component wise addition and multiplication is also a comm ring with unity.

$(a_1, \dots, a_n), (b_1, \dots, b_n) \in R = R_1 \times \cdots \times R_n$

$\Rightarrow a_i, b_i \in R_i$

$(a_1, \dots, a_n) \cdot (b_1, \dots, b_n) := (a_1 b_1, a_2 b_2, \dots, a_n b_n)$

$(a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 + b_1, \dots, a_n + b_n)$

Check all the rings axioms for R.

$1_R = (1_{R_1}, 1_{R_2}, \dots, 1_{R_n})$ is unity of R.

Note: $p_i : R \to R_i$ is a

$(a_1, \dots, a_n) \mapsto a_i$

ring homo. (trivial)

Ideals in product of rings

⊗ Let $I \subseteq R = R_1 \times R_2 \times \cdots \times R_n$ be an ideal of R then

$$I = I_1 \times \cdots \times I_n .$$

Note: $I_1 \times I_2 \times \cdots \times I_n$ is a R-ideal if I_j is an R_j-ideal $1 \le j \le n$.

Pf: $I_j = p_j(I)$ is an ideal. $a_j, b_j \in I_j$ & $r_j \in R_j$

$\Rightarrow \exists\, a, b \in I$ s.t. $a_j = p_j(a)$ & $b_j = p_j(b)$ $\exists\, r \in R$ s.t. $p_j(r) = r_j$ ($\because p_j$ is surj)

$\Rightarrow p_j(a+b) = a_j + b_j \in I_j$ ($\because a+b \in I$)

$p_j(ra) = p_j(r)\,p_j(a) = r_j a_j \in I_j$ ($\because ra \in I$)

So I_j are ideals. Claim: $I = I_1 \times \cdots \times I_n$. ($\supseteq$: $(0,0,\ldots,a_j,0,\ldots,0) \in I$ for $a_j \in I_j$ $\forall j$)

$\exists\, a \in I$ s.t. $p_j(a) = a_j$, $a = (r_1, r_2, \ldots, r_{j-1}, a_j, r_{j+1}, \ldots, r_n)$ for some $r_i \in R_i$ $i \neq j$

(j^{th} place)

$e_j = (0,0,\ldots,0,1,0,\ldots,0) \in R$ & $e_j a = (0,0,\ldots,0,a_j,0,0,\ldots,0) \in I$

$\supseteq$: ✓

$\subseteq$: $a \in I \Rightarrow a = (a_1, \ldots, a_n)$ & $a_j \in p_j(I) = I_j$

$\Rightarrow a \in I_1 \times \cdots \times I_n$

∎

Lecture 11: Chinese remainder theorem

24 September 2020
12:36

Recall: $R_1, \dots, R_n$ comm rings with unity then $R_1 \times \cdots \times R_n$ (= R) with componentwise addition & multiplication is also a comm ring with unity. $1_R = (1_{R_1}, \dots, 1_{R_n})$

(*) Ideals in $R_1 \times \cdots \times R_n$ are of the form $I_1 \times \cdots \times I_n$ where I_j is an R_j ideal. (Note: this is not true for subgroups of a group or subspaces of a vector space)

(*) Prime ideals in $R_1 \times R_2 \times \cdots \times R_n$ ($= R$ say)

Example: In $\mathbb{Z} \times \mathbb{Z}$, give an example of a prime ideal. $\mathbb{Z} \times \{0\} \subseteq \mathbb{Z} \times \mathbb{Z}$

$a, b \in \mathbb{Z} \times \mathbb{Z}$ $\quad ab \in \mathbb{Z} \times \{0\}$

$\{0\} \times \{0\} = \{(0,0)\}$ $\quad (1,0) \cdot (0,1) = (0,0)$

(*) Let $P \subseteq R$ be a prime ideal then $P = I_1 \times I_2 \times \cdots \times I_n$ s.t. $I_j = R_j$ for all but one subscript j_0 & I_{j_0} is prime ideal of R_{j_0} and conversely.

Pf: conversely is easy to see, since if $I = R_1 \times \cdots \times R_{j_0-1} \times P_{j_0} \times R_{j_0+1} \times \cdots \times R_n$ then $R/I \cong R_{j_0}/P_{j_0}$ which is an integral domain (P_{j_0} is prime)

Hence I is a prime ideal of R.

$R \xrightarrow{p_{j_0}} R_{j_0} \xrightarrow{\alpha} R_{j_0}/P_{j_0}$, $\theta = \alpha \circ p_{j_0}$

$\ker(p_{j_0}) = R_1 \times \cdots \times R_{j_0-1} \times \{0\} \times R_{j_0+1} \times \cdots \times R_n$; $\ker(\theta) = I$

$\ker(\theta) = p_{j_0}^{-1}(\ker(\alpha)) = p_{j_0}^{-1}(P_{j_0}) = I$

($\Rightarrow$): i.e. $P \subseteq R$ prime then $P = I_1 \times \cdots \times I_n$ I_j an R_j-ideal

$$R/P = \frac{R_1 \times R_2 \times \cdots \times R_n}{I_1 \times I_2 \times \cdots \times I_n} \cong R_1/I_1 \times R_2/I_2 \times \cdots \times R_n/I_n$$

$r = (r_1, \dots, r_n) \in R$

$(r + P) \longmapsto (r_1 + I_1, r_2 + I_2, \dots, r_n + I_n)$

And $R_1/I_1 \times \cdots \times R_n/I_n$ is not an integral domain if $\exists\, 1 \le i, j \le n$ $i \ne j$ s.t. $I_i \ne R_i$ & $I_j \ne R_j$

(i.e. $\bar{e}_i = (0, 0, \dots, 0, 1, 0, \dots, 0)$ with 1 in the ith factor, $\bar{e}_j \in R_1/I_1 \times \cdots \times R_n/I_n$)

$\bar{e}_i \cdot \bar{e}_j = 0$ but $\bar{e}_i, \bar{e}_j \ne 0$

Hence $I_j = R_j$ $\forall\, 1 \le j \le n$ except one (say j_0).

Then $R/P \cong R_{j_0}/I_{j_0}$ and this is an int dom iff I_{j_0} is a prime ideal of R_{j_0}. ∎

(*) Note $R = R_1 \times \cdots \times R_n$ then e_j have the property $e_j^2 = e_j$ $\quad e_i e_j = 0$ if $i \ne j$ $\quad (1 - e_j) e_j = 0$

Idempotents: Let R be a ring an element $e \in R$ is called an idempotent if $e^2 = e$.

Eg: 0_R & 1_R are idempotents is every ring with unity.

(*) Let $e \in R$ be an idempotent then $1-e$ is also an idempotent and $R \cong eR \times (1-e)R$ (i.e. eR & $(1-e)R$ are rings & their product is isom to R)

$S \subseteq R$

$1_S = 1_R$

$eR \subseteq R$

$1_{eR} \neq 1_R$

Pf: $(1-e)^2 = 1 - e - e + e^2$

$= 1 - e \quad (\because e^2 = e)$

So $1-e$ is an idempotent.

Claim: eR is comm ring with unity

eR is an ideal in R & hence closed under addition and multiplication satisfying all the ring axioms

Also $e \in eR$ & $e \cdot x = x \quad \forall x \in eR$

$(\because x \in eR \Rightarrow x = ey$ for some $y \in R)$

$\Rightarrow ex = e^2 y = ey = x$

Hence the claim.

So $(1-e)R$ is also a comm ring with unity

$(1-e)$ as $1_{(1-e)R}$. Also note $e(1-e) = 0$

$e - e^2 = 0$

$eR \times (1-e)R \xrightarrow{\psi} R$

$(ex, (1-e)y) \longmapsto ex + (1-e)y$

$R \xrightarrow{\varphi} eR \times (1-e)R$

$x \longmapsto (ex, (1-e)x)$

$\varphi \circ \psi (ex, (1-e)y) = \varphi(ex + (1-e)y) = (ex, (1-e)y)$

$\psi \circ \varphi = id_R$ & $\varphi \circ \psi = id_{eR \times (1-e)R}$

$\varphi(x+y) = (e(x+y), (1-e)(x+y)) = (ex, (1-e)x) + (ey, (1-e)y)$

$= \varphi(x) + \varphi(y)$

Now $\varphi(xy) = (exy, (1-e)xy)$

$= (exey, (1-e)x(1-e)y)$

$= (ex, (1-e)x) \cdot (ey, (1-e)y)$

$= \varphi(x)\varphi(y)$ ∎

Chinese Remainder Theorem: (Classical version): Let $n_1, n_2, \dots, n_k$ be pairwise positive coprime integers. Let $0 \le a_i < n_i$ be integers $1 \le i \le k$ then

$\exists$ an integer a s.t.

$$a \equiv a_i \pmod{n_i} \quad \forall \ 1 \le i \le k$$

Abstract version: Let R be a comm ring with unity. Let $I_1, I_2, \dots, I_k$ be R-ideals s.t. they are pairwise comaximal (i.e. $I_j + I_{j'} = R$ for $j \neq j'$). Then the $I_1 \cap \dots \cap I_k = I_1 \cdots I_k$. Moreover the ring homo $\varphi : R \to R/I_1 \times \dots \times R/I_n$ is surj with $\ker(\varphi) = I_1 \cap \dots \cap I_k$. In part.

$$R/I_1 \cdots I_k = R/I_1 \cap \dots \cap I_k \cong R/I_1 \times \dots \times R/I_n$$

$r \mapsto (r+I_1, \dots, r+I_n)$

Pf of Abstract version $\Rightarrow$ classical version

$R = \mathbb{Z}$, $I_j = (n_j)$ n_j's pairwise coprime $\Rightarrow$ I_j's are pairwise comaximal.

$$\mathbb{Z} \to \mathbb{Z}/(n_1) \times \dots \times \mathbb{Z}/(n_k) \quad (\text{surj})$$
$$n \mapsto ([n]_{n_1}, [n]_{n_2}, \dots, [n]_{n_k})$$

(By Abstract version)

$\Rightarrow$ Classical version of CRT

Pf of Abs version of CRT: case $k=2$. So $I_1+I_2=R$.

Hence $\exists\ x_1\in I_1$ & $x_2\in I_2$ s.t. $x_1+x_2=1$

Let $x\in I_1\cap I_2$ then $x=1\cdot x=(x_1+x_2)x=x_1x+xx_2$

$x_1\in I_1$, $x\in I_1I_2$; $x_2\in I_2$, $x\in I_1I_2$

Hence $I_1\cap I_2\subseteq I_1I_2$

$\Rightarrow I_1I_2=I_1\cap I_2$ ($\because I_1I_2\subseteq I_1\cap I_2$ is always true)

$\varphi: R\to R/I_1\times R/I_2$

$r\mapsto (r+I_1,\ r+I_2)$

$(\bar a,\bar b)\in R/I_1\times R/I_2$ $a(\bar 1,\bar 0)+b(\bar 0,\bar 1)$

is surj if

$(\bar 1,\bar 0)=(1+I_1,\ I_2)$ & $(I_1,\ 1+I_2)=(\bar 0,\bar 1)$ are in the image

$\varphi(x_2)$ $\qquad$ $\varphi(x_1)$

$(x_2+I_1,\ x_2+I_2)$

$x_1+x_2+I_1$ $\qquad$ I_2

$1+I_1$

Hence φ is surjective.

Now $k\geq 3$

Claim: I_1 & $I_2\cdots I_k$ are comaximal

Claim $\Rightarrow I_1\cdot I_2\cdots I_k=I_1\cap I_2\cdots I_k$ ($k=2$ case)

$=I_1\cap I_2\cap\cdots\cap I_k$.

Pf: $I_1+I_j=R\quad\forall\ j\geq 2$

$\Rightarrow x_j+y_j=1$ for some $x_j\in I_1$ & $y_j\in I_j$ $\forall\ j\geq 2$

$(x_2+y_2)(x_3+y_3)\cdots(x_k+y_k)=1$

$\alpha + y_2y_3\cdots y_k=1$

$\alpha\in I_1$, $y_2y_3\cdots y_k\in I_2\cdots I_k$

Hence the claim.

Abstract version: Let R be a comm ring with unity. Let $I_1, I_2, \dots, I_k$ be R-ideals s.t. they are pairwise comaximal, (i.e. $I_j + I_{j'} = R$ for $j \neq j'$). Then the $I_1 \cap \dots \cap I_k = I_1 \cdots I_k$. Moreover the ring homo $\varphi : R \to R/I_1 \times \dots \times R/I_k$, $r \mapsto (r+I_1, \dots, r+I_k)$ is surj with $\ker(\varphi) = I_1 \cap \dots \cap I_k$. In fact.

$$R/I_1 \cdots I_k = R/I_1 \cap \dots \cap I_k \cong R/I_1 \times \dots \times R/I_k .$$

Pf: So far we saw: 1) $k=2$ case
2) $I_1 \cap \dots \cap I_k = I_1 \cdots I_k$
3) I_1 & $I_2 \cdots I_k$ are comaximal

$j \geq 2$: $x_j \in I_1$ & $y_j \in I_j$, $x_j + y_j = 1$

Like (3) I_j & $\prod_{\substack{r=1 \\ r \neq j}}^{k} I_r$ are comaximal.

To show φ is surjective enough to show e_j $(1 \leq j \leq k)$ are in the image of φ.

$e_j = (0, \dots, 0, \underset{\uparrow j^{th} \text{ spot}}{1}, 0, \dots, 0) \in R/I_1 \times \dots \times R/I_k$

$\exists\, x_j \in I_j$ & $y_j \in \prod_{\substack{r=1 \\ r \neq j}}^{k} I_r$ s.t. $x_j + y_j = 1$

Then $\varphi(y_j) = (y_j + I_1, \dots, y_j + I_k)$
$= (I_1, \dots, \underset{x_j + y_j}{1} + I_j, I_{j+1}, \dots, I_k)$ $(\because y_j \in I_r \ \forall r \neq j)$
$= (\bar{0}, \dots, \bar{0}, \bar{1}, \bar{0}, \dots, \bar{0}) = e_j$ (*)

Let $(\bar{a}_1, \dots, \bar{a}_k) \in R/I_1 \times \dots \times R/I_k$ $\quad (a_1 + I_1, \dots, a_k + I_k)$

Then $\varphi\left(\sum_{j=1}^{k} a_j y_j\right) = \sum_{j=1}^{k} \varphi(a_j)\varphi(y_j)$
$= \sum_{j=1}^{k} (\bar{a}_j, \bar{a}_j, \dots, \bar{a}_j)\, e_j$ (from (*))
$= \sum_{j=1}^{k} (0, \dots, 0, \underset{\uparrow j^{th} \text{ spot}}{\bar{a}_j}, 0, \dots, 0)$
$= (\bar{a}_1, \dots, \bar{a}_k)$

Note $\ker(\varphi) = I_1 \cap I_2 \cap \dots \cap I_k$.

$x \in \ker\varphi \iff x + I_j = I_j \ \forall 1 \leq j \leq k$
$\iff x \in I_j \ \forall 1 \leq j \leq k$
$\iff x \in I_1 \cap \dots \cap I_k$

Now use 1st isom thm to conclude $R/I_1 \cap \dots \cap I_k \cong R/I_1 \times \dots \times R/I_k$ ∎

Euclidean domain (ED)

Def^n: A Euclidean domain A is an integral domain R s.t. there exist a function $N: R^\times \to \mathbb{Z}_{\geq 0}$ ($R^\times = R\setminus\{0\}$) satisfying the following conditions.

For $a, b \in R^\times$ $\exists\ q, r \in R$ s.t.

$$a = bq + r \quad \text{with} \quad N(r) < N(b)$$

or $r = 0$.

N will be called a Euclidean norm.

Eg: 1) $\mathbb{Z}$, $N: \mathbb{Z}^\times \to \mathbb{Z}_{\geq 0}$, $a \mapsto |a|$

$a, b \in \mathbb{Z}^\times$, By remainder's thm $\exists\ q \in \mathbb{Z}$ & $a = bq + r$ $0 \leq r < |b|$

$r \neq 0$ $N(r) = |r| < |b| = N(b)$

2) $\mathbb{Q}[x]$ or $k[x]$, k a field.

$$N: k[x]^\times \to \mathbb{Z}_{\geq 0}, \quad f \mapsto \deg(f)$$

Remainder's thm: $f(x), g(x) \in k[x]$, by Division algo. $\exists\ q(x)$ & $r(x)$ s.t.

$$f(x) = q(x)g(x) + r(x) \quad \text{where}$$

$$\deg(r(x)) < \deg(g(x)) \text{ or } r(x) = 0$$

$\Rightarrow$ N is a euclidean norm & $k[x]$ is ED.

3) Valuation rings with valuations as Euclidean norm. (HW)

Principal ideal domain (PID)

Def^n: An integral domain R is called PID if every R-ideal is principal, i.e. every R-ideal is generated by one element.

Ex: Fields, $\mathbb{Z}$, $\mathbb{Q}[x]$, $k[x]$

(*) Let R be an int domain. An element $x \in R$ is called irreducible if x is a nonzero nonunit and if $x = yz$ for some $y, z \in R$ then either y is a unit of z is a unit.

An element $x \in R$ is called a prime element if whenever $x \mid ab \Rightarrow x \mid a$ or $x \mid b$ for $a, b \in R$.

(*) x is prime iff (x) is a prime ideal.

Pf: $(x) \neq R \iff x$ is a nonunit

$ab \in (x) \iff x \mid ab$

x is prime $\iff$ x is a nonunit & "$x \mid ab \Rightarrow x \mid a$ or $x \mid b$" for $\forall a, b \in R$

$\iff (x) \neq R$ & "$ab \in (x) \Rightarrow a \in (x)$ or $b \in (x)$ $\forall a, b \in R$"

$\iff (x)$ is a prime ideal

(*) Let R be an int domain & $x \in R$ be a prime element then x is irred.

Pf: Let $x = yz$ for some $y, z \in R$

$\Rightarrow x \mid yz \Rightarrow x \mid y$ or $x \mid z$

$x \mid y \Rightarrow \exists a \in R$ s.t. $y = ax$

$\Rightarrow x = axz$

($\because x \neq 0$, R int domain)

$\Rightarrow 1 = az \Rightarrow z$ is a unit

If y $x \mid z \Rightarrow y$ is a unit.

Hence x is irred. ∎

Example: 1) In $\mathbb{Z}$, the prime elements are precisely the prime numbers. Also {irreducibles} = {primes}

2) In $\mathbb{Q}$ (or any field) no irred or primes.

3) In $k[x]$, k a field. A poly is irreducible if it is an irreducible element of $k[x]$. Also irreducible polynomials are prime elements.

In fact we will see the following:

Thm: Let R be a PID then every irred element of R is a prime element.

Pf: Let $a \in R$ be an irred. element. Then (a) is a proper R-ideal. Let $m \subseteq R$ be a maximal ideal containing (a). Since R is a PID, $m = (b)$ for some $b \in R$.

$a \in m = (b) \Rightarrow a = bc$ for some $c \in R$

But a is irred & b is not a unit $\Rightarrow c$ is a unit $\Rightarrow b = ca \Rightarrow m = (b) = (a)$. Hence (a) is a prime ideal $\Rightarrow a$ is a prime element. ∎

Cor: (of the proof) In a PID every nonzero prime ideal is maximal ideal.

Thm: Every Euclidean domain is a PID.

Pf: Let R be a ED & let $N: R^* \longrightarrow \mathbb{Z}_{\geq 0}$ be a Euclidean norm.

Let $I \subseteq R$ be a nonzero ideal. Let $a \in I$ be such that $N(a)$ is the smallest.

Claim: $(a) = I$.

$(a) \subseteq I$. ✓

Let $b \in I$, so axiom of Euclidean norm $\exists q, r \in R$ s.t.

$b = qa + r$ with $r = 0$ or $N(r) < N(a)$ (Not possible, since $r = b - qa \in I$ $\Rightarrow N(r) \geq N(a)$)

$\Rightarrow b = qa$

$\Rightarrow b \in (a)$

Hence claim and hence every ideal in R is principal. ∎

Lecture 13: ED, PID continued.

29 September 2020
17:42

Recall: 1) An int dom R is a ED if $\exists$ a norm $N: R^\times \to \mathbb{Z}_{\geq 0}$ s.t. $\forall a, b \in R^\times$ $\exists q, r \in R$ satisfying $a = bq + r$ with $r = 0$ or $N(r) < N(b)$.

2) An ID R is a PID if every R-ideal is principal (gen by 1 element)

(✓) R ED $\Rightarrow$ R PID

(✓) x irred if x nonzero nonunit & $x = yz \Rightarrow$ y is a unit or z is a unit

(✓) x prime if " " " & $x \mid ab \Rightarrow x \mid a$ or $x \mid b$.

(✓) R an int dom. x prime $\Rightarrow$ x irred.

(✓) R PID. x irred $\iff$ x prime.

(✓) R a PID then every nonzero prime ideal is maximal.

Def^n: Let R be a comm ring with unity & $a, b \in R$ then $d \in R$ is said to be a gcd of a, b in R if $d \mid a$, $d \mid b$ and if $d' \in R$ is s.t. $d' \mid a$ & $d' \mid b \Rightarrow d' \mid d$. $d = \gcd(a, b)$ or $d = (a, b)$ (Caution: gcd is not unique!)

Eg: In $\mathbb{Z}$, $\gcd(4, 6) = 2, 1, -1, -2 \leftarrow$ gcd

Prop: Let R be a ring & $a, b \in R$ s.t. $(a, b)R$ is a principal ideal dR, i.e. $(a, b) = (d)$ then d is the $\gcd(a, b)$. Moreover, $d = ax + by$ for some $x, y \in R$.

Pf: Since $a, b \in (d)$ $d \mid a$ & $d \mid b$. Let $d' \in R$ be s.t. $d' \mid a$ & $d' \mid b \Rightarrow a, b \in (d') \Rightarrow (d) = (a, b) \subseteq (d')$

$\Rightarrow d \in (d') \Rightarrow d' \mid d$. Moreover, follows since $d \in (a, b)$.

Cor: R a PID & $a, b \in R$ then $\gcd(a, b)$ exist. In fact $\gcd(a, b)$ is the generator d of the ideal (a, b) &

$$d = ax + by \text{ for some } x, y \in R.$$

(✓) gcd may not be unique.

(✓) gcd may exist even if (a, b) is not principal

Eg: In $\mathbb{Z}[X]$, $(X, 2)$. If $(f(X)) = (X, 2) \Rightarrow f(X) \mid X$

$\Rightarrow f(X) = \pm X$

But $2 \notin (f(X))$.

So $(X, 2)$ is not principal.

$\gcd(X, 2) = 1$

(X) 1) $\mathbb{Z}[X]$ is not a PID. (X) is prime ideal.

2) $\mathbb{Z}[\sqrt{-3}]$ is not a PID.

$\mathbb{Z}[\sqrt{-3}] \subseteq \mathbb{Q}[\sqrt{-3}] \subseteq \mathbb{C}$

$\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$

$I = (1+\sqrt{-3}, 2) \subseteq \mathbb{Z}[\sqrt{-3}] = \{a+b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$

$\mathbb{Z}[\sqrt{D}]$ is not a PID whenever D is squarefree & $D \equiv 1 \pmod 4$

claim: $I \cap \mathbb{Z} = 2\mathbb{Z}$

$x \in$ $\supseteq$ ✓

$(1+\sqrt{-3})(1-\sqrt{-3}) = 4$

$x = \alpha(1+\sqrt{-3}) + \beta 2 \in \mathbb{Z}$ $\quad \alpha \in \mathbb{Z}[\sqrt{-3}]$, $\beta \in \mathbb{Z}$

$\Rightarrow \alpha = a(1-\sqrt{-3})$ where $a \in \mathbb{Z}$, $x = 4a + 2\beta$

$\Rightarrow x \in 2\mathbb{Z}$

So $1 \notin I$. If $I = (a+b\sqrt{-3})$

Since $1+\sqrt{-3} \notin 2\mathbb{Z}[\sqrt{-3}] \Rightarrow I$ is not generated by integer.

So $b \neq 0$. $2 = (c+d\sqrt{-3})(a+b\sqrt{-3})$ (*)

$\Rightarrow c+d\sqrt{-3} = e(a-b\sqrt{-3})$

$N: \mathbb{Q}[\sqrt{-3}] \to \mathbb{Q}$

$a+b\sqrt{-3} \mapsto a^2+3b^2$

$4 = (c^2+3d^2)(a^2+3b^2)$

$b \neq 0 \Rightarrow b = \pm 1$, $a = \pm 1$

$d = 0$, $c = 1$

N satisfies $N(\alpha\beta) = N(\alpha)N(\beta)$ $\forall \alpha, \beta \in \mathbb{Q}[\sqrt{-3}]$

If $\alpha \in \mathbb{Z}[\sqrt{-3}]$ then $N(\alpha) \in \mathbb{Z}$

i.e. $\pm 1 \pm \sqrt{-3}$

But $2 = (1+\sqrt{-3})\frac{(1-\sqrt{-3})}{2}$ not in $\mathbb{Z}[\sqrt{-3}]$

$\Rightarrow 2 \notin (1+\sqrt{-3})$

In fact $\mathbb{Z}[\sqrt{d}]$ is not a PID if $d \equiv (1 \bmod 4)$ & d is squarefree

(*) $\mathbb{Z}[i]$ is a Euclidean domain and hence a PID. $i = \sqrt{-1}$, $\mathbb{Z}[i] = \{a+ib \mid a,b \in \mathbb{Z}\}$

Pf: $N : \mathbb{Z}[i]^\times \longrightarrow \mathbb{Z}_{\geq 0}$, $a+bi \longmapsto a^2+b^2$

Claim N is a Euclidean norm.

Let $\alpha, \beta \in \mathbb{Z}[i]^\times$ then $\alpha = a+bi$ & $\beta = c+di$ for some $a,b,c,d \in \mathbb{Z}$

Want $\alpha = \beta q + r$ with $N(r) < N(\beta) \Leftrightarrow r = 0$

$\frac{\alpha}{\beta} = \frac{(a+bi)(c-di)}{c^2+d^2} = u+vi$ $u,v \in \mathbb{Q}$

Let $p, q \in \mathbb{Z}$ be s.t. $|u-p| \leq \frac{1}{2}$ and $|v-q| \leq \frac{1}{2}$

$\alpha = \beta(p+qi) + \beta\underbrace{(u-p+(v-q)i)}_{=\gamma \in \mathbb{Z}[i]}$

$N(\gamma) = N(\beta)\left((u-p)^2 + (v-q)^2\right)$

$\leq \frac{1}{2} N(\beta) < N(\beta)$

Hence the claim. i.e. $\mathbb{Z}[i]$ is ED.

Thm: R a comm ring with unity s.t. $R[X]$ is a PID then R is a field.

Pf: $R \subseteq R[X]$ is a subring and hence an int domain.

Let $\varphi : R[X] \longrightarrow R$ be the map $f(X) \longmapsto f(0)$

Then φ is a surj ring homo.

& $\ker(\varphi) = (X)$

$\supseteq$ ✓

$\subseteq$: $\varphi(f(X)) = 0$ for $f(X) = a_n X^n + a_{n-1}X^{n-1} + \dots + a_1 X + a_0$

then $a_0 = 0 \Rightarrow f(X) = X(a_{n-1}X^{n-1} + \dots + a_1) \in (X)$

Hence $R[X]/(X) \cong R \Rightarrow (X)$ is a prime ideal in the PID $R[X]$.

Hence (X) is maximal ideal of $R[X]$.

$\Rightarrow$ R is a field.

Ex $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ is a PID but not ED.

R $\subseteq$ $\mathbb{Q}[\sqrt{-19}]$ $\quad N\left(\frac{1+\sqrt{19}}{2}\right) = \frac{1+19}{2} = 10 \in \mathbb{Z}$

Prop Let R be a ED but not a field then it contains a "universal side divisor", i.e. an element u which is non zero nonunit s.t. $\forall x \in R^\times \exists q \in R$ satisfying $x - qu$ is either zero or a unit. $x = qu + r$

Pf: Let u be a nonzero nonunit in R with least Euclidean norm. Then u is a universal side divisor. $\left(x \in R^\times \Rightarrow \exists q, r \in R \text{ s.t. } x = uq + r \text{ with } N(r) < N(u) \text{ or } r = 0 \Rightarrow r = 0 \text{ or } r \text{ is a unit}\right)$

Units in $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$

$N: R \to \mathbb{Z}$ $\quad \alpha$ is a unit iff $N(\alpha)$ is a unit. $\left(\Rightarrow \alpha\alpha^{-1} = 1 \Rightarrow N(\alpha)N(\alpha^{-1}) = N(1) = 1\right)$

Let $\alpha = a + b\left(\frac{1+\sqrt{-19}}{2}\right)$ $\quad \alpha^* \cdot \alpha = \pm 1$

$N(\alpha) = \alpha\bar{\alpha} = \left(a + b\left(\frac{1+\sqrt{-19}}{2}\right)\right)\left(a + b\left(\frac{1-\sqrt{-19}}{2}\right)\right)$

$= a^2 + b^2\frac{1+19}{4} + ab$

$= a^2 + 5b^2 + ab$

α is a unit $\Leftrightarrow N(\alpha) = \pm 1$

$\Leftrightarrow a^2 + ab + 5b^2 = \pm 1$

$\left(a + \frac{1}{2}b\right)^2 + \frac{19}{4}b^2 = \pm 1$

$(2a + b)^2 + 19b^2 = \pm 4$

$\Rightarrow b = 0$ & $a = \pm 1$

Units in $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ is ± 1

Check $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ has no universal side divisor. u

$x = 2 \quad 2 = uq + r$

$u = \{\pm 2, \pm 3\}$ $\quad r = \pm 1$ or 0

Prop R is a PID iff R has Dedekind-Hasse norm.

where $N: R^\times \to \mathbb{Z}_{>0}$ is a Dedekind-Hasse norm if $\forall a, b \in R^\times$ either $a \in (b)$, i.e. $b \mid a$ or $\exists r \in (a, b)$ s.t. $N(r) < N(b)$

$\exists x, y \in R$ $r = ax + by$ $\quad N(ax + by) < N(b)$

Pf: $(\Leftarrow)$: $I \subseteq R$ a nonzero ideal

Let $b \in I$ be of least norm then $I = (b)$ (If $a \in I$ then $\exists r \in (a, b]$ with $N(r) < N(b)$ or $a \in (b)$. Not possible)

$(\Rightarrow)$ Later.

$\exists q, r$ s.t. $a = bq + r$ $\quad N(r) < N(b)$ or $r = 0$

$r = bq + a$

$\exists q', q$ s.t. $r = bq + aq'$ with $N(r) < N(b)$ or $r = 0$

Check that

$$N: \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]^{\times} \longrightarrow \mathbb{Z}_{>0}$$

$$\omega = \frac{1+\sqrt{-19}}{2}$$

$$a+b\omega \longmapsto a^2+ab+5b^2$$

is a Dedekind-Hasse norm.

(*) Let D be squarefree integer.

$\mathbb{Q}(\sqrt{D})$ is a field

$$R = \begin{cases} \mathbb{Z}[\sqrt{D}] & \text{if } D \not\equiv 1 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] & \text{if } D \equiv 1 \pmod 4 \end{cases}$$

Then R is called ring of integers in $\mathbb{Q}(\sqrt{D})$

$$N: \mathbb{Q}(\sqrt{D}) \longrightarrow \mathbb{Q}$$

$$(a+b\sqrt{D}) \longmapsto a^2 - Db^2$$

$$N|_R : R \longrightarrow \mathbb{Z}$$

$$N(\alpha\beta) = N(\alpha)N(\beta)$$

$N(\alpha)$ is a unit in $\mathbb{Z}$ $\iff$ α is unit in R.

α is unit $\Rightarrow \alpha\alpha^{-1} = 1$

$$1 = N(1) = N(\alpha)N(\alpha^{-1})$$

$N(\alpha)$ is unit in $\mathbb{Z}$

$$\pm 1 = N(\alpha) = \alpha\bar{\alpha} \Rightarrow \alpha \text{ is unit}$$

∎

Lecture 14: Unique factorization domain(UFD)

05 October 2020
11:30

Recall: 1) An int dom R is a ED if $\exists$ a norm $N: R^\times \to \mathbb{Z}_{\geq 0}$ s.t. $\forall a, b \in R^\times$ $\exists q, r \in R$ satisfying $a = bq + r$ with $r = 0$ or $N(r) < N(b)$.

2) An ID R is a PID if every R-ideal is principal (gen by 1 element)

(1) R ED $\Rightarrow$ R PID

(2) x irred if x nonzero nonunit & $x = yz \Rightarrow$ y is a unit or z is a unit

(3) x prime if " " " & $x \mid ab \Rightarrow x \mid a$ or $x \mid b$.

(4) R an int dom. x prime $\Rightarrow$ x irred.

(5) R PID. x irred $\iff$ x prime.

(6) R a PID then every nonzero prime ideal is maximal. $\mathbb{Z}[x]$ is not a PID.

(7) $R[x]$ is a PID iff R is a field.

(8) $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ is a PID but not a ED.

(9) R is a PID iff R has Dedekind-Hasse norm.
i.e. $N: R^\times \to \mathbb{Z}_{>0}$ s.t.
$\forall a, b$, $b \mid a$ or $\exists x, y \in R$
s.t. $N(ax+by) < N(b)$

(Saw if part)

(10) R is a ED but not a field. Then R has "universal side divisor" ie. $u \in R$ nonzero nonunit s.t. $\forall x \in R$ either $u \mid x$ or $x - uq$ is a unit for some q in R.

Definition: Unique Factorization Domain (UFD).

Let R be an integral domain such that for any $x \in R$ nonzero nonunit, x can be uniquely written as product of irreducibles, where uniqueness means the following:

$x = p_1 \cdots p_n = q_1 \cdots q_m$ where $p_1, \ldots, p_n, q_1, \ldots, q_m$ are irreducible. Then

$n = m$ & after a reordering p_i & q_i are associates for all $1 \le i \le n$. "(i.e. $p_i = u_i q_i$ for some unit $u_i \in R$)"

Def^n: Let R be a comm ring with unity and $x, y \in R$ then x, y are said to be associates if $\exists\, u \in R$ unit s.t. $x = uy$.

Its denoted by $x \sim y$.

Note that $\sim$ is an equivalence relation

$\sim$ is reflexive & symmetric ✓

$x \sim y$ & $y \sim z \Rightarrow \exists\, u, v \in R$ units s.t. $x = uy$ & $y = vz$.

$\Rightarrow x = uvz$. But uv is a unit.

Hence $x \sim z$.

Ex: $\mathbb{Z}$ is a UFD.

(*) x irred iff $y \mid x \Rightarrow [y] = [1]$ or $[y] = [x]$ (associate)

i.e. $y \sim 1$ or $y \sim x$

Prop: Let R be a PID then R is a UFD.

Pf: Let $x \in R$ be a nonzero nonunit

$\exists$ a maximal ideal $P_1 \subseteq R$ s.t. $x \in P_1$.

Then $P_1 = (p_1)$ & $x \in (p_1) \Rightarrow \exists\, x_2 \in R$ s.t. $x = x_1 = p_1 x_2$. Note p_1 is irreducible (prime and hence irreducible)

If x_2 is a unit then $x = x_1$ is irreducible. Stop.

Otherwise repeat to get

$x_2 = p_2 x_3$ where p_2 is irred & $x_3 \in R$.

$\Rightarrow x_1 = p_1 p_2 x_3$ if x_3 is a unit, then stop.

$= p_1 x_2$ is prod of irred. ($x_2 = p_2 x_3$ is irred. if x_3 is unit)

Otherwise continue ....

Suppose this never stops. Let $x_1, x_2, x_3, \ldots$ be obtained by this process.

$I = (x_1, x_2, x_3, \ldots)$ be the ideal gen by $x_1, x_2, \ldots$

Since R is a PID $\exists\, y \in I$ s.t. $I = (y)$.

Note $(x_1) \subseteq (x_2) \subseteq (x_3) \subseteq \ldots$

So $I = \bigcup_{i \geq 1} (x_i)$. Hence $y \in (x_n)$ for some n. Then $y = u x_n$ for some $u \in R$

Also $x_n = p_n x_{n+1}$, p_n irred.; $x_{n+1} \in (y) = I$

$\Rightarrow x_{n+1} = vy$ for some $v \in R$.

Hence $y = u x_n = u p_n x_{n+1} = uv p_n y$

$\Rightarrow uv p_n = 1$ is a unit. A contradiction! (p_n is irred. and hence nonunit)

Hence $\exists\, n$ s.t. x_n is a unit.

$\Rightarrow x = x_1 = p_1 x_2 = p_1 p_2 x_3 = \cdots = p_1 p_2 \cdots p_{n-1} x_n$

where $p_1, \ldots, p_{n-1}$ are irred.

So $x = p_1 \cdots p_{n-2} \cdot (p_{n-1} x_n)$

Uniqueness:

Let $x = p_1 \cdots p_n = q_1 \cdots q_m$ be product of irred. i.e. $p_1, \ldots, p_n$ & $q_1, \ldots, q_m$ are irred elements of R.

p_1 is irred & R is a PID $\Rightarrow$ p_1 is a prime element. Since $p_1 \mid x = q_1 \cdots q_m$

p_1 is a prime element $\Rightarrow$ $p_1 \mid q_{i_1}$ for some $i_1 \in \{1, \ldots, m\}$

$\Rightarrow q_{i_1} = u_1 p_1$

But q_{i_1} is irred. so u_1 is a unit. $\Rightarrow$ p_1 & q_{i_1} are associates

After reordering q_i's (i.e. interchanging q_1 & q_{i_1}) we obtain that p_1 & q_1 are associates. ($q_1 = u_1 p_1$, u_1: unit)

$$x = p_1 p_2 \cdots p_n = q_1 \cdots q_m = u_1 p_1 q_2 \cdots q_m$$

$$\Rightarrow p_2 \cdots p_n = u_1 q_2 \cdots q_m$$

$$\Rightarrow p_2 \mid u_1 p_2 \cdots p_n = q_2 \cdots q_m$$

p_2 is prime $\Rightarrow$ $p_2 \mid q_{i_2}$ for some $2 \le i_2 \le m$

So $q_{i_2} = u_2 p_2$ for some $u_2 \in R$

But q_{i_2} is irred., hence u_2 is a unit.

Again reorder q's to get $p_2 \sim q_2$

Continuing this way, we get a reordering of q's s.t. $p_i \sim q_i$ $1 \le i \le n$.

and $m \ge n$. But by symmetry $n \ge m$

Hence $n = m$. ∎

Example: 1) $k[x]$ where k is a field.
2) $\mathbb{Z}[x]$ is a UFD.
3) $k[x_1, \dots, x_n]$ is a UFD for k a field or $k = \mathbb{Z}$.

Non examples: 1) $\mathbb{Z}[\sqrt{5}]$ or $\mathbb{Z}[\sqrt{-3}]$ is not a UFD.

2) $\bar{x}, \bar{y}, \bar{z}, \bar{w} \in \dfrac{\mathbb{Q}[x, y, z, w]}{(xy - zw)} = R$

$\bar{x}\bar{y} \in R$ $=$ $\bar{z}\bar{w}$

But $\bar{x}, \bar{y}, \bar{z}, \bar{w}$ are irred but none of them are assosiates to each other.

(*) Let R be a UFD & $x \in R$. Then x is irred $\Leftrightarrow$ x is prime.

Pf: Enough to show: ($\Rightarrow$):

Suppose $x \mid ab$ for $a, b \in R$.

$\Rightarrow$ (*) $\boxed{ab = xy}$ for some $y \in R$

If a is unit or b is a unit then $x \mid b$ or $x \mid a$ and we are done.

Otherwise $\exists\, p_1, \dots, p_n \in R$ irred & $q_1, \dots q_m \in R$ irred. s.t.

$a = p_1 \cdots p_n$ & $b = q_1 \cdots q_m$.

Also $y = r_1 \cdots r_k$ r_i irred. in R

$x r_1 \cdots r_k = p_1 \cdots p_n q_1 \cdots q_m$ from (*)

Uniqueness for irreducible factorization implies $x \sim p_i$ for some $1 \le i \le n$ or $\Rightarrow x \mid a$

$x \sim q_j$ " " $1 \le j \le m \Rightarrow x \mid b$

Lecture 15: UFD continued

07 October 2020
10:29

Recall: 1) R is a UFD if it is an int. domain and every nonzero nonunit can be written uniquely as product of irreducible elements of R.

2) A PID is a UFD. (Converse is not true)

3) R a UFD $\Rightarrow R[X]$ a UFD (Will be proved later)

4) In a UFD, irreducibles are primes.

5) $\mathbb{Z}[\sqrt{-3}]$ is not a UFD; $\frac{\mathbb{Q}[X,Y,Z,W]}{(XY-ZW)}$ is not a UFD.

$1+\sqrt{-3} = (a+b\sqrt{-3})(c+d\sqrt{-3})$ $\quad a,b,c,d \in \mathbb{Z}$

Apply norm $\quad 4 = (a^2+3b^2)(c^2+3d^2)$

May assume $b=0$

$(1+\sqrt{-3}) = a(c+d\sqrt{-3})$

$ac = 1$ & $ad = 1$

$\Rightarrow a = \pm 1 \Rightarrow 1+\sqrt{-3}$ is irred.

$(1+\sqrt{-3})(1-\sqrt{-3}) = 4 \Rightarrow 1+\sqrt{-3} \mid 4 = 2\cdot 2$

But $1+\sqrt{-3} \nmid 2$

$(1+\sqrt{-3})(a+b\sqrt{-3}) \neq 2 \quad \forall\, a,b \in \mathbb{Z}$

$\Rightarrow 1+\sqrt{-3}$ is not a prime.

X is irred. but not a prime.

Prop: Let R be a UFD and $a, b \in R$. Then

$a = u p_1^{e_1} \cdots p_r^{e_r}$ for some $r \geq 0$, $u, v \in R$ unit, $p_1, \ldots, p_r$ irred elements of R and $e_1, \ldots, e_r, f_1, \ldots, f_r \in \mathbb{Z}_{\geq 0}$.

$b = v p_1^{f_1} \cdots p_r^{f_r}$

and $\gcd(a, b) = p_1^{\min(e_1, f_1)} p_2^{\min(e_2, f_2)} \cdots p_r^{\min(e_r, f_r)}$

Pf: Since R is a UFD

$a = u p_1^{e_1} \cdots p_n^{e_n}$ for some $n \geq 0$, $p_1, \ldots, p_n, u \in R$ with u unit $p_1, \ldots, p_n$ irred & $e_1, \ldots, e_n \in \mathbb{Z}_{>0}$.

and $b = v p_1^{f_1} \cdots p_n^{f_n} p_{n+1}^{f_{n+1}} \cdots p_r^{f_r}$ for some $r \geq n$, $v \in R$ unit, $p_{n+1}, \ldots, p_r$ irred. & $f_1, \ldots, f_r \in \mathbb{Z}_{\geq 0}$

Set $e_{n+1} = e_{n+2} = \cdots = e_r = 0$

Let $d = p_1^{\min(e_1, f_1)} \cdots p_r^{\min(e_r, f_r)}$ then

$d \mid a$ & $d \mid b$. Let $d' \mid a$ & $d' \mid b$.

($a = d u p_1^{e_1 - \min(e_1, f_1)} \cdots p_r^{e_r - \min(e_r, f_r)}$)

Then $a = d' a_1$ & $b = d' b_1$. By uniqueness of factorization in UFD, factorizing d' we get, $d' = w p_1^{h_1} \cdots p_r^{h_r}$ with w unit & $h_i \leq e_i$ (as $d' \mid a$) and $h_i \leq f_i$ (as $d' \mid b$)

Hence $h_i \leq \min(e_i, f_i) \Rightarrow d' \mid d \Rightarrow$

$d = \gcd(a, b)$. ∎

Prob: Every PID admits a Dedekind-Hasse norm.

Pf: $N : R^\times \longrightarrow \mathbb{Z}_{>0}$

units $\longmapsto 1$

x non unit, $x = p_1 \cdots p_n \longmapsto 2^n$ where p_i irred.

$$N(x) = 2^n$$

WTS:

Let $a, b \in R$ either $b \mid a$ or $\exists\, x, y \in R$ s.t. $N(ax+by) < N(b)$.

Suppose $b \nmid a$. Let $(d) = (a, b)$

$d \mid b$ & $b \nmid d$ ($\because$ if $b \mid d \Rightarrow b \mid a$)

Let $d = p_1 \cdots p_n$ then

& $b = p_1 \cdots p_n q_1 \cdots q_m$ & $m \geq 1$

$\Rightarrow N(d) = 2^n < N(b) = 2^{n+m}$

& $d = ax + by$ for some $x, y \in R$. ∎

"$N(x) = n+1$ should work"

Thm: Let R be an integral domain. R is a UFD iff

1) Every irred element in R is prime and
2) Every strictly increasing chain of principal ideals is of finite length.

Pf: ($\Rightarrow$): (1) ✓

(2): Let

$(0) \subsetneq (x_1) \subsetneq (x_2) \subsetneq (x_3) \subsetneq \cdots$ be a strictly increasing chain of principal ideals.

Let $x_1 = p_1 \cdots p_n$ $p_i \in R$ irred.

$x_1 \in (x_2) \Rightarrow x_2 \mid x_1$ & $(x_2) \neq (x_1) \Rightarrow x_1 \nmid x_2$ } $x_1 = x_2 y_1$ for $y_1 \in R$ where y_1 is nonzero non unit

No of irreducible factors in x_2 is strictly less than n. Let $x_2 = q_1 \cdots q_m$ as prod of irr

$y = r_1 \cdots r_k$

$p_1 \cdots p_n = q_1 \cdots q_m r_1 \cdots r_k$

Uniqueness $\Rightarrow$ $m+k = n \Rightarrow m < n$

Illy No of irr factors of $x_3 <$ No of irr factors of x_2 and so on. So the length of the chain of the principal ideals

$(x_1) \subsetneq (x_2) \subsetneq \cdots$ can be at most n.

($\Leftarrow$):

Let $x \in R$ nonzero nonunit.

Want to show x is a product of irreducibles.

Claim: $x = p_1 y$ where p_1 is irred. & $y \in R$.

If x is irred then done.

otherwise $\exists\ x_1, y_1 \in R$ s.t.

$x = x_1 y_1$ where x_1 & y_1 are nonunits.

$\Rightarrow (x) \subsetneq (x_1)$ ($\because$ y_1 is nonunit)

Now if x_1 is irred then we have shown that $x = p_1 y_1$ where p_1 is irred & $y_1 \in R$ with $p_1 = x_1$ in R

otherwise $x_1 = x_2 y_2$ where x_2, y_2 are nonunit.

and $(x_1) \subsetneq (x_2)$

Continuing this way we obtain a strictly increasing seq of principal ideals

$(x) \subsetneq (x_1) \subsetneq (x_2) \subsetneq \cdots$

So by (2) it must stop say at n^{th} spot. So x_n must be irred.

So $x = x_1 y_1 = x_2 y_2 y_1 = \cdots = x_n y_n y_{n-1} \cdots y_1$

$\Rightarrow x = p_1 y$ where p_1 is irred & $y \in R$.

with $p_1 = x_n$ in R & $y = y_1 \cdots y_n$

Claim: $x = p_1 \cdots p_n$ where $p_i \in R$ are irred.

Pf: By prev claim

$x = p_1 y_1$ for some $p_1 \in R$ irred & $y_1 \in R$.

If y_1 is a unit or irred then done

otherwise

$y_1 = p_2 y_2$ where p_2 irr & $y_2 \in R$

and continue this way if y_2 is not irred.

$(x) \subsetneq (y_1) \subsetneq (y_2) \subsetneq \cdots$

(strictness is true because p_1, p_2 are irred & hence not a unit)

Again by (2) this has to stop at say after n steps. Then

$x = p_1 \cdots p_n y_n$ as product of irred.

Exc: Show uniqueness of irred factorization using (1).

Hint: See PIDs are UFDs proof.

Lecture 16: Field of fractions, Localization

08 October 2020
13:31

⊛ Construction of $\mathbb{Z}$ to $\mathbb{Q}$:

$$\mathbb{Q} = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z}, b \neq 0 \right\} = \{(a,b) \mid a,b \in \mathbb{Z}, b \neq 0\} / \sim$$

$(a,b) \sim (c,d)$ if $ad = bc$

So we are inverting all nonzero elements of $\mathbb{Z}$ to obtain $\mathbb{Q}$.

Lets generalize this to arbitrary rings.

Def^n: Let R be a comm ring with unity & $S \subseteq R$ be subset. Then S is said to be multiplicative subset if $1 \in S$ & $\forall\, x, y \in S$, $xy \in S$.

Example: (R any ring)

1) $S = \{1\}$
2) S = set of units, 2') $S = R$ ← Not interesting
3) R an integral domain like $\mathbb{Z}$; $S = R \setminus \{0\}$. ←
4) In $\mathbb{Z}$, $S = \mathbb{Z}_{>0}$
5) R any ring, & $x \in R$, $S = \{1, x, x^2, x^3, \ldots\}$ is a multiplicative set.
6) R any ring, $S = I \cup \{1\}$ is a multiplicative set. (Not interesting for localization)
7) Let R be any ring and $P \subseteq R$ a prime ideal. Then $S = R \setminus P$ is a multiplicative set.

   ⊃. $b \in S \Rightarrow ab \notin P$ ($\because$ P prime ideal) $\Rightarrow ab \notin P \Rightarrow ab \in S$.

Define a relation on $S \times R$ where R is comm ring with unity and S is a mult set.

$$S \times R = \{(s,r) \mid s \in S \ \& \ r \in R\}$$

$(s_1, r_1) \sim (s_2, r_2)$ if $s(s_2 r_1 - s_1 r_2) = 0$ for some $s \in S$.

Prop: $\sim$ is an equivalence relation

Pf: $(s_1, r_1) \sim (s_1, r_1)$ by taking $s = 1$

$1(s_1 r_1 - s_1 r_1) = 0$

$\sim$ is reflexive

$\sim$ is symmetric

$(s_1, r_1) \sim (s_2, r_2)$ then $\exists s \in S$

s.t. $s(s_2 r_1 - s_1 r_2) = 0$

$\Rightarrow \quad s(s_1 r_2 - s_2 r_1) = 0$

$\Rightarrow (s_2, r_2) \sim (s_1, r_1)$

$\sim$ is transitive:

Let $(s_1, r_1) \sim (s_2, r_2)$ & $(s_2, r_2) \sim (s_3, r_3)$

$\exists s, s' \in S$ s.t.

$s(s_2 r_1 - s_1 r_2) = 0$ ... ① & $s'(s_3 r_2 - s_2 r_3) = 0$ ... ②

$s' s_3$ ① $+ s s_1$ ② gives

$s' s s_2 s_3 r_1 - s' s s_1 s_3 r_2 + s s' s_3 s_1 r_2 - s s' s_2 s_1 r_3 = 0$

$s' s s_2 (s_3 r_1 - s_1 r_3) = 0$

Also $s' s s_2 \in S$ ($\because$ S is multiplicative)

Hence $\sim$ is an equivalence relation.

Def^n/Prop: The set of equivalence classes $S \times R/\sim$ is denoted by $S^{-1}R$. The equivalence class $[(s,r)]$ will be denoted by $\frac{r}{s}$.

The binary operators $\frac{r_1}{s_1} \oplus \frac{r_2}{s_2} := \frac{s_2 r_1 + s_1 r_2}{s_1 s_2}$ and

$\frac{r_1}{s_1} \odot \frac{r_2}{s_2} = \frac{r_1 r_2}{s_1 s_2}$ are well defined. Moreover $(S^{-1}R, \oplus, \odot)$ is a commutative ring with unity. The map

$\varphi : R \longrightarrow S^{-1}R$ is a ring homo.

$r \longmapsto \frac{r}{1}$

Pf: $\frac{r_1}{s_1} = \frac{r_1'}{s_1'}$ $\frac{r_2}{s_2} = \frac{r_2'}{s_2'}$ $r_1, r_1', r_2, r_2' \in R$ $s_1, s_1', s_2, s_2' \in S$ $\Rightarrow (s_1, r_1) \sim (s_1', r_1')$ $\Rightarrow (s_2, r_2) \sim (s_2', r_2')$

WTS: $\frac{s_2 r_1 + s_1 r_2}{s_1 s_2} = \frac{s_2' r_1' + s_1' r_2'}{s_1' s_2'}$

$\exists\, u, v \in S$ s.t.

$u(s_1' r_1 - s_1 r_1') = 0$ ---① & $v(s_2' r_2 - s_2 r_2') = 0$ ---②

WTS: $\exists\, w \in S$ s.t.

$$w\left[s_1' s_2' (s_2 r_1 + s_1 r_2) - s_1 s_2 (s_2' r_1' + s_1' r_2')\right] = 0$$

$s_2 s_2' v$ ① + $s_1 s_1' u$ ② gives

$$s_2 s_2' v u s_1' r_1 - s_2 s_2' v u s_1 r_1' + s_1 s_1' u v s_2' r_2 - s_1 s_1' u v s_2 r_2' = 0$$

$$uv\left[s_1' s_2' (s_2 r_1 + s_1 r_2) - s_1 s_2 (s_2' r_1' + s_1' r_2')\right] = 0$$

So take $w = uv \in S$ ($\because S$ is multiplicative)

Ill-def by ⊙ is well-defined.

Claim: $(S^{-1}R, \oplus, \cdot)$ is a comm ring with unity

1) $(S^{-1}R, \oplus)$ is an abelian group

- check $\oplus$ is associative (check)
- $\frac{0}{1}$ is the additive identity ✓ $\frac{r_1}{s_1} \oplus \frac{0}{1} = \frac{1r_1 + s_1 0}{s_1} = \frac{r_1}{s_1}$
- $\oplus$ is commutative ✓
- $\frac{r}{s} \oplus \frac{-r}{s} = 0$ $\quad \frac{r}{s} \oplus \frac{-r}{s} = \frac{sr - sr}{ss} = \frac{0}{ss} = \frac{0}{1}$

But $\frac{0}{ss} = \frac{0}{1}$ $(\because 1(1 \cdot 0 - ss \cdot 0) = 0)$

2) $\cdot$ is associative

easily follows from $\cdot$ is assoc in R

- $\cdot$ is commutative

easily " " " comm in R.

- $\frac{1}{1}$ is unity. (trivial)
- Distributive laws (check)

$$\varphi(r + r') = \frac{r + r'}{1} = \frac{r}{1} \oplus \frac{r'}{1} = \varphi(r) \oplus \varphi(r')$$

$$\varphi(r r') = \frac{r r'}{1} = \frac{r}{1} \cdot \frac{r'}{1} = \varphi(r)\varphi(r')$$

Hence φ is ring homo. Also $\varphi(1) = \frac{1}{1}$ is unity in $S^{-1}R$.

Lecture 17: Universal property of localization

09 October 2020
13:19

Define a relation on $S \times R$ where R is comm ring with unity and S is a mult set.

$$S \times R = \{(s,r) \mid s \in S \ \& \ r \in R\}$$

$(s_1, r_1) \sim (s_2, r_2)$ if $s(s_2 r_1 - s_1 r_2) = 0$ for some $s \in S$.

(*) $\sim$ is an equivalence relation. $[(s,r)] = \frac{r}{s}$

Def^n/Prop: The set of equivalence classes $S \times R / \sim$ is denoted by $S^{-1}R$. The equivalence class $[(s,r)]$ will be denoted by $\frac{r}{s}$.

The binary operators $\frac{r_1}{s_1} \oplus \frac{r_2}{s_2} := \frac{s_2 r_1 + s_1 r_2}{s_1 s_2}$ and

$$\frac{r_1}{s_1} \odot \frac{r_2}{s_2} := \frac{r_1 r_2}{s_1 s_2}$$

are well defined. Moreover $(S^{-1}R, \oplus, \odot)$ is a commutative ring with unity. The map

$$\varphi : R \longrightarrow S^{-1}R, \quad r \longmapsto \frac{r}{1}$$

is a ring homo.

$$0_{S^{-1}R} = \frac{0}{1} = \frac{0}{s} \quad \forall s \in S$$

$$1_{S^{-1}R} = \frac{1}{1} = \frac{s}{s} \quad \forall s \in S$$

Ex: ① $R = \mathbb{Z}$ & $S = \mathbb{Z} \setminus \{0\}$.

$S \times R = \{(s, r) \mid s \neq 0, s, r \in R\}$

$(s_1, r_1) \sim (s_2, r_2)$ if $\exists s \in \mathbb{Z} \setminus \{0\}$ s.t

$s(s_2 r_1 - s_1 r_2) = 0$

$\Uparrow$

$s_2 r_1 - s_1 r_2 = 0$

$\Uparrow$

$s_2 r_1 = s_1 r_2$

$\frac{r_1}{s_1} = \frac{r_2}{s_2}$ iff $s_2 r_1 = s_1 r_2$

So $S^{-1}R = \mathbb{Q}$.

Def w/ Prop: More generally if R is an integral domain & $S = R \setminus \{0\}$ then the ring $S^{-1}R$ is a field. This field is denoted by $\mathrm{frac}(R)$ or $QF(R)$ and is called field of fractions of R. Moreover $\varphi : R \hookrightarrow \mathrm{frac}(R)$ is injective and if K is a field containing R as a subring then K contains $\mathrm{frac}(R)$.

Pf: Let $\alpha \in S^{-1}R = \text{frac}(R)$, $\alpha \neq 0$ in $S^{-1}R$

$\alpha = \frac{r}{s}$ $r \in R$ & $s \in S = R \setminus \{0\}$

Since $\alpha \neq 0$ is $S^{-1}R \Rightarrow r \neq 0 \Rightarrow r \in S$

$\Rightarrow \frac{s}{r} \in S^{-1}R$. Then

$$\frac{s}{r} \cdot \frac{r}{s} = \frac{sr}{sr} = \frac{1}{1} = 1_{S^{-1}R}$$

Hence $S^{-1}R$ is a field.

$$\varphi : R \longrightarrow S^{-1}R$$
$$r \longmapsto \frac{r}{1}$$

$$\ker(\varphi) = \left\{ r \,\middle|\, \frac{r}{1} = \frac{0}{1} \quad r \in R \right\}$$

$$= \{ r \in R \mid \exists\, s \in R \setminus \{0\} \text{ s.t. } s(1 \cdot r - 1 \cdot 0) = 0_R \}$$

$$= \{ r \in R \mid sr = 0, \ s \neq 0 \text{ some } s \in R \}$$

$$= \{ r \in R \mid r = 0 \} = \{0\}$$

$\Rightarrow \varphi$ is injective.

Let K be a field & $R \subseteq K$ be a subring. Let $\frac{r}{s} \in S^{-1}R$ then $s \neq 0$ in R & $r \in R \Rightarrow \frac{r}{s} \in K$.

So $S^{-1}R \subseteq K$.

⊛ Let R be a comm ring with unity and S a mult. subset of R. Then $\varphi(s)$ is a unit in $S^{-1}R$ $\forall s \in S$. Here $\varphi : R \to S^{-1}R$ is the natural map.

$$r \longmapsto \frac{r}{1}$$

Pf: $\varphi(s) = \frac{s}{1} \in S^{-1}R$, so $s \in S$.

so $\frac{1}{s} \in S^{-1}R$ and $\frac{s}{1} \cdot \frac{1}{s} = \frac{s}{s} = \frac{1}{1} = 1_{S^{-1}R}$

Hence $\varphi(s)$ is a unit.

⊛ If $0 \in S$ then $S^{-1}R$ is the zero ring.

Pf: Claim $\frac{r}{s} = \frac{0}{1}$ $\forall r \in R$ & $s \in S$

the above equality holds if $u(1r - s0) = 0$ for some $u \in S$

Take $u = 0 \in S$. Hence the claim.

Hence $S^{-1}R = \{0\}$. ∎

⊛ In general, S mult subset of a comm ring R & $\varphi : R \to S^{-1}R$ then

$$r \longmapsto \frac{r}{1}$$

$$\ker(\varphi) = \{ r \in R \mid sr = 0 \text{ for some } s \in S \}.$$

In particular if S consist of nonzero divisors in R then φ is injective. Converse also holds.

Thm (Universal property of Localization):
Let R be comm ring with unity. $S \subseteq R$ be a mult. subset of R. Let

$f : R \longrightarrow A$ be a ring homomorphism.

where A is a comm ring with unity such that $\forall s \in S$ $f(s)$ is a unit in A. Then $\exists!$ ring homo.

$\tilde{f} : S^{-1}R \longrightarrow A$ s.t. $\tilde{f} \circ \varphi = f$.

$$\begin{array}{ccc} R & \xrightarrow{f} & A \\ & \searrow^{\varphi} & \uparrow \exists! \tilde{f} \\ & & S^{-1}\varphi \end{array}$$

Pf: $\tilde{f} : S^{-1}R \longrightarrow A$

Let $\frac{r}{s} \in S^{-1}R$ for some $r \in R$ & $s \in S$

$\tilde{f}\left(\frac{r}{s}\right) = f(s)^{-1} f(r)$ (Note $f(s)$ is a unit in A. Hence $f(s)^{-1}$ make sense)

$\tilde{f}$ is well-defined:

Let $\frac{r'}{s'} = \frac{r}{s}$

$\Rightarrow \exists\, u \in S$ s.t. $u(sr' - s'r) = 0$ in R

$\because f$ is a ring homo $\Rightarrow f(u)\left(f(s)f(r') - f(s')f(r)\right) = 0$ in A

$f(u)$ is a unit $\Rightarrow f(s)f(r') = f(s')f(r)$ in A

$\cdot f(s)^{-1}f(s')^{-1} \Rightarrow f(s')^{-1}f(r') = f(s)^{-1}f(r)$

Hence $\tilde{f}\left(\frac{r'}{s'}\right) \quad f\left(\frac{r}{s}\right)$

$\tilde{f}$ is well-defined.

For $\frac{r}{s}, \frac{r'}{s'} \in S^{-1}R$

$$\tilde{f}\left(\frac{r}{s}+\frac{r'}{s'}\right) = \tilde{f}\left(\frac{s'r+sr'}{ss'}\right)$$

$$= f(ss')^{-1} f(s'r+sr')$$

$$= f(s)^{-1} f(s')^{-1} \left[f(s') f(r) + f(s) f(r') \right]$$

$$= f(s)^{-1} f(r) + f(s')^{-1} f(r')$$

$$= \tilde{f}\left(\frac{r}{s}\right) + \tilde{f}\left(\frac{r'}{s'}\right)$$

Illy $\tilde{f}\left(\frac{r}{s} \cdot \frac{r'}{s'}\right) = \tilde{f}\left(\frac{r}{s}\right) \tilde{f}\left(\frac{r'}{s'}\right)$

For $r \in R$ $\tilde{f} \circ \varphi(r) = \tilde{f}\left(\frac{r}{1}\right) = f(1)^{-1} f(r) = f(r)$

$\Rightarrow \tilde{f} \circ \varphi = f$

Finally $\tilde{f}$ is unique: Let $h : S^{-1}R \to A$ be another ring homo. s.t. $h \circ \varphi = f$.

Let $\frac{r}{s} \in S^{-1}R$ $\quad h\left(\frac{r}{s}\right) = h\left(\frac{r}{1} \cdot \frac{1}{s}\right) = h\left(\frac{r}{1}\right) h\left(\frac{1}{s}\right)$

$$= h \circ \varphi(r) \cdot h\left(\frac{s}{1}\right)^{-1}$$

$$= f(r) \cdot \left(h \circ \varphi(s)\right)^{-1}$$

$$= f(r) f(s)^{-1}$$

$$= \tilde{f}\left(\frac{r}{s}\right)$$

$\Rightarrow h = \tilde{f}$ ∎

Lecture 18: Ideals in Localization, Local rings

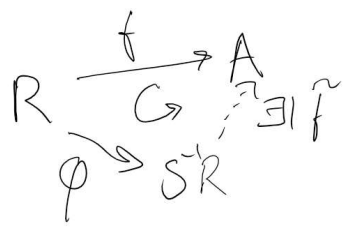
13 October 2020
13:32

(*) Let R be a comm ring with unity and S a mult. subset of R. Then $\varphi(s)$ is a unit in $S^{-1}R$ $\forall s \in S$. Here $\varphi : R \to S^{-1}R$ is the natural map.

$$r \longmapsto \frac{r}{1}$$

Thm (Universal property of Localization):
Let R be comm ring with unity. $S \subseteq R$ be a mult. subset of R. Let

$f : R \to A$ be a ring homomorphism where A is a comm ring with unity such that $\forall s \in S$, $f(s)$ is a unit in A. Then $\exists!$ ring homo. $\tilde{f} : S^{-1}R \to A$ s.t. $\tilde{f} \circ \varphi = f$.



(*) $0 \in S \Rightarrow S^{-1}R = \{0\}$

(*) $\forall s \in S$ nonzero divisor $\Leftrightarrow \varphi : R \to S^{-1}R$ is injective

(*) $\ker(\varphi) = \{r \in R \mid sr = 0 \text{ for some } s \in S\}$.

(*) Let R be an integral domain, a field K is called the field of fractions of R if R is a subring of K and no proper subfield of K contains R.

(*) R an int domain and $S = R \setminus \{0\}$ then $\varphi : R \to S^{-1}R$ is injective ring homo & $S^{-1}R$ is the field of fractions of R where we identify R with $\varphi(R)$.

(*) $\mathbb{Z}[\pi]$, $\mathbb{Z}[x]$, $\mathbb{Z}[e]$ are isom rings
$\mathbb{Q}(\pi)$, $\mathbb{Q}(x)$, $\mathbb{Q}(e)$ are their fraction fields

More formally, let R be an integral domain. The field of fractions of R is an injective ring homo. $i: R \hookrightarrow K$ s.t. K is a field and for any subfield K_0 of K containing $i(R)$, $K_0 = K$.

(*) $\mathbb{Z}[\sqrt[3]{2}] \subseteq \mathbb{Q}(\sqrt[3]{2})$ s.t. $\mathbb{Q}(\omega\sqrt[3]{2})$

$\mathbb{Z}[\omega\sqrt[3]{2}]$

$\mathbb{Z}[x]/(x^3-2)$

(*) Field of fraction is unique upto unique isomorphism. i.e.

i.e. $R \xrightarrow{i} K$, $R \xrightarrow{i'} K'$ are field of fractions

$\exists!\, f: K \to K'$ s.t. f is an isom. & $f \circ i = i'$

(*) S consist of units then

$\varphi: R \to S^{-1}R$ is an isomorphism.

$r \mapsto \frac{r}{1}$

Pf: $id: R \to R$ is a ring homo.

$id(s) = s$ is a unit $\forall\, s \in S$.

Universal prop of localization $\Rightarrow \exists!\, \widetilde{id}$ s.t.

$R \xrightarrow{id} R$, $R \xrightarrow{\varphi} S^{-1}R \xrightarrow{\widetilde{id}} R$, $\frac{r}{s} \mapsto \frac{r}{s}$, $\frac{1}{s} \mapsto s$

$\widetilde{id} \circ \varphi = id$

φ is injective ($\because \widetilde{id} \circ \varphi$ is injective)

Let $\frac{r}{s} \in S^{-1}R$ then

$\frac{r}{s} = \frac{r}{1} \cdot \frac{1}{s} = \frac{r}{1} \cdot \frac{s^{-1}}{1} = \varphi(r)\varphi(s^{-1})$

Note $s^{-1} \in R$.

Ex: R a comm ring with unity, $x \in R$; $S = \{1, x, x^2, \ldots\}$

Then $S^{-1}R = R[\frac{1}{x}] \cong \frac{R[z]}{(xz-1)}$

Notation

where $R[z]$ is the polynomial ring over R.

Pf: $\phi : R \longrightarrow \frac{R[z]}{(xz-1)}$

$r \longmapsto \bar{r}$

$$R \xrightarrow{i} R[z] \xrightarrow{q} \frac{R[z]}{(xz-1)}$$

$\phi = q \circ i$

Note: $\phi(x)\,\bar{z} = \bar{x}\,\bar{z} = \bar{1}$ $\left(\because xz - 1 \in (xz-1)\right)$

$\Rightarrow$ $\phi(x)$ is a unit in $\frac{R[z]}{(xz-1)}$

$\Rightarrow \exists\, \tilde{\phi} : S^{-1}R \longrightarrow \frac{R[z]}{(xz-1)}$ s.t.

$\tilde{\phi}(\frac{r}{s}) = \phi(s)^{-1}\phi(r)$ $\quad \forall\, s \in S$

$= \bar{z}^n \bar{q}_1$

Note $s = x^n$ for some n.

$$\alpha : R[z] \longrightarrow S^{-1}R$$

$$z \longmapsto \frac{1}{x}$$

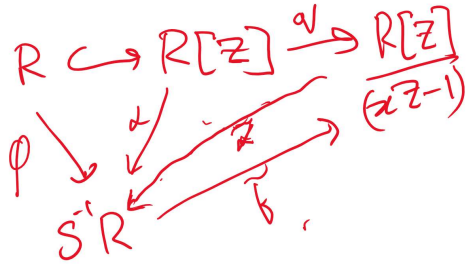
$$a_n z^n + a_{n-1} z^{n-1} + \dots + a_0 \longmapsto \frac{a_n}{x^n} + \frac{a_{n-1}}{x^{n-1}} + \dots + \frac{a_1}{x} + \frac{a_0}{1}$$

where $a_i \in R$

α is a ring homo. $\left(\because \alpha(p(z)) = p\left(\frac{1}{x}\right) \right)$

$$\alpha(xz - 1) = \frac{x}{x} - \frac{1}{1} = 0$$

$$\Rightarrow (xz-1) \subseteq \ker(\varphi)$$



$\tilde{\alpha} \circ q = \alpha$, $\alpha \circ i = \varphi$

$\tilde{f} \circ \varphi = q \circ i \; (= f)$

1st isom. $\Rightarrow$

$$\tilde{\alpha} : \frac{R[z]}{(xz-1)} \longrightarrow S^{-1}R$$

$$\tilde{\alpha}\left(\overline{p(z)}\right) \longmapsto \alpha(p(z)) = p\left(\frac{1}{x}\right)$$

Check: $\tilde{\alpha} \circ \tilde{f}\left(\frac{r}{s}\right) = \tilde{\alpha}\left(\overline{z^n}\, r\right) = r\,\frac{1}{x^n}$

$\left(s \in S \Rightarrow s = x^n \text{ for some } n \right)$

$$= \frac{r}{s}$$

$$\tilde{f} \circ \tilde{\alpha}\left(\overline{p(z)}\right) = \tilde{f}\left(p\left(\frac{1}{x}\right)\right) = \tilde{f}\left(\frac{a_n}{x^n} + \frac{a_{n-1}}{x^{n-1}} + \dots + \frac{a_0}{1}\right)$$

where $p(z) = a_n z^n + \dots + a_0$

$$= \tilde{f}\left(\frac{a_n + a_{n-1}x + \dots + a_0 x^n}{x^n}\right)$$

$$= \overline{z^n}\left(\overline{a_n} + \overline{a_{n-1}}\,\overline{x} + \dots + \overline{a_0}\,\overline{x^n}\right)$$

$$= \overline{a_n}\,\overline{z^n} + \overline{a_{n-1}}\,\overline{z^{n-1}} + \dots + \overline{a_1}\,\overline{z} + \overline{a_0}$$

$$= \overline{p(z)}$$

∎

Local rings: A comm ring with unity is called a local ring if it has exactly one maximal ideal.

Examples: 1) Fields
2) valuation rings
3) $\mathbb{Z}/4\mathbb{Z}$, More generally $\mathbb{Z}/p^n\mathbb{Z}$ $n \geq 1$ & p prime are local rings

$R = \mathbb{Z}$, $S = \{1, 2, 2^2, \dots\}$

$S^{-1}R = \mathbb{Z}\left[\frac{1}{2}\right] \subseteq \mathbb{Q}$

$\| \quad \left\{ \frac{a}{b} \mid b = 2^n \text{ for some } n \right\}$

4) $R = \mathbb{Z}$, $S = \{\text{odd integers}\} = \mathbb{Z} \setminus 2\mathbb{Z}$

$S^{-1}R = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, b \text{ odd} \right\} = \mathbb{Z}_{(2)}$

$\mathbb{Z} \subseteq S^{-1}R \subseteq \mathbb{Q}$

(2)

$2S^{-1}R$ is the maximal ideal of $S^{-1}R$.
$\|$
$\mathbb{Z}_{(2)}$

So $S^{-1}R$ is local ring

Lecture 19: Local rings and Ideals in Localization

15 October 2020
13:11

(*) R a comm ring with unity. S a mult. set. We constructed a ring homo $\varphi: R \to S^{-1}R := \{\frac{r}{s} \mid r \in R, s \in S\}$ where $\frac{r}{s} = \frac{r'}{s'}$ if $\exists u \in S$ s.t. $u(s'r - sr') = 0$

($*$) R int domain then $\mathrm{frac}(R) = S^{-1}R$ where $S = R \setminus \{0\}$.

(**) $R[\frac{1}{x}] := S^{-1}R \cong \frac{R[z]}{(xz-1)}$ where $S = \{1, x, x^2, \dots\}$ for $x \in R$

Eg: $S_1 = \{1, 30, 30^2, \dots\}$, $S_2 = \{1, 2, 3, 5, 2^{n_2}3^{n_3}5^{n_5} ; n_2, n_3, n_5 \geq 0\}$

$\subseteq \mathbb{Z}$. $S_1^{-1}\mathbb{Z}$, $S_2^{-1}\mathbb{Z}$

$\mathbb{Z}[\frac{1}{30}] \subseteq \mathbb{Q}$

$S_1^{-1}\mathbb{Z} = S_2^{-1}\mathbb{Z}$ as subsets of $\mathbb{Q}$ ✓

$\frac{a}{2^{n_2}3^{n_3}5^{n_5}} = \frac{a\,2^{n-n_2}3^{n-n_3}5^{n-n_5}}{30^n}$ $n > n_2, n_3, n_5$

(*) A comm ring with unity is called a local ring if it has exactly one maximal ideal.

Example: R a ring. $P \subseteq R$ a prime ideal. Then $S = R \setminus P$ is a mult. set. Then $S^{-1}R = \{\frac{r}{s} \mid r, s \in R, s \notin P\}$ is a local ring with the unique maximal ideal of $S^{-1}R$ $PS^{-1}R = \{\frac{r}{s} \mid r \in P, s \notin P\}$ $= S^{-1}P$

Pf: $\frac{x_1}{s_1}, \frac{x_2}{s_2} \in PS^{-1}R$ then $\frac{x_1}{s_1} + \frac{x_2}{s_2} = \frac{s_2x_1 + s_1x_2}{s_1s_2} \in PS^{-1}R$ & $\frac{r}{s} \cdot \frac{x_1}{s_1} = \frac{rx_1}{ss_1} \in PS^{-1}R$

$\frac{r}{s} \notin PS^{-1}R$ then $r \notin P \Rightarrow \frac{s}{r} \in S^{-1}R \Rightarrow \frac{r}{s} \cdot \frac{s}{r} = 1_{S^{-1}R} \Rightarrow \frac{r}{s}$ is a unit in $S^{-1}R$

Hence $PS^{-1}R$ is the maximal ideal of $S^{-1}R$. ∎

$S^{-1}R$ is also denoted by R_P.

Prop: Let R be a comm ring with unity and m a maximal ideal of R. TFAE

1) R is a local ring.
2) The set of nonunits of R form the ideal m.
3) If x is a unit $\forall\, x \in m$.

Pf: (1) $\Rightarrow$ (2): Let J = set of non units in R.

Let $x \in J$, $(x) = I \subsetneq R$ ($\because x$ is nonunit

So $\exists$ a max ideal of R containing I (and hence x). But (1) $\Rightarrow I \subseteq M$.

Hence $x \in M$. i.e. $J \subseteq M$

$M \subseteq J$ (trivial since M is a proper ideal)

$M = J$.

(2) $\Rightarrow$ (3): If $1+x$ is not a unit then

by (2) $1+x \in M$ ($\because$ M contains all non units)

And $x \in M \Rightarrow 1 \in M$ a contradiction

$\Rightarrow$ $1+x$ is a unit.

(3) $\Rightarrow$ (1): Let $M' \subseteq R$ be another maximal ideal. Let $x \in M$

$\Rightarrow$ $ax \in M \Rightarrow a \in R$

$\Rightarrow$ $1+ax$ is a unit $\forall\, a \in R$

$\Rightarrow$ $x \in \mathrm{Jac}(R)$

$\Rightarrow$ $x \in M'$

$\Rightarrow$ $M \subseteq M'$

$\Rightarrow$ $M = M'$

Ideals of $S^{-1}R$: $\varphi : R \to S^{-1}R$; $\varphi(P)$ need not be an ideal.

$r \mapsto \frac{r}{1}$

Ex: $\mathbb{Z} \hookrightarrow \mathbb{Q}$

$2\mathbb{Z}$ $\quad$ $2\mathbb{Z}$ not a $\mathbb{Q}$-ideal

(*) $\varphi(P)S^{-1}R = S^{-1}P := PS^{-1}R := \left\{ \frac{r}{s} \mid r \in P \ \& \ s \in S \right\}$

LHS $= \left(\frac{r}{1} \mid r \in P \right)$ $\quad \frac{r}{1} \in S^{-1}P \ \forall \ r \in P$

$\Rightarrow \varphi(P)S^{-1}R \subseteq S^{-1}P$

$\frac{r}{s} \in S^{-1}P$; $\frac{r}{s} = \frac{r}{1} \cdot \frac{1}{s}$

$\Rightarrow \frac{r}{s} \in \varphi(P)S^{-1}R$

(*) Let R be comm ring with unity & S a mult. subset. $\varphi : R \to S^{-1}R$ the nat' map.

Let $I \subseteq S^{-1}R$ be an ideal then

$J = \varphi^{-1}(I)$ is an ideal of R.

1) If I is a proper ideal $J \cap S = \phi$.

2) $(\varphi(J)) = JS^{-1}R = I$

Caution! $J \subseteq R$ ideal then $\varphi^{-1}(JS^{-1}R) \neq J$.

Pf: (1) Let $x \in J \cap S$ then $\varphi(x) \in I$ but $x \in S \Rightarrow \varphi(x)$ is a unit $\Rightarrow I = S^{-1}R$.

(2) Let $x \in \varphi(J) \Rightarrow \exists y \in J$ s.t. $x = \varphi(y) \Rightarrow x \in I$. "$\varphi^{-1}(I)$"

$\Rightarrow (\varphi(J)) \subseteq I$.

Let $x \in I \Rightarrow x = \frac{r}{s}$ $r \in R$ & $s \in S$

$\Rightarrow \frac{s}{1} \cdot \frac{r}{s} \in I$

$\Rightarrow \frac{r}{1} \in I$

$\Rightarrow r \in J$

$\Rightarrow \frac{r}{1} \in \varphi(J) \Rightarrow x = \frac{r}{s} = \frac{1}{s} \cdot \frac{r}{1} \in (\varphi(J))$

$\Rightarrow I \subseteq (\varphi(J))$.

Example: Every ideal in $S^{-1}R$ is of the form $JS^{-1}R$ for some R-ideal J.

1) $R = \mathbb{Q}[X, Y]$, $S = \{1, X, X^2, \dots\}$

$J_1 = (X)$ then $J_1 S^{-1}R = S^{-1}R$ | $S^{-1}R = \mathbb{Q}[X, Y, \frac{1}{X}]$

$J_2 = (X, Y)$ then $J_2 S^{-1}R = S^{-1}R$

$J_3 = (X+1)$ $\quad J_3 S^{-1}R = \left\{ \frac{(X+1) f(X,Y)}{X^n} \;\middle|\; n \geq 0,\ f(X,Y) \in R \right\}$

$J_4 = (XY)$, $J_5 = (X^2 Y)$

$J_4 S^{-1}R = (Y)$, $J_5 S^{-1}R = (Y)$

$\varphi^{-1}(J_4 S^{-1}R) = (Y)\,\mathbb{Q}[X, Y]$

Lecture 20: Gauss' lemma

16 October 2020
12:50

Defn: Let R be an int dom (which admits gcd) & $f(x) = a_n x^n + a_{n-1}x^{n-1} + \dots + a_0 \in R[x]$ be a nonzero poly. Then content of f denoted by $c(f) = \gcd(a_n, a_{n-1}, \dots, a_0)$.

Note $c(f)$ is defined upto an associate, i.e. $c = c(f)$ iff $uc = c(f)$ for any unit $u \in R$.

Also $d = \gcd(a_0, \dots, a_n)$ if $d \mid a_i$ $\forall\, 0 \le i \le n$ and if $d' \in R$ be s.t. $d' \mid a_i$ $0 \le i \le n \Rightarrow d' \mid d$.

Gauss' Lemma

version 1: Let R be a UFD and $f(x), g(x) \in R[x]$ then

$$c(fg) = c(f)c(g)$$

i.e. $d = \gcd(\text{coeff of } fg)$, $d_1 = \gcd(\text{coeff of } f)$, $d_2 = \gcd(\text{coeff of } g)$

$d \sim d_1 d_2$

version 2: Let R be a UFD & $K = QF(R)$. Let $f(x) \in R[x] \subseteq K[x]$.

If $f(x) = g(x)h(x)$ for some $g, h \in K[x]$

then $f(x) = G(x)H(x)$ for some $G, H \in R[x]$ with

$\deg(G) = \deg(g)$ & $\deg(H) = \deg(h)$

Cor: Let R be a UFD & $K = QF(R)$. A poly $f(x) \in R[x]$ of content 1 is irreducible in $R[x]$ iff $f(x)$ is irred in $K[x]$. (A poly of content 1 is called a primitive poly)

Pf: ($\Leftarrow$) $f(x)$ is reducible in $R[x] \Rightarrow f(x) = g(x)h(x)$ where $g(x), h(x) \in R[x] \subseteq K[x]$ are non units.

Since $c(f) = 1$, $g(x)$ and $h(x)$ are non constant poly. Hence they are non units in $K[x]$. Hence $f(x)$ is reducible in $K[x]$.

Conversely, $f(x)$ is reducible in $K[x] \Rightarrow f(x) = g(x)h(x)$ $g(x), h(x) \in K[x]$ are nonconst. poly. Hence by Gauss' lemma $f(x)$ is reducible in $R[x]$.

version 1 $\Rightarrow$ version 2 :

Let $g(X) = b_m X^m + b_{m-1} X^{m-1} + \dots + b_1 X + b_0$ and

$h(X) = c_\ell X^\ell + c_{\ell-1} X^{\ell-1} + \dots + c_1 X + c_0$ where b's & c's $\in K$

collecting denominator $\exists\, b, c \in R$ s.t.

$G_1(X) = bg(X) \in R[X]$ & $H_1(X) = ch(X) \in R[X]$

Hence $bc\, f(X) = G_1(X) H_1(X)$ in $R[X]$

($\because f(X) = g(X)h(X)$)

version 1 $\Rightarrow$ $bc\, c(f) = c(G_1)\, c(H_1)$ ---- (*)

say $b_i = \frac{b_i'}{b_i''}$, $b_i', b_i'' \in R$, $b = \prod_{i=0}^{m} b_i''$

Now $G_1(X) = c(G_1)\, G(X)$ for some $G(X) \in R[X]$

& $H_1(X) = c(H_1) H(X)$ " " $H(X) \in R[X]$

and $f(X) = c(f) F(X)$ " " $F(X) \in R[X]$

$bc\, f(X) = G_1(X) H_1(X) \Rightarrow$

$bc\, c(f) F(X) = c(G_1)\, c(H_1)\, G(X) H(X)$

(*) $\Rightarrow$ $F(X) = G(X) H(X)$

$\cdot c(b) \Rightarrow$ $f(X) = \underbrace{c(f) G(X)}_{\in R[X]} H(X)$ & $\deg(c(f) G(X)) = \deg g(X)$

& $\deg(H(X)) = \deg h(X)$

(Gauss' original result)

(*) A primitive poly $f(X) \in \mathbb{Z}[X]$

is $g(X) h(X)$ for some $g, h \in \mathbb{Q}[X]$

Then $f(X) = G(X) H(X)$ in $\mathbb{Z}[X]$

with $\deg G = \deg g$ &

$\deg H = \deg h$.

Pf of version 1:

Let $f(X) = g(X)h(X)$ for $f, g, h \in R[X]$

$g(X) = c(g)\,G(X)$, $h(X) = c(h)\,H(X)$ for some $G, H \in R[X]$

So $f(X) = c(g)c(h)\,G(X)H(X)$

Hence $c(g)c(h) \mid c(f)$

Let $c(g)c(h) = p_1 \cdots p_n$ where $p_i \in R$ are irreducible.

$\Rightarrow$ $c(f) = p_1 \cdots p_n q_1 q_2 \cdots q_m$ for some $m \geq 0$

$q_i \in R$ are irred.

Suppose $m \neq 0$ then q_1 exist.

$c(f) = c(g)\,c(h)\,d$ for some $d \in R$

Also $f(x) = c(f)\,F(X)$ for some $F[x] \in R[X]$

$c(f)F(X) = c(g)\,c(h)\,G(X)H(X)$

$dF[x] = G(X)H(X)$ where G, H are primitive. and $d = q_1 \cdots q_m$

$q_1 \mid G(X) H(X)$

$G(X) = b_m X^m + b_{m-1} X^{m-1} + \cdots + b_0$

$H(X) = c_\ell X^\ell + c_{\ell-1} X^{\ell-1} + \cdots + c_0$

Let i_0 be the smallest integer s.t. $q_1 \nmid b_{i_0}$

j_0 " " " " " $q_1 \nmid c_{j_0}$

Note $i_0 \leq m$ & $j_0 \leq \ell$. ($\because G, H$ are primitive)

Consider the coeff of $X^{i_0+j_0}$ in

$G(X) H(X)$. $a = b_{i_0} c_{j_0} + b_{i_0+1} c_{j_0-1} + \cdots + b_{i_0+j_0} c_0$

$+ \quad b_{i_0-1} c_{j_0+1} + \cdots + b_0 c_{i_0+j_0}$.

By hyp $q_1 \mid a$. Also q_1 divides all the terms except $b_{i_0} c_{j_0}$.

Hence $q_1 \mid b_{i_0} c_{j_0}$. This contradicts that q_1 is prime element of R

(as $q_1 \nmid b_{i_0}$ & $q_1 \nmid c_{j_0}$ but q_1 is irred element of a UFD.)

∎

Lecture 21: Applications of Gauss' lemma, Noetherian rings

27 October 2020
16:06

Recall: Gauss' Lemma

version 1: Let R be a UFD and $f(x), g(x) \in R[x]^*$ then

$$c(fg) = c(f)c(g)$$

version 2: Let R be a UFD & $K = QF(R)$. Let $f(x) \in R[x] \subseteq K[x]$.

If $f(x) = g(x)h(x)$ for some $g, h \in K[x]$

then $f(x) = G(x)H(x)$ for some $G, H \in R[x]$ with

$\deg(G) = \deg(g)$ & $\deg(H) = \deg(h)$. In fact $G = ag$, $H = bh$ where $a, b \in K^*$.

Cor: Let R be a UFD & $K = QF(R)$. A poly $f(x) \in R[x]$ of content 1 is irreducible in $R[x]$ iff $f(x)$ is irred in $K[x]$.

Example: 1) $f(x) = 3x - 6 \in \mathbb{Z}[x]$ $\quad f(x) = 3(x-2)$ is red in $\mathbb{Z}x$.

But in $\mathbb{Q}[x]$ $f(x)$ is irred.

2) $\mathbb{Q}[x,y]$, $\mathbb{Q}(x)[y]$ where $\mathbb{Q}(x)$ is fraction field of $\mathbb{Q}[x]$

$f(x,y) = 3y^3 + 2xy^2 + 7y + 3x + 5$

Is $f(x,y)$ irred?

$f(x,y) \in \mathbb{Q}(y)[x]$ $\quad R = \mathbb{Q}[y]$, $K = \mathbb{Q}(y)$

$(2y^2+3)x + 3y^3 + 7y + 5$ is irred in $\mathbb{Q}(y)[x]$

$\gcd(2y^2+3,\ 3y^3+7y+5) = 1$ ($\because 2y^2+3$ is irred. & $2y^2+3 \nmid 3y^3+7y+5$)

Gauss' Lemma $\Rightarrow$ f is irred in $\mathbb{Q}[x,y]$

Gauss' Lemma $\Rightarrow$ " " " " $\mathbb{Q}(x)[y]$ (here $R = \mathbb{Q}[x]$, $R[y] = \mathbb{Q}[x,y]$)

(*) Note $f(x) = g_1 \cdots g_n$ in $K[x]$ in version 2 then

$f(x) = G_1 \cdots G_n$ in $R[x]$ where $G_i = a_i g_i$ for some $a_i \in K^*$

Thm: Let R be a UFD then $R[X]$ is a UFD.

Pf: Let $K = QF(R)$ and $f(X) \in R[X]$. Assume $f(X)$ is nonzero nonunit.

Then $f(X) = c(f)F(X)$ for some $F(X) \in R[X]$

Since R is a UFD, $\forall\, c(f) = p_1 \cdots p_r$ product irred in R (this exists since R is a UFD)

if $c(f)$ is not a unit

$F(X) \in R[X] \subseteq K[X]$ and $K[X]$ is a UFD.

Hence $F(X) = g_1(X) \cdots g_s(X)$ where $g_1, \dots, g_s \in K[X]$ are irred.

if $F(X)$ is non constant.

By Gauss' lemma

$F(X) = G_1(X) \cdots G_s(X)$ where $G_i(X) \in R[X]$ and $\deg g_i = \deg G_i$ in fact $G_i(X)$ are irred in $K[X]$ as g_i are irred & $G_i \sim g_i$ in $K[X]$ (associate)

Also $c(F) = 1$

version 1 $\Rightarrow$ $c(G_1)\, c(G_2) \cdots c(G_s) = 1 \Rightarrow c(G_i) = 1$

$\Rightarrow$ G_i's are primitive poly irred in $K[X]$.

Cor to Gauss' lemma $\Rightarrow$ G_i's are irred in $R[X]$.

Also p_i's are irred in $R \Rightarrow p_i$'s are irred in $R[X]$.

Hence $f(X) = p_1 \cdots p_r G_1(X) \cdots G_s(X)$ can be written as a product of irred elements of $R[X]$.

For Uniqueness, suppose $f(x) = q_1(x) \cdots q_t(x)$ be product of irred in $R[x]$.

Since $q_i(x) \in R[x]$ are irred. and

$q_i(x) = c(q_i)\, Q_i(x)$ for some $Q_i(x) \in R[x]$

either $c(q_i) = 1$ or $Q_i(x) = 1$, i.e. $q_i(x)$ is a const or q_i is a primitive poly.

Let $q_1, \dots, q_n$ be const. & $q_{n+1}, \dots, q_t$ be primitive poly

then $c(f) = q_1 \cdots q_n$ (Gauss' lemma $\Rightarrow q_{n+1} \cdots q_t$ is prim poly)

But R is a UFD $\Rightarrow n = r$ & after reordering

$p_i \sim q_i$ in $R \Rightarrow p_i \sim q_i$ in $R[x]$

Also $F(x) = q_{n+1}(x) \cdots q_t(x) = G_1(x) \cdots G_s(x)$

and $q_{n+i}(x)$ are irred in $K[x]$

(Gauss' lemma & q_{n+i}'s are irred prim poly in $R[x]$)

Hence $t = n+s$ ($= r+s$) & after reordering

$q_{n+i} \sim G_i$ in $K[x]$ for $1 \le i \le s$

i.e. $q_{n+i} = u_i G_i$ for some $u_i \in K \setminus \{0\}$, $u_i = \frac{a_i}{b_i}$, $a_i, b_i \in R$, $b_i \neq 0$

But q_{n+i} & G_i are primitive in $R[x]$

$\Rightarrow u_i$ is a unit in R.

$\Rightarrow q_{n+i} \sim G_i$ in $R[x]$.

$b_i\, q_{n+i} = a_i G_i$

$b_i = c(b_i q_{n+i}) = c(a_i G_i) = a_i$

i.e. $b_i \sim a_i$ in R

$\Rightarrow u_i = \frac{a_i}{b_i}$ is a unit in R

∎

Noetherian Rings

Prop: Let R be a commutative ring with unity. The following are equivalent:

(1) Every R-ideal is finitely generated.

(2) Every increasing chain of R-ideals is eventually constant.

i.e. $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$ be a seq of R-ideals then $\exists N$ s.t. $\forall n \geq N \;\; I_n = I_N$.

(3) Every non-empty collection of R-ideals has a maximal element. w.r.t inclusion

Def^n A ring satisfying the above equivalent conditions is called a noetherian ring.

Examples: Fields, PID. Hilbert basis thm: R is noeth $\Rightarrow R[x]$ is noeth.

(*) Localization of noetherian is noetherian.

(**) R is noeth I R-ideal then R/I is noeth.

(***) $R_1, \ldots, R_n$ noeth. $\Rightarrow R_1 \times \cdots \times R_n$ is noeth.

Proof of the proposition:

(1) $\Rightarrow$ (2): Let $I_0 \subseteq I_1 \subseteq \cdots$ be inc seq of R-ideals

$I = \bigcup_{n \geq 0} I_n$ is an ideal of R.

By (1) $I = (x_1, \ldots, x_m)$ for some $m \geq 1$ & $x_1, \ldots, x_m \in R$.

So $x_i \in I = \bigcup_{n \geq 0} I_n$

$\Rightarrow x_i \in I_{n_i}$ $\quad n_i \geq 0 \quad 1 \leq i \leq m$

Then take $N = \max\{n_i \mid 1 \leq i \leq m\}$

$I \subseteq I_N$ $\quad (\because x_i \in I_N \;\; \forall \, 1 \leq i \leq m)$

$\Rightarrow I_N = I = I_n \quad \forall \; n \geq N.$

(2) $\Rightarrow$ (3): Let Ω be a nonempty collection of R-ideals. Suppose Ω has no maximal element.

Let $I_0 \in \Omega$. Since I_0 is not maximal element of Ω

$\exists\, I_1 \in \Omega$ s.t. $I_0 \subsetneq I_1$

continue this way to construct a seq of R-ideals

$$I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq I_3 \cdots$$

But this contradicts (2).

③ ⇒ ①: Let

$I \subseteq R$ be an ideal

Let $x_0 \in I$

If $I_0 = (x_0) = I$ then done

otherwise let $x_1 \in I \setminus I_0$.

Let $I_1 = (x_0, x_1) \subseteq I$

again if $I_1 = I$ then done

otherwise let $x_2 \in I \setminus I_1$ &

$I_2 = (x_0, x_1, x_2)$. Continuing this way, we construct a collection of ideals $I_0, I_1, I_2, \ldots$

If this process doesn't stop then $\Omega = \{ I_k \mid k \geq 0 \}$ is a nonempty collection of ideals no maximal element.

$(\because I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \cdots)$

contradicting ③ ∎

Lecture 22: Hilbert basis theorem; Modules

02 November 2020
16:46

Recall:

Noetherian Rings

Prop: Let R be a commutative ring with unity. The following are equivalent:

(1) Every R-ideal is finitely generated.

(2) Every increasing chain of R-ideals is eventually constant.

i.e. $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$ be a seq of R-ideals then $\exists N$ s.t. $\forall n \geq N \;\; I_n = I_N$.

(3) Every non-empty collection of R-ideals has a maximal element. w.r.t inclusion

Def^n A ring satisfying the above equivalent conditions is called a noetherian ring.

Examples: Fields, PID. Hilbert basis thm: R is noeth $\Rightarrow R[x]$ is noeth.

(*) Localization of noetherian is noetherian.

(*) R is noeth I R-ideal then R/I is noeth.

(*) $R_1, \ldots, R_n$ noeth. $\Rightarrow R_1 \times \cdots \times R_n$ is noeth.

(*) Let R be noeth ring and S be a mult. subset of R.

Let $I \subseteq S^{-1}R$ be an $S^{-1}R$-ideal.

We know that $I = S^{-1}J$ where $J = \varphi^{-1}(I)$ is an R-ideal $\varphi: R \to S^{-1}R$

But R is noeth $\Rightarrow \exists\, x_1, \ldots, x_n \in J$ s.t. $J = (x_1, \ldots, x_n)$

Claim: $I = \left(\frac{x_1}{1}, \ldots, \frac{x_n}{1}\right)$ is $S^{-1}R$.

$\alpha \in I$ then $\alpha = \frac{x}{s}$ for some $x \in J$ & $s \in R$.

But $x = r_1 x_1 + \cdots + r_n x_n \quad r_1, \ldots, r_n \in R$

$\Rightarrow \alpha = \frac{x}{s} = \frac{r_1}{s}\frac{x_1}{1} + \cdots + \frac{r_n}{s}\frac{x_n}{1}$ & note $\frac{r_i}{s} \in S^{-1}R \;\; \forall 1 \leq i \leq n$

Hence the claim.

Hence $S^{-1}R$ is noeth.

(*) R noeth & $J \subseteq R/I$ an ideal of R/I where I is an R-ideal.

Then $J = \widetilde{J}/I$ where $\widetilde{J}$ is an R-ideal containing I.

But R noeth $\Rightarrow \widetilde{J} = (x_1, \ldots, x_n)$ for some $x_1, \ldots, x_n \in \widetilde{J}$

$\Rightarrow J = (\bar{x}_1, \ldots, \bar{x}_n)$. Hence R/I is noeth.

(*) $R = R_1 \times \cdots \times R_n$ where R_i's are noeth and $I \subseteq R$ is an ideal. Then

$$I = I_1 \times \cdots \times I_n \quad \text{where } I_j \subseteq R_j \text{ is an ideal } 1 \le j \le n$$

Since $I_1, \ldots, I_n$ are f.g., hence I is f.g.

$I_j = (x_{jk} \mid 1 \le k \le n_j)$ then I is gen by

$$\{(x_{1k_1}, x_{2k_2}, \ldots, x_{nk_n}) \mid 1 \le k_j \le n_j\}$$

Hence R is noeth.

Ex: $\underbrace{\mathbb{Q}[x_1, x_2, \ldots, x_n]}_{R_n} \subseteq \underbrace{\mathbb{Q}[x_1, x_2, \ldots, x_{n+1}]}_{R_{n+1}}$

$R = \bigcup_{n \ge 1} R_n$ is a ring which is

$= \mathbb{Q}[x_1, x_2, \ldots]$

not noetherian

Hilbert basis theorem Let R be a noetherian ring then $R[x]$ is also noetherian.

Pf: Let $I \subseteq R[x]$ be an ideal of $R[x]$.

Let $f_1(x) \in I$ be a nonzero poly of least degree n_1 and $I_1 = (f_1(x))$ be an $R[x]$-ideal

If $I_1 = I$ done.

otherwise $f_2(x) \in I \setminus I_1$ be of least degree n_2 and $I_2 = (f_1, f_2)$ be an $R[x]$-ideal and so on

$f_{i+1} \in I \setminus I_i$ be of least degree n_{i+1} & $I_{i+1} = (f_1, \ldots, f_{i+1})$

Let a_i be the leading coeff of f_i and $J = (a_1, a_2, \ldots)$ be a R-ideal. Since R is noetherian, $J = (a_1, \ldots, a_N)$ for some $N \geq 1$.

Claim: $I = (f_1, \dots, f_N)$

Pf: If not then f_{N+1} exist and $f_{N+1} \in I \setminus I_N$

where $I_N = (f_1, \dots, f_N)$.

$f_{N+1}(x) = a_{N+1} x^{n_{N+1}} +$ lower terms. (degree)

$a_{N+1} \in J = (a_1, \dots, a_N) \Rightarrow \exists b_i \in R$ s.t.

$a_{N+1} = b_1 a_1 + \dots + b_N a_N$

Also $n_{N+1} = \deg f_{N+1} \geq \deg f_i$ for $i < N+1$

Let $g(x) = f_{N+1}(x) - b_1 x^{n_{N+1} - n_1} f_1(x) - b_2 x^{n_{N+1} - n_2} f_2(x) - \dots - b_N x^{n_{N+1} - n_N} f_N(x)$

Since $(f_1, \dots, f_N) = I_N$ and $f_{N+1} \notin I_N$

$\Rightarrow g(x) \notin I_N$. Also $g(x) \in I$

So $g(x) \in I \setminus I_{N+1}$. Also $\deg(g(x)) < n_{N+1} = \deg f_{N+1}$

contradicting the choice of f_{N+1}.

Hence the claim & R is noetherian ∎

(*) Note $R[x]$ is noeth $\Rightarrow$ R noeth.

(*) Caution! Subring of noeth need not be noeth.

Example: $\mathbb{Q}[\pi, t] \subset \mathbb{C}$

π, t algebraically independent over $\mathbb{Q}$

t_1

Continue this way

$R = \mathbb{Q}[t_1, t_2, \ldots] \subseteq \mathbb{C}$

s.t. $\mathbb{Q}[t_1, t_2, \ldots, t_i] \cong \mathbb{Q}[X_1, \ldots, X_i]$

$R \cong \mathbb{Q}[t_1, t_2, \ldots]$ is not noeth.

Modules and submodules

② Given a comm ring with unity R, want to define R-modules.

④ In fact if R is field then R-modules are same as R-vector spaces

Def: Let R be a field. A R-vector space is a $(M, +, s, R)$ where $+$ is a binary operation on M and $s: R \times M \to M$ is a function

satisfying the following axioms

1) $(M, +)$ is an abelian group with identity 0_M.

2) $s(\alpha, x_1 + x_2) = s(\alpha, x_1) + s(\alpha, x_2)$ $\quad \forall \alpha \in R \ \& \ x_1, x_2 \in M$

3) $s(\alpha_1 + \alpha_2, x) = s(\alpha_1, x) + s(\alpha_2, x)$ $\quad \forall x \in M, \ \forall \alpha_1, \alpha_2 \in R$

4) $s(\alpha_1 \alpha_2, x) = s(\alpha_1, s(\alpha_2, x))$

5) $s(1, x) = x \quad \forall x \in M.$

If $\alpha \in R$ & $x \in M$ then $\alpha x \in M$, $\alpha x = s(\alpha, x)$

$(\alpha_1 + \alpha_2) \cdot x = \alpha_1 x + \alpha_2 x$

$(\alpha_1 \alpha_2) \cdot x = \alpha_1 \cdot (\alpha_2 \cdot x)$

Def: Let R be a ring. An **R-module** is a $(M, +, s, R)$ where $+$ is a binary operation on M and $s: R \times M \to M$ is a function

satisfying the following axioms

1) $(M, +)$ is an abelian group with identity 0_M.

2) $s(\alpha, x_1 + x_2) = s(\alpha, x_1) + s(\alpha, x_2)$ $\quad \forall \alpha \in R \ \& \ x_1, x_2 \in M$

3) $s(\alpha_1 + \alpha_2, x) = s(\alpha_1, x) + s(\alpha_2, x)$ $\quad \forall x \in M, \ \forall \alpha_1, \alpha_2 \in R$

4) $s(\alpha_1 \alpha_2, x) = s(\alpha_1, s(\alpha_2, x))$

5) $s(1, x) = x \quad \forall x \in M.$

If $\alpha \in R$ & $x \in M$ then $\alpha x \in M$, $\alpha x = s(\alpha, x)$

$(\alpha_1 + \alpha_2) \cdot x = \alpha_1 x + \alpha_2 x$

$(\alpha_1 \alpha_2) \cdot x = \alpha_1 \cdot (\alpha_2 \cdot x)$

Ex: 1) R a field then R-modules are R-vs

2) $R = \mathbb{Z}$ then $M = \mathbb{Z}$ then $s: R \times M \to M$ is the usual multi of integers then M is a R-mod.

More generally R a ring then $(R, +)$ is an R-mod. as well.

③ $R \subseteq R'$ then any R'-mod is an R-mod.

Lecture 23: Modules, submodules, linear maps

04 November 2020
23:47

Def: Let R be a commutative ring with unity. An **R-module** is a $(M, +, s, R)$ where $+$ is a binary operation on M and $s: R \times M \to M$ is a function

satisfying the following axioms

1) $(M, +)$ is an abelian group with identity 0_M.
2) $s(\alpha, x_1 + x_2) = s(\alpha, x_1) + s(\alpha, x_2)$ $\quad \forall \alpha \in R \ \& \ x_1, x_2 \in M$
3) $s(\alpha_1 + \alpha_2, x) = s(\alpha_1, x) + s(\alpha_2, x)$ $\quad \forall x \in M, \ \forall \alpha_1, \alpha_2 \in R$
4) $s(\alpha_1 \alpha_2, x) = s(\alpha_1, s(\alpha_2, x))$
5) $s(1, x) = x \quad \forall x \in M.$

$\alpha \in R$ & $x \in M$ then $\alpha x \in M$, $\alpha x = s(\alpha, x)$

$(\alpha_1 + \alpha_2) \cdot x = \alpha_1 x + \alpha_2 x$ ←

$(\alpha_1 \alpha_2) \cdot x = \alpha_1 \cdot (\alpha_2 \cdot x)$ ←

$1 \cdot x = x$

Ex: 1) R a field then R-modules are R-vs

2) $R = \mathbb{Z}$ then $M = \mathbb{Z}$ then $s: R \times M \to M$ is the usual multi of integers then M is an R-mod.

More generally R a ring then $(R, +)$ is an R-mod. as well.

3) $R \subseteq R'$ then any R'-mod is an R-mod.

M is an R-module where R is a ring.

Facts: 1) $0_R \cdot m = 0_M \quad \forall m \in M \quad (s(0_R, m) = 0_M)$

2) $r \cdot 0_M = 0_M \quad \forall r \in R \quad (s(r, 0_M) = 0_M)$

$$0_R \cdot m = (0_R + 0_R) \cdot m = 0_R \cdot m + 0_R \cdot m$$
$$\Rightarrow 0_R \cdot m = 0_M \quad \text{Similarly 2)}$$

Example 3) R a ring, I an R-ideal. Then I is an R-module w.r.t usual multiplication as scalar multiplication.

Submodule and quotient module $(M,+,s)$

Def^n: Let R be a ring and M be an R-module.
An R-submodule N of M is a subset $N \subseteq M$ s.t. $(N, +, s_{|R\times N})$ is an R-module.

i.e. N is a subgroup of M and
$\forall\, r\in R \;\&\; n\in N,\ s(r,n)\in N$.

$\Updownarrow$

$r\cdot n \in N$ $\quad \forall\, n_1,n_2\in N,\ n_1+n_2 \in N$ and

(*) N is a R-submodule of M iff $\forall\, r\in R \;\&\; n\in N$ $r\cdot n\in N$

Example: 1) R is an R-module & I is an R-submodule of R.

2) $\{0_M\}$ and M are R-submod of M.

3) $m\in M$ and $Rm = \{rm \mid r\in R\}$ is an R-submod of M.

(*) Let M be a R-mod and I an R-ideal then
$IM = \{x_1m_1 + x_2m_2 + \cdots + x_nm_n \mid n\geq 1,\ x_1,\dots,x_n\in I \;\&\; m_1,\dots,m_n\in M\}$
is an R-submodule of M.

Pf: closed under addition is trivial.
Let $\alpha\in IM$ & $r\in R$ then
$\alpha = x_1m_1 + \cdots + x_nm_n$ for some $x_i\in I$ & $m_i\in M$ $1\leq i\leq n$

then $r\alpha = r(x_1m_1 + \cdots + x_nm_n)$
$= r(x_1m_1) + \cdots + r(x_nm_n)$
$= (rx_1)m_1 + \cdots + (rx_n)m_n$
$\in IM$ ($\because$ I is an ideal $\Rightarrow rx_i\in I$ $\forall\, 1\leq i\leq n$)

Quotient modules

Prop/Def^n: Let M be an R-mod & N be an R-submod. Then the abelian group M/N has a natural R-mod structure given by $r \cdot (m+N) = rm + N$. (M/N with this scalar multication is called the quotient of M by N.

Pf: WTS: $r \cdot (m+N) = rm + N$ is well-defined

Let $m, m' \in M$ be s.t. $m + N = m' + N$ & $r \in R$

$\Rightarrow m - m' \in N$

$\Rightarrow r(m-m') \in N$ ($\because$ N is an R-submod)

$\Rightarrow rm - rm' \in N$

$\Rightarrow rm + N = rm' + N$

Hence scalar multiplication is well-defined

Note M/N is an abelian grp

For $r_1, r_2 \in M$ & $m + N \in M/N$

$$\begin{aligned}(r_1 + r_2)\cdot(m+N) &= (r_1+r_2)m + N \\ &= (r_1 m + r_2 m) + N \\ &= (r_1 m + N) + (r_2 m + N) \\ &= r_1 \cdot (m+N) + r_2 (m+N)\end{aligned}$$

WTS check $r \cdot (m_1 + N + m_2 + N) = r(m_1+N) + r(m_2+N)$

$$(r_1 r_2)\cdot(m+N) = r_1 (r_2 (m+N))$$

$$1 \cdot (m+N) = 1m + N = m + N$$

In particular, M/IM is an R-mod $\forall$ R-mod M and R-ideal I.

Prop: Let M be an R-mod & I an R-ideal then M/IM is naturally an R/I-module where the scalar multiplication is given by:

$$R/I \times M/IM \xrightarrow{s} M/IM$$

$$(r+I,\ m+IM) \longmapsto rm+IM$$

$$(\bar{r},\ \bar{m}) \longmapsto \overline{rm} \qquad (\bar{r}\cdot\bar{m} = \overline{rm})$$

Pf: s is well-defined

Note $r\cdot(m+IM) = rm+IM$ is well-defined

Let $r+I = r'+I$ for $r, r' \in R$
& $m+IM = m'+IM$ for $m, m' \in M$

$\Rightarrow x := r-r' \in I$ & $m-m' \in IM$

WTS: $rm+IM = r'm'+IM$

$$rm - r'm' = (r-r')m + r'(m-m')$$
$$= \underset{\uparrow}{xm} + \underset{\uparrow}{r'(m-m')}$$
$$IM \qquad IM$$

($\because IM$ is a R-submod of M)

$\Rightarrow rm+IM = r'm'+IM$

Check that this is a module structure.

Lecture 24: Linear maps, Isomorphism theorems

06 November 2020
10:54

Recall: Modules, Submodules, Quotient modules over a ring R.

- $(M, +, s)$

Ex: $R = \mathbb{Z}$, $M = (\mathbb{Z}, +, \cdot)$ then every ideal is a submod of M, e.g. $n\mathbb{Z}$ $n \in \mathbb{Z}$. Then $\mathbb{Z}/n\mathbb{Z}$ is also a $\mathbb{Z}$-mod

$r \cdot [m]_n = [rm]_n$ $\quad r \cdot \overline{m} = \overline{rm}$

$r \cdot (m + nN) = rm + nN$

- The notion $\mathbb{Z}$-module is same as abelian groups.

  Let A be an abelian group then A has a natural $\mathbb{Z}$-mod str which is $n \cdot a = a + \dots + a$ if $n \geq 0$ e.w. $-a + \dots + -a$ if $n < 0$.

Def^n: Let R be a ring and M, N be R-modules. A map $\varphi : M \to N$ is called an R-linear map or an R-mod homo if φ is a group homo and $\varphi(r \cdot m) = r \cdot \varphi(m)$ $\forall r \in R$ & $m \in M$.

More precisely, $(M, +, s_1)$ & $(N, +, s_2)$ are R-mod then $\varphi(s_1(r, m)) = s_2(r, \varphi(m))$.

- $\varphi : M \to N$ is an R-lin map iff $\varphi(rm_1 + m_2) = r\varphi(m_1) + \varphi(m_2)$ $\forall r \in R$ & $\forall m_1, m_2 \in M$

Example 1) M an R-mod & N a submod then $i: N \hookrightarrow M$ is an R-lin map also called R-mod monomorphism.

$q: M \longrightarrow M/N$ is a R-lin map also an R-lin epimorphism. For $r \in R$ & $m \in M$

$$\begin{aligned} q(r \cdot m) &= rm + N \\ &= r \cdot (m+N) \quad (R\text{-mod str on } M/N) \\ &= r \cdot q(m) \end{aligned}$$

2) $R = \mathbb{Z}/6\mathbb{Z}$, Does $\mathbb{Z}$ have $\mathbb{Z}/6\mathbb{Z}$-mod str.?

$n \in \mathbb{Z}$ & $[1]$

$[1] \cdot n = n$

$\underbrace{([1] + [1] + \dots + [1])}_{6 \text{ times}} \cdot n = n + n + \dots + n$

$0 = [0] \cdot n = 6n$ contradiction.

$M = \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ $([a]_6, [b]_3) \in M$ then

$[r]_6 \in R$ then $[r]_6 \cdot ([a]_6, [b]_3) = ([ra]_6, [rb]_3)$

$N = \langle ([1]_6, [0]_3) \rangle$ then N is a submod

$M/N \cong \mathbb{Z}/3\mathbb{Z}$

(*) An R-lin map of R-mod is an isom if it is bijective.

$N_1 = \langle ([2]_6, [1]_3) \rangle$ then $M/N_1 \cong \mathbb{Z}/6\mathbb{Z} = \langle a \rangle$

$= \{ ([2]_6, [1]_3), ([4]_6, [2]_3), ([0]_6, [0]_3) \}$ $M/N_1 = \langle (\overline{1,0}) \rangle$

$[1]_6 \cdot a = a$ $[2] \cdot a = 2a$

Prop: Let $\varphi : M \to N$ be a R-lin map of R-mod

$\ker(\varphi)$ is an R-submod of M & $\operatorname{im}(\varphi)$ is an R-submod of N.

Pf:

Let $x, y \in \ker(\varphi)$

Enough to show: $rx + y \in \ker\varphi \quad \forall r \in R$

$$\varphi(rx+y) = r\varphi(x) + \varphi(y) = r0_N + 0_N = 0_N$$

So $\ker\varphi$ is an R-submod of M.

(ii) $x, y \in \operatorname{im}(\varphi)$ & $r \in R$ then

$$rx + y = r\varphi(x_1) + \varphi(y_1) \quad \text{for some } x_1, y_1 \in M$$
$$= \varphi(rx_1 + y_1)$$

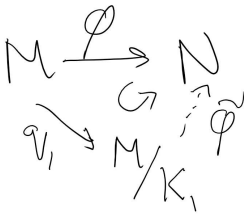
$\Rightarrow \operatorname{Im}(\varphi)$ is an R-submod of N

$\square$

Isomorphism theorems

First Isom thm

version 1: Let R be a ring. Let $\varphi: M \to N$ be an R-mod homo. Let $K = \ker(\varphi)$ and let $K_1 \subseteq K$ be an R-submod of K. Then K_1 is also an R-submod of M. There exist a unique R-lin map $\tilde{\varphi}: M/K_1 \to N$ s.t. $\tilde{\varphi} \circ q_1 = \varphi$ where $q_1: M \to M/K_1$



Pf: For $m \in M$ $\tilde{\varphi}(m + K_1) = \varphi(m)$ (i.e. $\tilde{\varphi}(q_1(m)) = \varphi(m)$)

So $\tilde{\varphi}$ is well-defined group homo follows from the 1st isom thm for groups. So we only need to check that $\tilde{\varphi}$ is R-lin.

For $r \in R$

$$\tilde{\varphi}(r \cdot (m + K_1)) = \tilde{\varphi}(rm + K_1) = \varphi(rm)$$
$$= r\varphi(m)$$
$$= r\tilde{\varphi}(m + K_1)$$

So $\tilde{\varphi}$ is R-lin. ∎

Cor: Let $\varphi: M \to N$ is an R-mod epimorphism then $\bar{\varphi}: M/\ker\varphi \to N$ is an isomorphism

2nd isomorphism thm

Let M be an R-mod.
Let N_1 and N_2 R-submod of M.

$$\frac{N_1 + N_2}{N_2} \cong N_1 / N_1 \cap N_2$$

Here $N_1 + N_2$ is the smallest submod of M containing N_1 & N_2. And $N_1 \cap N_2$ is also an R-submod of M.

(*) $N_1 + N_2 := \{ n_1 + n_2 \mid n_1 \in N_1 \text{ \& } n_2 \in N_2 \}$ is the smallest R-submod of M containing N_1 & N_2.

Easy to see $N_1 + N_2$ is closed under addition & scalar multi.

(**) Let N_α be R-submod of M
$\alpha \in \Omega$ indexing set. then
$\bigcap_{\alpha \in \Omega} N_\alpha$ is an R-submod of M.

Third isom thm: Let M be an R-mod, N be an R-submod of M and K be an R-submod of N then

$$M/N \cong \frac{M/K}{N/K}$$

One checks that N/K is a submod of M/K.

Lecture 25: Basics of linear maps.

10 November 2020
10:29

Recall: • R-linear maps $M \xrightarrow{\varphi} N$ are maps which send rm_1+m_2 to $r\varphi(m_1)+\varphi(m_2)$ $\forall r \in R$, $m_1, m_2 \in M$. ->

- $\ker(\varphi)$ & $\mathrm{Im}(\varphi)$ are submod of M and N resp.
- $N \subseteq M$ R-modules then $q: M \to M/N$ is R-lin
- Intersection of R-submod of an R-mod is an R-submod
- N_1, N_2 R-submod of M then $N_1+N_2 = \{n_1+n_2 \mid n_1 \in N_1 \ \& \ n_2 \in N_2\}$ is an R-submod of M.

- First isom thm $M \xrightarrow{\varphi} N$ φ R-lin then $M/\ker\varphi \cong \varphi(M)$
- Second isom thm $N_1, N_2 \subseteq M$ R-submod of M then $N_1+N_2/N_2 \cong N_1/N_1 \cap N_2$
- Third isom thm: $K \subseteq N \subseteq M$ be R-modules then

$$\left(M/K\right)\Big/\left(N/K\right) \cong M/N$$

⊛ Basics of linear maps

1) Let M, N be R-modules & $\varphi, \psi : M \to N$ be R-lin maps then (a) $\varphi + \psi : M \to N$ is an R-lin map.
$(\varphi+\psi)(m) = \varphi(m)+\psi(m)$

(b) For $r \in R$ $r\varphi : M \to N$ is an R-lin map
$m \mapsto r\varphi(m)$

2) Let M, N, K be R-mod $\varphi : M \to N$ & $\psi : N \to K$ be R-lin map then $M \xrightarrow{\psi\circ\varphi} K$ is R-lin.

Pf: Let $r \in R$ & $m_1, m_2 \in M$

a) $(\varphi+\psi)(rm_1+m_2) = \varphi(rm_1+m_2) + \psi(rm_1+m_2)$

$= r\varphi(m_1) + \varphi(m_2) + r\psi(m_1) + \psi(m_2)$

$= r(\varphi(m_1) + \psi(m_1)) + \varphi(m_2) + \psi(m_2)$

$= r(\varphi+\psi)(m_1) + (\varphi+\psi)(m_2)$

Hence $\varphi+\psi$ is R-lin

$r' \in R$, $r \in R$

b) $(r\varphi)(r'm_1+m_2) = r \cdot \varphi(r'm_1+m_2)$

$= rr'\varphi(m_1) + r\varphi(m_2)$

$= r'(r\varphi)(m_1) + (r\varphi)(m_2)$

$\Rightarrow r\varphi$ is R-linear.

(2) Let $m_1, m_2 \in M$ & $r \in R$

$\psi \circ \varphi(rm_1+m_2) = \psi(r\varphi(m_1) + \varphi(m_2))$

$= r\psi(\varphi(m_1)) + \psi(\varphi(m_2))$

$= r\psi\circ\varphi(m_1) + \psi\circ\varphi(m_2)$

So $\psi \circ \varphi$ is R-linear.

Cor: M, N R-modules. Let $\mathrm{Hom}_R(M,N)$ be the set R-lin maps from M to N. Then $\mathrm{Hom}_R(M,N)$ with addition of lin maps and scalar mult defined in ① is an R-mod.

Pf: Additive identity of $\mathrm{Hom}_R(M,N)$

$$0: M \longrightarrow N, \quad m \longmapsto 0 \qquad \forall\, m \in M$$ the zero map

φ R-lin then $-\varphi = -1 \cdot \varphi$ is also and $\varphi + -\varphi = 0$. So $\mathrm{Hom}_R(M,N)$ is a abelian group.

- $r_1, r_2 \in R$ & $\varphi \in \mathrm{Hom}_R(M,N)$

check: $(r_1+r_2)\varphi \overset{?}{=} r_1\varphi + r_2\varphi$

Let $m \in M$

$$\begin{aligned}((r_1+r_2)\varphi)(m) &= (r_1+r_2)\cdot\varphi(m) \\ &= r_1\varphi(m) + r_2\varphi(m) \\ &= (r_1\varphi)(m) + (r_2\varphi)(m)\end{aligned}$$

- $(r_1 r_2)\varphi = r_1(r_2\varphi)$ for $r_1, r_2 \in R$ & $\varphi \in \mathrm{Hom}_R(M,N)$
- $r(\varphi_1+\varphi_2) = r\varphi_1 + r\varphi_2$ $\forall r \in R$ & $\varphi_1, \varphi_2 \in \mathrm{Hom}_R(M,N)$

Cor: $\mathrm{End}_R(M)$ is a ring where M is an R-module.

Here $\mathrm{End}_R(M) := \mathrm{Hom}_R(M, M)$ and addition is as in (1) & multiplication is composition.

Pf: Exc

(*) Free modules

Example: $R = \mathbb{Z}$ & $M = \mathbb{Z}/5\mathbb{Z}$ is an R-module.

$\{[1]_5\} \subseteq M$ is a gen set of M.

$5[1]_5 = 0_M = [0]_5$ but $5 \in R$, $5 \neq 0$.

Def^n: • Let M be an R-mod. Let $S \subseteq M$ be a subset of M. The R-submod of M gen by S is the smallest R-submod of M containing S. This is denoted by $\langle S \rangle$.

We say S is a gen set of M if $\langle S \rangle = M$.

• An R-mod M is said to be f.g. if M is gen by a finite subset.

• An R-mod is called cyclic if it is gen by one element.

Prop: Let M be an R-mod and S be a subset of M. Then

$$\langle S\rangle = \underbrace{\left\{ r_1 m_1 + r_2 m_2 + \cdots + r_n m_n \;\middle|\; \begin{array}{l} \text{where } n \geq 1, \\ m_i \in S \ \& \\ r_i \in R \ \ 1 \leq i \leq n \end{array} \right\}}_{N}$$

Pf: Let N be the RHS.

Note that $S \subseteq N$.

Let $x, y \in N$ then

$x = r_1 m_1 + r_2 m_2 + \cdots + r_n m_n$ for some $r_i \in R$ & $m_i \in S$

$y = r_1' m_1' + r_2' m_2' + \cdots + r_{n'}' m_{n'}'$ for some $r_i' \in R$ & $m_i' \in S$

& $r \in R$

$$rx + y = r r_1 m_1 + r r_2 m_2 + \cdots + r r_n m_n + r_1' m_1' + r_2' m_2' + \cdots + r_{n'}' m_{n'}'$$

$$\in N$$

Hence $\langle S\rangle \subseteq N$.

Also if $m_1, \ldots, m_n \in S$ then $r_1 m_1 + \cdots + r_n m_n \in \langle S\rangle$ $\forall\, r_1, \ldots, r_n \in R$ since $\langle S\rangle$ is an R-submod of M. Hence $N \subseteq \langle S\rangle$.

∎

Free modules: A subset S of an R-module M is called a **basis of M** if S is a linearly independent gen set.

i.e. if $\sum_{i=1}^{n} r_i m_i = 0$ for some $n \geq 1$, $m_i \in S$ $\forall 1 \leq i \leq n$ & $r_i \in R$ $\forall 1 \leq i \leq n$

then $r_i = 0$ $\forall 1 \leq i \leq n$.

An R-module M is called a free module if it has a basis.

Eg: 1) $R = k[x,Y]$ k is a field. Give an example of a free R-module. Here R is a free R-module. R^n where scalar multiplication is component-wise is a free R-module $\forall n \geq 1$.

2) R any ring then R^n is a free R-mod.

(*) Every f.g. free R-mod is isomorphic to R^n for some n.

Pf: Let M be a f.g. free R-module. Then M has basis S containing n element for some $n \geq 1$.

$S = \{x_1, \ldots, x_n\}$

$\varphi : R^n \longrightarrow M$ φ is a well-defined.

$(r_1, \ldots, r_n) \longmapsto \sum_{i=1}^{n} r_i x_i$

$$\varphi\left(\underset{\sim}{r} + \underset{\sim}{r'}\right) = \sum_{i=1}^{n} (r_i + r_i') x_i \qquad \text{where } \underset{\sim}{r} = (r_1, \ldots, r_n), \ \underset{\sim}{r'} = (r_1', \ldots, r_n')$$

$$= \sum_{i=1}^{n} r_i x_i + \sum_{i=1}^{n} r_i' x_i$$

$$= \varphi(\underset{\sim}{r}) + \varphi(\underset{\sim}{r'})$$

Check for $a \in R$ & $\underset{\sim}{r} \in R^n$

$\varphi(a\underset{\sim}{r}) = a\varphi(\underset{\sim}{r})$

So φ is R-lin and $\ker(\varphi) = \left\{ \underset{\sim}{r} \mid \sum_{i=1}^{n} r_i x_i = 0 \right\}$

$= \{\underset{\sim}{0}\}$ $(\because \{x_i\}$ is a basis$\}$

& φ is surj, since S is a gen set.

Lecture 26: R[X]-module & R-linear Endomorp; Caley-Hamilton thm

11 November 2020
20:36

Recall: Let R be a comm ring with unity and M, N be R-mod

then 1) $\mathrm{Hom}_R(M,N)$ is an R-mod.

2) $\mathrm{End}_R(M)$ is an R-algebra (i.e. $\mathrm{End}_R(M)$ is a ring & there is a ring homo $R \to \mathrm{End}_R(M)$, $r \mapsto \mu_r : M \to M$, $m \mapsto rm$)

(*) Finitely generated R-modules

(**) Free modules. f.g. free R-mod is isom to R^n for some n.

(***) M, N are R-modules then $M \oplus N$ is an R-module via the scalar multip. $r \cdot (m,n) = (r \cdot m, r \cdot n)$

Example: 1) $R = \mathbb{Z}$, $M = \mathbb{Z}/5\mathbb{Z}$

$\mathrm{End}_{\mathbb{Z}}(M) = \mathrm{Hom}(\mathbb{Z}/5\mathbb{Z}, \mathbb{Z}/5\mathbb{Z}) \cong \mathbb{Z}/5\mathbb{Z}$ •

$f \longmapsto f(1)$

$\mathbb{Z} \longrightarrow \mathrm{End}_{\mathbb{Z}}(\mathbb{Z}/5\mathbb{Z}) \longrightarrow \mathbb{Z}/5\mathbb{Z}$

$1 \longmapsto \overline{1}$

2) $R = \mathbb{Q}$, $M = \mathbb{Q}^n$ then $\mathrm{End}_{\mathbb{Q}}(M) \overset{?}{\cong} M_{n\times n}(\mathbb{Q})$

$\mathbb{Q} \longrightarrow M_{n\times n}(\mathbb{Q})$

$r \longmapsto rI$

Facts: (*) M an R-mod then $\mathrm{Hom}_R(R, M) \cong M$

(**) M, N, K R-mod then $\mathrm{Hom}_R(M, N \oplus K) \cong \mathrm{Hom}_R(M,N) \oplus \mathrm{Hom}_R(M,K)$

and $\mathrm{Hom}(M \oplus N, K) \cong \mathrm{Hom}(M,K) \oplus \mathrm{Hom}(N,K)$

(***) $\mathbb{Q}$ is a $\mathbb{Z}$-module which is not free.

(****) R a comm ring with unity & S a mult subset of R then $S^{-1}R$ is an R-mod.

(*****) In fact $\varphi : R_1 \to R_2$ is a ring homo. then R_2 is a R_1-mod via for $r \in R_1$ & $m \in R_2$

$r \cdot m := \varphi(r) \cdot_{R_2} m$.

(X) Let R be a ring and M be an $R[x]$-mod where $R[x]$ is the poly ring over R.

Then note that M is also an R-module since R is a subring of $R[x]$.

Note $\varphi : M \to M$, $m \mapsto x \cdot m$ is a R-lin map.

$$\{R[x]\text{-modules}\} \underset{\Theta_2}{\overset{\Theta_1}{\rightleftarrows}} \{R\text{-modules} + \text{an } R\text{-lin endo of the module}\}$$

(X) Conversely let M be an R-mod & $\varphi \in \mathrm{End}_R(M)$ then

for $f(x) \in R[x]$ and $m \in M$ define

$f(x) = a_n x^n + a_{n-1}x^{n-1} + \dots + a_0$

$$f(x)\cdot m := a_n \cdot \varphi^n(m) + a_{n-1}\cdot \varphi^{n-1}(m) + \dots + a_1\varphi(m) + a_0 m$$

$$:= f(\varphi)(m)$$

Claim: This makes M into an $R[x]$-module

- $f(x), g(x) \in R[x]$ then

$$\begin{aligned}(f(x)+g(x))\cdot m &= (f+g)(\varphi)(m)\\ &= (f(\varphi)+g(\varphi))(m)\\ &= f(\varphi)(m) + g(\varphi)(m)\\ &= f(x)\cdot m + g(x)\cdot m\end{aligned}$$

Note that $x \cdot m = \varphi(m)$ and hence

$$\begin{aligned}x^2 \cdot m = x\cdot(x\cdot m) &= x\cdot\varphi(m)\\ &= \varphi(\varphi(m)) = \varphi^2(m)\end{aligned}$$

So more generally $f(x)\cdot m = f(\varphi)(m)$.

Hence $\Theta_2 \circ \Theta_1$ gives you isom objects. i.e. we recover the $R[x]$-module M.

Now going the other way, we start with R-mod M & $\varphi \in \mathrm{End}_R(M)$ then $R[x]$-mod str on M is defined so that $x \cdot m = \varphi(m)$.

And then from this $R[x]$-mod M we get linear map. by mult. by x. Hence the linear map is φ.

(*) If $\mu: R \longrightarrow \mathrm{End}_R(M)$ is injective then M is called a faithful

$r \longmapsto \mu_r : m \mapsto rm$

R-module.

(*) Let M be an R-mod $m \in M$, then annihilator of m,

$$\mathrm{ann}(m) = \{ r \in R \mid rm = 0_M \} \subseteq R \quad \text{is an } R\text{-ideal.}$$

Let $N \subseteq M$ be R-submod then annihilator of N,

$$\mathrm{Ann}(N) = \bigcap_{m \in N} \mathrm{ann}(m) = \{ r \in R \mid rm = 0 \ \forall m \in N \} \text{ is also an } R\text{-ideal.}$$

HW Show that M is a faithful R-mod iff $\mathrm{Ann}(M) = 0$.

Caley-Hamilton theorem: Let R be a ring and $A \in M_{n\times n}(R)$. Let $p_A(X) = \det(XI - A) \in R[X]$. Then $p_A(A) = 0$ in $\mathrm{End}_R(R^n)$.

Thm: Let M be a f.g. R-mod. and $\varphi \in \mathrm{End}_R(M)$ s.t. $\varphi(M) \subseteq IM$ where I is an R-ideal.

Then $\varphi^n + a_1\varphi^{n-1} + \dots + a_{n-1}\varphi + a_n = 0$ for some $a_i \in I^i$, $1 \le i \le n$.

Cor (Nakayama): Let M be f.g. R-module s.t $M = IM$ for some ideal $I \subseteq \mathrm{Jac}(R)$ then $M = 0$.

Lecture 27: Caley-Hamilton theorem, Nakayama's lemma

13 November 2020
10:45

Note $\varphi: M \to M$ is a R- in map.
$m \mapsto X \cdot m$

$\{R[X]\text{-modules}\} \xrightarrow[\theta_2]{\theta_1} \{R\text{-modules} + \text{an } R\text{-lin endo of the module}\}$

$X \cdot m := \varphi(m)$

$\mathrm{Hom}_R(R[X], R)$
$\cong$
$R\text{-mod} + \varphi: R[X] \to R$
$R[X]\text{-mod}$
$R\text{-mod} + \text{lin map} \mid \mathrm{End}_R(M)$

Caley-Hamilton theorem: Let R be a ring and $A \in M_{n\times n}(R)$. Let $p_A(X) = \det(XI - A) \in R[X]$. Then $p_A(A) = 0$ in $\mathrm{End}_R(R^n) = M_{n\times n}(R)$.

Thm: Let M be a f.g. R-mod. and $\varphi \in \mathrm{End}_R(M)$ s.t. $\varphi(M) \subseteq IM$ where I is an R-ideal.

Then $\varphi^n + a_1\varphi^{n-1} + \dots + a_{n-1}\varphi + a_n = 0$ for some $a_i \in \underbrace{I \cdot I \cdots I}_{i \text{ times}} = I^i \subseteq I$, $1 \le i \le n$.

Cor (Nakayama): Let M be f.g. R-module s.t. $M = IM$ for some ideal $I \subseteq \mathrm{Jac}(R)$ then $M = 0$.

Cor (Nakayama): Let (R, m) be a local ring and let M be a f.g. R-mod s.t. $M = mM$ then $M = 0$.

Pf: $M = IM$ where $I \subseteq \mathrm{Jac}(R)$ and M is f.g.
Take $\varphi = Id$ and apply the thm to conclude that

$I + a_1 I + a_2 I + \dots + a_n I = 0$ in $\mathrm{End}_R(M)$ where $a_i \in I$ $\forall\, 1 \le i \le n$

$\Rightarrow (1 + a)I = 0$ where $a = a_1 + \dots + a_n \in I$ in $\mathrm{End}_R(M)$

M is an R-mod $\Rightarrow \mu: R \to \mathrm{End}_R(M)$

So $(1+a)\cdot m = 0 \quad \forall\, m \in M$
But $1+a$ is a unit in R as $a \in I \subseteq \mathrm{Jac}(R)$

$\Rightarrow m = 0 \quad \forall\, m \in M.$
$\Rightarrow M = 0$

Pf of C-H thm:

$((a_{ij})) = A$ defines a linear map

$$\varphi_A : R^n \longrightarrow R^n$$
$$e_k \longmapsto \sum_{i=1}^{n} a_{ki} e_i$$

$e_k = (0, \dots, \underset{k^{th}\text{ spot}}{1}, \dots, 0)$

$$\varphi_A(e_k) = e_k A$$

So can make the R-mod R^n into an $R[X]$-mod via:

$$X \cdot e_k = \varphi_A(e_k) = \sum_{i=1}^{n} a_{ki} e_i \quad 1 \le k \le n$$

← zero of R^n

$$X \cdot e_1 - a_{11} e_1 - a_{12} e_2 - \dots - a_{1n} e_n = 0$$
$$-a_{21} e_1 + X \cdot e_2 - a_{22} e_2 - a_{23} e_3 \dots - a_{2n} e_n = 0$$

$$\vdots$$

$$-a_{n1} e_1 + \dots - a_{nn-1} e_{n-1} + X e_n - a_{nn} e_n = 0$$

$$(XI - A) \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = 0$$

$B = \mathrm{Adj}(XI - A) \in M_{n \times n}(R[X])$

$$B(XI - A) \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

← zero of R^n

$$\det(XI - A) \, I \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

$$\Rightarrow \det(x - IA)\, e_k = 0 \quad \forall 1 \le k \le n$$

$$\Rightarrow p_A(x) \cdot e_k = 0 \quad \forall 1 \le k \le n$$

$$\Rightarrow p_A(\varphi_A)(e_k) = 0 \quad \forall 1 \le k \le n$$

$$\Rightarrow e_k p_A(A) = 0 \quad \left(\because \varphi_A(e_k) = e_k A \right)$$

$$\forall 1 \le k \le n$$

$$\Rightarrow p_A(A) = 0 \quad \left(\because \{e_1, \dots, e_n\} \text{ gen } \mathbb{R}^n \right)$$

Pf of thm

We know M is f.g. R-mod

Let $\{e_1, \dots, e_n\}$ be gen set of M.

$\varphi : M \longrightarrow M$ R-linear

So this gives an $R[X]$-mod str on M

$$X \cdot m = \varphi(m) \quad \forall m \in M$$

$$\varphi(e_k) = X \cdot e_k = \sum_{j=1}^{n} a_{kj} e_j \quad 1 \le k \le n$$

Moreover

$$\varphi(M) \subseteq IM$$

$\Rightarrow$ we can choose $a_{kj} \in I$

$$X \cdot e_k \in IM$$
$$X \cdot e_k = \sum b_j m_j \quad b_j \in I$$
$$m_j = \sum_{l=1}^{n} \alpha_{jl} e_l$$

$$(XI - A) \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = \begin{pmatrix} 0_M \\ \vdots \\ 0_M \end{pmatrix}$$

$$\Rightarrow \quad p_A(x) \cdot e_k = 0 \quad \forall\ 1 \le k \le n$$

$$\Rightarrow \quad p_A(\varphi)(e_k) = 0 \quad \forall\ 1 \le k \le n$$

$$\Rightarrow \quad p_A(\varphi) = 0 \qquad \left(\because \{e_1, \dots, e_n\} \text{ gen } M \right)$$

$$p_A(x) = \det(xI - A)$$

$$= \det \begin{pmatrix} x - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & x - a_{22} & \cdots & -a_{2n} \\ \vdots & & & \\ -a_{n1} & \cdots & -a_{nn-1} & x - a_{nn} \end{pmatrix}$$

$$= x^n + a_1 x^{n-1} + \dots + a_n$$

$$a_1 \in I,\ a_2 \in I^2, \dots, a_n \in I^n$$

Lecture 28: Noetherian modules

18 November 2020
19:00

Def^n/Prop: Let R be a ring and M be an R-module. TFAE

(1) Every R-submodule of M is finitely generated.

(2) Every increasing chain of submodules of M is eventually constant
i.e. $M_0 \subseteq M_1 \subseteq \dots \subseteq M_n \subseteq \dots$ are R-submod of M
then $\exists N$ s.t. $M_n = M_N \ \forall n > N$.

(3) Every nonempty collection Ω of R-submod of M has a maximal element.

An R-mod M satisfying the above equivalent conditions is called a noetherian module.

Pf: (1) $\Rightarrow$ (2): Take $M_s = \bigcup_{i \geq 0} M_i$, M_s is f.g. by $m_1, \dots, m_k$. Take N s.t. $m_1, \dots, m_k \in M_N$.

(2) $\Rightarrow$ (3): $M_0 \in \Omega$ as $\Omega \neq \emptyset$. Lack of maximal element in Ω allows us to build a chain of strictly inc seq of R-submod of M.

(3) $\Rightarrow$ (1): Let M_0 be a submod of M. Take $m_1 \in M_0$, $M_1 = Rm_1$, $m_2 \in M_0 \setminus M_1$ if nonempty
$M_2 = Rm_1 + Rm_2$ and so on to construct $\Omega = \{M_i \mid i \geq 1\}$
a collection of R-submod of M without a maximal element
if M is not fin gen.

Examples: (1) R a noetherian ring then R as an R-module is noetherian.
Since every submod of R is an R-ideal.
In fact R as an R-mod is noetherian iff R is a noeth ring.

(2) $R = \mathbb{Z}$ then every f.g. $\mathbb{Z}$-mod is noeth. By str. thm
$\mathbb{Z}^r \oplus M$ where M is a finite abelian grp.

(3) R a ring M an R-mod s.t. M is a finite set then
M is noeth.

(4) $R = \mathbb{Z}$ then $\mathbb{Q}$ is not noetherian $\mathbb{Z}$-mod.
$\mathbb{Z} \times \mathbb{Z} \times \cdots$ infinite copies. are non noetherian R-mod

(*) M is a noeth R-mod then any R-submod of M is noeth.

(*) M a f.g. R-mod & N an R-submod of M then M/N is a f.g. R-mod.

Pf: Let $M = Rm_1 + \dots + Rm_n$ then $M/N = R\bar{m}_1 + \dots + R\bar{m}_n$

(*) M a noeth R-mod $\Rightarrow$ M/N is noeth & N submod

Pf: $\bar{K} \subseteq M/N$ is a submod then $\bar{K} = K/N$ for some R-submod K of M containing N.

Prop: R noeth ring and M a f.g. R-module then M is a noetherian R-module.

Pf: Let $m_1, \dots, m_n \in M$ s.t.

$$M = Rm_1 + \dots + Rm_n$$

Let $\varphi : R^n \longrightarrow M$

$$e_i \longmapsto m_i$$

$$(a_1, \dots, a_n) \longmapsto \sum_{i=1}^{n} a_i m_i \quad \text{for } a_i \in R$$

φ is surjective ✓ and R-linear.

Let $x \in R$ & $\underset{\sim}{a}, \underset{\sim}{b} \in R^n$

$$\varphi(x\underset{\sim}{a} + \underset{\sim}{b}) = \varphi((xa_1 + b_1, xa_2 + b_2, \dots, xa_n + b_n))$$

$$= \sum_{i=1}^{n} (xa_i + b_i) m_i$$

$$= \sum_{i=1}^{n} [x(a_i m_i) + b_i m_i]$$

$$= x \sum_{i=1}^{n} a_i m_i + \sum_{i=1}^{n} b_i m_i$$

$$= x\varphi(\underset{\sim}{a}) + \varphi(\underset{\sim}{b})$$

$\Rightarrow$ $M \cong R^n / \ker(\varphi)$ by 1st isom thm.

Hence enough to show R^n is noeth R-mod $\forall\ n \geq 1$.

Proof by induction. $n=1$ ✓ Since R is noeth some ring.

Assume R^{n-1} is a noeth R-mod for $n \geq 2$.

- $R^n = R^{n-1} \times R$. WTS every submod of R^n is f.g.

Let $M \subseteq R^n$ be a R-submod.

$R^{n-1} \subseteq R^n$ as $\{(a_1, \dots, a_{n-1}, 0) \mid a_i \in R\}$ is an R-submod of R^n.

$\pi : R^n \longrightarrow R$ is R-lin map

$(a_1, \dots, a_n) \longmapsto a_n$

$\ker(\pi) = R^{n-1} = \{(a_1, \dots, a_{n-1}, 0) \mid a_i \in R\}$

$M_1 = M \cap \ker(\pi) \subseteq R^{n-1}$ is a R-submod of R^{n-1}

M_1 is f.g. since R^{n-1} is noeth. say by $\{x_1, \dots, x_k\} \subseteq M$

$M_2 = \pi(M)$ is a submod of R. Hence M_2 is also f.g. R-mod say by $\{y_1, \dots, y_l\}$

Let $z_i \in M$ be s.t. $\pi(z_i) = y_i$ $1 \leq i \leq l$.

Claim: $\{x_1, \dots, x_k, y_1, \dots, y_l\}$ gen M.

Let $x \in M$ then

$\pi(x) \in M_2$

$$\Rightarrow \pi(x) = \sum_{i=1}^{l} a_i y_i \quad \text{for some } a_i \in R$$

$$\Rightarrow \pi(x) = \sum_{i=1}^{l} a_i \pi(y_i)$$

$$\Rightarrow \pi\left(x - \sum_{i=1}^{l} a_i y_i\right) = 0$$

$$x - \sum_{i=1}^{l} a_i y_i \in \ker(\pi) \cap M = M_1$$

$$\Rightarrow x - \sum_{i=1}^{l} a_i y_i = \sum_{j=1}^{k} b_j x_j \quad \text{for } b_j \in R, \ 1 \le j \le k$$

$$\Rightarrow x = \sum_{i=1}^{l} a_i y_i + \sum_{j=1}^{k} b_j x_j$$

Lecture 29: Localization of modules

20 November 2020
10:11

Recall: An R-module M is noetherian if all its submod are finitely generated.

(*) Submodules and quotient modules of noetherian modules are noetherian
⊙ Let M be an R-mod $N \subseteq M$ be noeth R-submod s.t. M/N is noeth then M is noeth.

(**) R a noetherian ring. An R-mod M is noetherian iff it is f.g.

Cor: R noeth ring. M a f.g. R-mod then any submod of M is f.g.

Example: $R = k[x_1, x_2, \dots]$ and $M = R$. Then M is generated by 1_R as an R-mod. But $I = (x_1, x_2, \dots) \subseteq M$ is not f.g. R-mod.

Localization of R-modules

Def^n/Prop: Let R be comm ring, $S \subseteq R$ be a mult set and M be an R-mod.

Define a relation on $S \times M = \{(s,m) \mid s \in S,\ m \in M\}$ as follows

$(s_1, m_1) \sim (s_2, m_2)$ if $\exists s \in S$ s.t. $s(s_1 m_2 - s_2 m_1) = 0_M$. ① Then $\sim$ is an equivalence relation. Let $\frac{m}{s}$ denote the equivalence class $[(s,m)]$ for $(s,m) \in S \times M$ and $S^{-1}M = S \times M / \sim$. ② Then $\frac{m_1}{s_1} \oplus \frac{m_2}{s_2} := \frac{s_2 m_1 + s_1 m_2}{s_1 s_2}$ is a well-defined binary operator on $S^{-1}M$. ③ The map $S^{-1}R \times S^{-1}M \xrightarrow{\sigma} S^{-1}M$, $\left(\frac{r}{s}, \frac{m}{s'}\right) \longmapsto \frac{rm}{ss'}$ is well-defined. ④ Moreover $S^{-1}M$ is a $S^{-1}R$-module via σ as the scalar multiplication. ⑤ In particular $S^{-1}M$ is an R-mod.

⑥ The map $\varphi : M \longrightarrow S^{-1}M$, $m \longmapsto \frac{m}{1}$ is an R-lin map.

Pf: $\sim$ is reflexive and symmetric follows trivially.

$(s_1, m_1) \sim (s_2, m_2)$ & $(s_2, m_2) \sim (s_3, m_3)$

$\exists u \in S$ & $v \in S$

$u \cdot (s_1 m_2 - s_2 m_1) = 0_M$ & $v \cdot (s_2 m_3 - s_3 m_2) = 0$

① ②

$s_3 v$ ① + $s_1 u$ ②

$s_3 u v s_1 m_2 - s_3 u v s_2 m_1 + s_1 u v s_2 m_3 - s_1 u v s_3 m_2 = 0$

$s_2 u v (s_1 m_3 - s_3 m_1) = 0$ $\quad s_2 u v \in S$

$\Rightarrow (s_1, m_1) \sim (s_3, m_3)$

② & ③ same as the ring case

For ④: • $S^{-1}M$ is an abelian group:

Note $\frac{0}{1} \oplus \frac{m}{s} = \frac{s \cdot 0 + 1 \cdot m}{s} = \frac{m}{s}$

So $\frac{0}{1}$ is the additive identity.

Assoc $\left(\frac{m_1}{s_1} \oplus \frac{m_2}{s_2}\right) \oplus \frac{m_3}{s_3} = \frac{s_2 m_1 + s_1 m_2}{s_1 s_2} \oplus \frac{m_3}{s_3}$

$= \frac{s_3 s_2 m_1 + s_3 s_1 m_2 + s_1 s_2 m_3}{s_1 s_2 s_3}$

$\frac{m_1}{s_1} \oplus \left(\frac{m_2}{s_2} \oplus \frac{m_3}{s_3}\right) = \frac{m_1}{s_1} \oplus \frac{s_3 m_2 + s_2 m_3}{s_2 s_3}$

$= \frac{s_2 s_3 m_1 + s_1 s_3 m_2 + s_1 s_2 m_3}{s_1 s_2 s_3}$

$\frac{-m}{s} \oplus \frac{m}{s} = \frac{0}{s^2} = \frac{0}{1}$

• $\frac{1}{1} \cdot \frac{m}{1} = \frac{1 \cdot m}{1 \cdot 1} = \frac{m}{1}$

• $\left(\frac{r_1}{s_1} + \frac{r_2}{s_2}\right) \cdot \frac{m}{s} = \frac{s_2 r_1 + s_1 r_2}{s_1 s_2} \cdot \frac{m}{s}$

$= \frac{s_2 r_1 m + s_1 r_2 m}{s_1 s_2 s}$

$\frac{r_1}{s_1} \cdot \frac{m}{s} + \frac{r_2}{s_2} \cdot \frac{m}{s} = \frac{r_1 m}{s_1 s} + \frac{r_2 m}{s_2 s}$

$= \frac{s_2 s r_1 m + s_1 s r_2 m}{s_1 s_2 s^2} = \frac{s(s_2 r_1 m + s_1 r_2 m)}{s(s_1 s_2 s)}$

$= \frac{s_2 r_1 m + s_1 r_2 m}{s_1 s_2 s}$

IIIly check

• $\frac{r}{s}\left(\frac{m_1}{s_1} + \frac{m_2}{s_2}\right) = \frac{r}{s} \cdot \frac{m_1}{s_1} + \frac{r}{s} \cdot \frac{m_2}{s_2}$

• $\frac{r_1}{s_1} \cdot \left(\frac{r_2}{s_2} \cdot \frac{m}{s}\right) = \frac{r_1 r_2 m}{s_1 s_2 s} = \left(\frac{r_1}{s} \cdot \frac{r_2}{s_2}\right) \cdot \frac{m}{s}$

Recall $R \longrightarrow S^{-1}R$ is a ring homo.

$r \longmapsto \frac{r}{1}$

Hence $S^{-1}M$ is an R-mod.

In fact $r \cdot \frac{m}{s} = \frac{r}{1} \cdot \frac{m}{s} = \frac{rm}{s}$.

Finally the map $\varphi : M \longrightarrow S^{-1}M$

$m \longmapsto \frac{m}{1}$

is R-lin. $\forall\, m_1, m_2 \in M$

$$\varphi(m_1 + m_2) = \frac{m_1 + m_2}{1} = \frac{m_1}{1} \oplus \frac{m_2}{1}$$
$$= \varphi(m_1) \oplus \varphi(m_2)$$

So φ is a grp homo.

For $r \in R$ & $m \in M$ $\quad \varphi(r \cdot m) = \frac{rm}{1} = r \cdot \frac{m}{1}$

$$= r\,\varphi(m)$$

So φ is R-mod homo.

Example: 1) $M = R$ then $S^{-1}M = S^{-1}R$ as an $S^{-1}R$-mod.

(2) $R = \mathbb{Z}$ and $M = \mathbb{Z} \times \mathbb{Z}/15$

(a) $S_3 = \{1, 3, 3^2, \dots\}$ $\leftarrow$ $S_3^{-1}M \cong \mathbb{Z}[\frac{1}{3}] \times \mathbb{Z}/5\mathbb{Z}$

(b) $S_{15} = \{1, 15, 15^2, \dots\}$ $S_{15}^{-1}M \cong \mathbb{Z}[\frac{1}{15}]$

(c) $S = \mathbb{Z} \setminus \{0\}$ $S^{-1}M \cong \mathbb{Q}$

$$S_3^{-1}\left(\mathbb{Z}/15\mathbb{Z}\right) = \left\{ \frac{[a]_{15}}{3^n} \;\middle|\; [a]_{15} \in \mathbb{Z}/15,\ n \geq 0 \right\}$$

Note $\frac{[1]}{1}$ has order 5 $\frac{[2]}{1}, \frac{[3]}{1}, \frac{[4]}{1}, \frac{[0]}{1}$

$\in S_3^{-1}\left(\mathbb{Z}/15\mathbb{Z}\right)$

given 3^n

$\frac{[1]}{9} \stackrel{?}{=} \frac{[4]}{1}$ $3^n[1-36] = 0$ in $\mathbb{Z}/15$

Let a be s.t

$a3^n \equiv 1 \pmod 5$

then $\frac{[1]}{3^n} = \frac{[a]}{1}$ $\frac{[b]}{3^n} = \frac{[ab]}{1}$

$$\mathbb{Z}/15\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$

(b) $\mathbb{Z}[\frac{1}{15}]$

(c) $\mathbb{Q}$

Lecture 30: Localization, rank, torsion

20 November 2020
16:04

Recall:

Localization of R-modules

Def^n/Prop: Let R be comm ring, $S \subseteq R$ be a mult set and M be an R-mod.

Define a relation on $S \times M = \{(s,m) \mid s \in S,\ m \in M\}$ as follows:

$(s_1, m_1) \sim (s_2, m_2)$ if $\exists s \in S$ s.t. $s(s_1 m_2 - s_2 m_1) = 0_M$. ① Then $\sim$ is an equivalence relation. Let $\frac{m}{s}$ denote the equivalence class $[(s,m)]$ for $(s,m) \in S \times M$ and $S^{-1}M = S \times M / \sim$. ② Then $\frac{m_1}{s_1} \oplus \frac{m_2}{s_2} := \frac{s_2 m_1 + s_1 m_2}{s_1 s_2}$ is a well-defined binary operator on $S^{-1}M$. ③ The map $S^{-1}R \times S^{-1}M \xrightarrow{\sigma} S^{-1}M$, $(\frac{r}{s}, \frac{m}{s'}) \mapsto \frac{rm}{ss'}$ is well-defined. ④ Moreover $S^{-1}M$ is a $S^{-1}R$-module via σ as the scalar multiplication. ⑤ In particular $S^{-1}M$ is an R-mod.

⑥ The map $\varphi : M \to S^{-1}M$, $m \mapsto \frac{m}{1}$ is an R-lin map.

Basic properties

⑦ R a ring, $S \subseteq R$ a mult subset. Let M, N be R-modules then $S^{-1}(M \times N) \cong S^{-1}M \times S^{-1}N$ as $S^{-1}R$-mod.

⑧ Note $\varphi\left(\frac{(m,n)}{s}\right) = \left(\frac{m}{s}, \frac{n}{s}\right)$ is well-defined $\varphi : S^{-1}(M \times N) \to S^{-1}M \times S^{-1}N$

$\frac{(m_1,n_1)}{s_1} = \frac{(m,n)}{s}$ in $S^{-1}(M \times N)$ $\Rightarrow \exists u \in S$ s.t. $u(s(m_1,n_1) - s_1(m,n)) = 0$ in $M \times N$

$\Rightarrow (u(sm_1 - s_1 m), u(sn_1 - s_1 n)) = 0$ in $M \times N$

$\Rightarrow u(sm_1 - s_1 m) = 0$ in M & $u(sn_1 - s_1 n) = 0$ in N

$\Rightarrow \frac{m_1}{s_1} = \frac{m}{s}$ in $S^{-1}M$ & $\frac{n_1}{s_1} = \frac{n}{s}$ in $S^{-1}N$

$\Rightarrow \left(\frac{m_1}{s_1}, \frac{n_1}{s_1}\right) = \left(\frac{m}{s}, \frac{n}{s}\right)$ in $S^{-1}M \times S^{-1}N$

φ is $S^{-1}R$-linear. (Check!) $\to \varphi\left(\frac{r}{s'} \cdot \frac{(m,n)}{s}\right) = \varphi\left(\frac{(rm, rn)}{s's}\right)$ for $\frac{r}{s'} \in S^{-1}R$ & $\frac{(m,n)}{s} \in S^{-1}(M \times N)$

$= \left(\frac{rm}{s's}, \frac{rn}{s's}\right)$

$= \frac{r}{s'} \cdot \left(\frac{m}{s}, \frac{n}{s}\right)$

$= \frac{r}{s'} \varphi\left(\frac{(m,n)}{s}\right)$

$\Psi : S^{-1}M \times S^{-1}N \to S^{-1}(M \times N)$, $\left(\frac{m}{s}, \frac{n}{s'}\right) \mapsto \frac{(s'm, sn)}{ss'}$

Check Ψ is well-defined

Check φ & Ψ are inverses to each other

$\Psi \circ \varphi\left(\frac{(m,n)}{s}\right) = \Psi\left(\left(\frac{m}{s}, \frac{n}{s}\right)\right) = \frac{(sm, sn)}{s^2} = \frac{(m,n)}{s} \Rightarrow \Psi \circ \varphi = id$

$\varphi \circ \Psi\left(\frac{m}{s}, \frac{n}{s'}\right) = \varphi\left(\frac{(s'm, sn)}{s's}\right) = \left(\frac{s'm}{s's}, \frac{sn}{ss'}\right) = \left(\frac{m}{s}, \frac{n}{s}\right) \Rightarrow \varphi \circ \Psi = id.$

(*) R, S as above, $I \subseteq R$ an ideal & $M = R/I$

$S^{-1}M \cong S^{-1}R/S^{-1}I$ as $S^{-1}R$-mod. $S^{-1}I = IS^{-1}R = \{\frac{x}{s} \mid x \in I, s \in S\}$

In particular if $I \cap S \neq \phi \Rightarrow S^{-1}(R/I) = 0$ $S = \{1, 3, 3^2, \dots\}$, $M = \mathbb{Z}/8\mathbb{Z}$

In fact more generally if N is a submod of an R-mod M. Then $S^{-1}(M/N) \cong S^{-1}M/S^{-1}N$

Pf: $\varphi : S^{-1}M \longrightarrow S^{-1}(M/N)$

$\frac{m}{s} \longmapsto \frac{\bar{m}}{s}$ where $\bar{m} = m + N$ in M/N

φ is well-defined: $\frac{m}{s} = \frac{m'}{s'} \Rightarrow \exists u \in S$ s.t. $u(s'm - sm') = 0$ in M

$\Rightarrow u(s'\bar{m} - s\bar{m}') = 0$ in M/N

($\because q : M \to M/N$ is R-lin map)

$\Rightarrow \frac{\bar{m}}{s} = \frac{\bar{m}'}{s}$ in $S^{-1}(M/N)$

check φ is $S^{-1}R$-lin (because q is) and surjective by definition.

$\ker(\varphi) = \{\frac{m}{s} \mid \frac{\bar{m}}{s} = \frac{0}{1} \text{ in } S^{-1}(M/N)\}$

$= \{\frac{m}{s} \mid \exists u \in S \quad u\bar{m} = 0 \text{ in } M/N\}$

$= \{\frac{m}{s} \mid \exists u \in S \quad um \in N\}$

Claim: $S^{-1}N \xrightarrow{i} S^{-1}M$ is injective, with image $\ker(\varphi)$. $S^{-1}R$-linear

$S \times N/\sim \ni (n, s) \longmapsto \frac{n}{s}$ $\quad S \times M/\sim$

Claim implies $S^{-1}N$ is an $S^{-1}R$-submod of $S^{-1}M$ and

By 1st isom thm $S^{-1}M/S^{-1}N \cong S^{-1}(M/N)$.

Pf of claim: $\frac{n}{s} = \frac{0}{1}$ in $S^{-1}M$ for $n \in N$ & $s \in S$

$\Rightarrow$ $\exists\, u \in S$ s.t. $un = 0$ in M.

$\Downarrow$

$un = 0$ in N

$\Rightarrow$ $\frac{n}{s} = \frac{0}{1}$ in $S^{-1}N$

Hence i is injective.

$i\left(\frac{n}{s} + \frac{n'}{s'}\right) = \frac{s'n + sn'}{ss'} = \frac{s'n + sn'}{ss'} = \frac{n}{s} + \frac{n'}{s'}$

well-defined

i is R-linear is tautological.

For $n \in N$ and $s \in S$, $\frac{n}{s} \in \ker(\varphi)$ as $1 \cdot n \in N$ Take $u = 1$

So $S^{-1}N = i(S^{-1}N) \subseteq \ker(\varphi)$.

Let $\frac{m}{s}$ be s.t. $um \in N$ for some $u \in S$ then

$\frac{m}{s} = \frac{um}{us} \in S^{-1}N$. Hence $\ker(\varphi) = S^{-1}N$ ∎

(*) $\varphi : N \longrightarrow M$ an R-mod homo

then $S^{-1}\varphi : S^{-1}N \longrightarrow S^{-1}M$ is an $S^{-1}R$-mod homo

$\frac{n}{s} \longmapsto \frac{\varphi(n)}{s}$

Exc

φ inj $\Rightarrow$ $S^{-1}\varphi$ inj

φ surj $\Rightarrow$ $S^{-1}\varphi$ surj

Rank of an R-mod for R an integral domain.

Def^n: Let R be an int domain and M be an R-mod.

Then $\operatorname{rank}(M) = \dim_{S^{-1}R}(S^{-1}M)$ where $S = R \setminus \{0\}$

$= \dim_K(S^{-1}M)$ where $S^{-1}R = K = \operatorname{frac}(R)$ as vector space

Example: ① $R = \mathbb{Z}$, $M = \mathbb{Z}^2 \oplus \mathbb{Q} \oplus \mathbb{Z}/15\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$

$\operatorname{rank}(M) = 3$

$S = R - \{0\}$

$S^{-1}M \cong S^{-1}\mathbb{Z} \oplus S^{-1}\mathbb{Z} \oplus S^{-1}\mathbb{Q} \oplus S^{-1}\mathbb{Z}/15S^{-1}\mathbb{Z} \oplus \frac{S^{-1}\mathbb{Z}}{9S^{-1}\mathbb{Z}}$

$\cong \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} = \mathbb{Q}^3$

$S^{-1}\mathbb{Q} \cong \mathbb{Q}$ check that this is an isom of $\mathbb{Q}$-vs.

$\frac{\kappa}{s} \longmapsto \frac{1}{s} \cdot \kappa$

$\frac{m/n}{s} = \frac{m}{ns}$ in $S^{-1}\mathbb{Q}$

② $R = \mathbb{Z}$, $M = 2\mathbb{Z}$, $\operatorname{rank}(M) = ?$

$S^{-1}M \cong \mathbb{Q}$ $\operatorname{rank}(M) = 1$

(*) $I \subseteq R$ is a nonzero ideal of an int domain R

then $\operatorname{rank}(I) = 1$

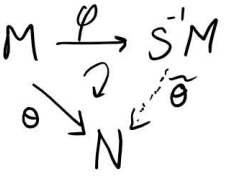
Universal property of Localization

M an R-mod & $S \subseteq R$ mult subset

$\varphi : M \to S^{-1}M$ φ is R-linear $S^{-1}M$ is $S^{-1}R$-mod

Let N be an $S^{-1}R$-mod then N has an R-mod structure via $r \cdot n = \frac{r}{1} \cdot n$

Let $\theta : M \to N$ which is R-linear then $\exists!$ $S^{-1}R$-lin map $\tilde{\theta} : S^{-1}M \to N$ s.t. $\tilde{\theta} \circ \varphi = \theta$



Pf: Claim: $\tilde{\theta}\left(\frac{m}{s}\right) := \frac{1}{s} \cdot \theta(m)$ is well-defined $S^{-1}R$-linear

$\frac{m}{s} = \frac{m'}{s'}$ in $S^{-1}M \Rightarrow \exists u \in S$ s.t. $u(s'm - sm') = 0$ in M

$\Rightarrow \theta(u(s'm - sm')) = 0$ in N

$\Rightarrow u(s'\theta(m) - s\theta(m')) = 0$ in N

$\overset{\frac{1}{u}}{\Rightarrow} s'\theta(m) - s\theta(m') = 0$ in N as u unit in $S^{-1}R$

$\overset{\frac{1}{ss'}}{\Rightarrow} \frac{1}{s}\theta(m) = \frac{1}{s'}\theta(m')$

check $\tilde{\theta}\left(\frac{m_1}{s_1} + \frac{r}{s}\frac{m_2}{s_2}\right) = \tilde{\theta}\left(\frac{m_1}{s_1}\right) + \frac{r}{s}\tilde{\theta}\left(\frac{m_2}{s_2}\right)$

check uniqueness $\alpha : S^{-1}M \to N$ s.t. $\alpha \circ \varphi = \theta$ then show $\alpha = \tilde{\theta}$

Def^n: Let R be ring & M be an R-mod.

$$T(M) = \{ m \in M : \exists\, r \in R,\ r \neq 0 \text{ \& } rm = 0 \}$$

$T(M)$ is a submod of M if R is an int domain.

M is called torsion free R-mod if $T(M) = 0$.

(**) Let R be an int domain M an R-mod then $M/T(M)$ is torsion free.

Pf: $r \cdot \bar{m} = 0$ in $M/T(M)$ $\quad r \neq 0$

$\Rightarrow \overline{rm} = 0$ in $M/T(M)$

$\Rightarrow rm \in T(M)$

$\exists \Rightarrow r' \in R,\ r' \neq 0$ s.t. $r'rm = 0$

$\Rightarrow m \in T(M$ $\quad (\because r'r \neq 0$ as R int dom)

$\Rightarrow \bar{m} = 0$

(**) R an int dom M an R-mod s.t. $M = T(M)$ then $\operatorname{rank}(M) = 0$.

Lecture 31: Structure theorem for f.g. modules over PID

25 November 2020
19:04

Def^n: Let R be an int domain and M be an R-mod.
Then $\operatorname{rank}(M) = \dim_{S^{-1}R}(S^{-1}M)$ where $S = R\setminus\{0\}$
$= \dim_K(S^{-1}M)$ where $K = \operatorname{frac}(R)$ as vector space

- $\operatorname{rank}(M)$ = size of the largest l.i. subset of M.

Def^n: Let R be ring & M be an R-mod.
$T(M) = \{m \in M : \exists\, r \in R,\ r \neq 0 \text{ & } rm = 0\} \iff \{m \in M \mid \operatorname{Ann}(m) \neq 0\}$
$T(M)$ is a submod of M if R is an int domain.
M is called torsion free R-mod if $T(M) = 0$.

(*) Let R be an int domain M an R-mod then $M/T(M)$ is torsion free.

such modules are called torsion modules

(**) R an int dom M an R-mod s.t. $M = T(M)$ then $\operatorname{rank}(M) = 0$.

Pf: Let $\alpha \in S^{-1}M$ then $\alpha = \frac{m}{s}$ for $m \in M$ & $s \in R\setminus\{0\}$
$\exists\ r \in R$ s.t. $rm = 0$ in M $\Rightarrow \alpha = \frac{m}{s} = \frac{rm}{rs}$ $(\because r \in R\setminus\{0\} \overset{''}{=} S)$
$= \frac{0}{rs} = \frac{0}{1}$

Hence $S^{-1}M = 0 \Rightarrow \operatorname{rank}(M) = 0$

(*) Even converse holds. Because $\operatorname{rank}(M) = 0 \Rightarrow S^{-1}M = 0$
$\Rightarrow \frac{m}{s} = \frac{0}{1}$ in $S^{-1}M$ $\forall\, m \in M$ & $s \in R\setminus\{0\}$
$\Rightarrow \frac{m}{1} = \frac{0}{1}$ in $S^{-1}M$
$\Rightarrow \exists\, r \in S \overset{''}{R\setminus\{0\}}$ s.t. $r(m-0) = 0 \Rightarrow rm = 0$
$\Rightarrow m \in T(M)$. $\forall\, m \in M$.

Thm (Str thm): Let R be a PID and M be a f.g. R-mod. Then

$$M \cong R^k \oplus R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m)$$

where $k = \text{rank}(M)$ and $a_1, \ldots, a_m \in R$ are nonzero nonunits s.t. $a_1 | a_2 | a_3 | \cdots | a_m$. Here k and m could be 0.

Cor: R a PID and M a f.g. torsion free R-mod then M is free R-mod.

Pf: $M \cong R^k \oplus R/(a_1) \oplus \cdots \oplus R/(a_m)$. But if $m \geq 1$ then $m_H(0, \bar{1}, 0, \ldots, 0) \in RHS$ then $a_1 m = a_1(0, \bar{1}, 0, \ldots, 0) = (0, 0, \ldots, 0)$. Contradicting M is torsion free.

Cor: Let G be a f.g. abelian group then

$$G \cong \mathbb{Z}^k \oplus \mathbb{Z}/a_1\mathbb{Z} \oplus \mathbb{Z}/a_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/a_m\mathbb{Z}$$ for some $n \geq 0$ and $a_1, \ldots, a_m \in \mathbb{Z}$ are s.t.

$$a_i | a_{i+1} \quad 1 \leq i \leq m-1.$$

Pf: $R = \mathbb{Z}$ then G is f.g. $\mathbb{Z}$-mod and apply str thm.

Cor: R a PID and M a submod of a f.g. free mod then M is free.

Pf: $M \subseteq R^n \Rightarrow M$ is also torsion free.

R noeth $\Rightarrow R^n$ is a noeth R-mod $\Rightarrow M$ is noeth R-mod.

Hence M is f.g. R-mod. ∎

Example: 1) $R = \mathbb{Z}[X]$ or $\mathbb{Q}[X, Y]$.

$M = (2, X)$ or $(X, Y) = M$

M is f.g. torsion free R-mod.

Is M free? Note $\operatorname{rank}(M) = 1$

But M is not a principal ideal.

$2, X$ are not l.i. as

$X \cdot 2 + (-2) \cdot X = 0$ in M.

2) R a PID. M torsion free $\overset{?}{\Rightarrow} M$ is free

Example: $\mathbb{Q}$ as a $\mathbb{Z}$-module

Let $S \subseteq \mathbb{Q}$ s.t. $|S| \geq 2$

then S is lin dep.

$sp\left(\frac{a}{s}\right) - \operatorname{Frac}(\mathbb{Z}) = 0$ & $\mathbb{Q} \cong \mathbb{Z}$.

Prop: Let R be a PID and F be a free R-module of rank n. Let N be a submodule of F. Then N is a free R-mod of rank $m \leq n$. Moreover there is a basis $x_1, \dots, x_n$ of F and $\exists\, a_1, \dots, a_m \in R^\times$ s.t. $a_1 | a_2 | \dots | a_m$ and $\{a_1 x_1, a_2 x_2, \dots, a_m x_m\}$ is a basis of N.

Prop $\Rightarrow$ str thm: Let M be a f.g. R-mod.

Let $m_1, \dots, m_n \in M$ s.t. $M = Rm_1 + \dots + Rm_n$.

$\Rightarrow$ $\varphi : F \longrightarrow M$, $e_i \longmapsto m_i$ where $F = R^n$ is a free mod of rank n and e_i's are std. basis vectors.

Then φ extends to R-lin surj map.

$$\varphi((b_1, \dots, b_n)) = \sum_{i=1}^{n} b_i m_i$$

We know φ is R-lin and since $\{m_i \mid 1 \leq i \leq n\}$ gen M, φ is surj.

$N = \ker(\varphi) \subseteq F$. By prop., $\exists$ $m \leq n$ a basis $\{x_1, \dots, x_n\}$ of F and $a_1, \dots, a_m \in R^\times$ s.t. $a_1 | a_2 | \dots | a_m$ and $\{a_1 x_1, a_2 x_2, \dots, a_m x_m\}$ is a basis of N.

$$N \subseteq F = Rx_1 \oplus Rx_2 \oplus \cdots \oplus Rx_n$$

$$\| $$

$$Ra_1x_1 \oplus Ra_2x_2 \oplus \cdots \oplus Ra_mx_m$$

$$M \cong F/N \quad \text{(by 1st isom thm)}$$

$$= \frac{Rx_1 \oplus Rx_2 \oplus \cdots \oplus Rx_n}{Ra_1x_1 \oplus Ra_2x_2 \oplus \cdots \oplus Ra_mx_m}$$

$$= Rx_1/Ra_1x_1 \oplus Rx_2/Ra_2x_2 \oplus \cdots \oplus Rx_m/Ra_mx_m \oplus Rx_{m+1} \oplus \cdots \oplus Rx_n$$

($\because$ $M_1, M_2, \ldots, M_n$ are R-mod & $N_i \subseteq M_i$ are R-submod then

$$M_1 \oplus M_2 \oplus \cdots \oplus M_n / N_1 \oplus N_2 \oplus \cdots \oplus N_n \cong M_1/N_1 \oplus M_2/N_2 \oplus \cdots \oplus M_n/N_n$$)

$$\cong R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m) \oplus R^{n-m}$$

($Rx_1 \overset{\alpha}{\cong} R$

$x_1 \longleftarrow 1$

$x_1 \longmapsto 1$

$\alpha(Ra_1x_1) = (a_1)$)

$a_1 | a_2 | \cdots | a_m \qquad a_i \in R^\times$.

Let $a_1, \ldots, a_r$ be units $r \le m$.

then $M \cong R/(a_{r+1}) \oplus \cdots \oplus R/(a_m) \oplus R^{n-m}$

and we get the sts thm by replacing m by m-r and a_i by a_{r+i}.

Finally note that $\operatorname{rank}(M) = \dim_{S^{-1}R}(S^{-1}M)$

where $S = R \setminus \{0\}$

$\Rightarrow S^{-1}(RHS) = (S^{-1}R)^{n-m}$

$\Rightarrow \operatorname{rank}(M) = n-m = k$.

Lecture 32: Structure theorem continued.

27 November 2020
10:22

Recall:

Thm (Str thm): Let R be a PID and M be a f.g. R-mod. Then

$$M \cong R^k \oplus R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m)$$

where $k = \operatorname{rank}(M)$ and $a_1, \ldots, a_m \in R$ are nonzero nonunits s.t. $a_1 | a_2 | a_3 | \cdots | a_m$. Here k and m could be 0.

Prop: Let R be a PID and F be a free R-module of rank n. Let N be a submodule of F. Then N is a free R-mod of rank $m \leq n$. Moreover there is a basis $x_1, \ldots, x_n$ of F and $\exists\, a_1, \ldots, a_m \in R^\times$ s.t. $a_1 | a_2 | \cdots | a_m$ and $\{a_1 x_1, a_2 x_2, \ldots, a_m x_m\}$ is a basis of N.

Prop $\Rightarrow$ str thm ✓

Pf of Prop: $N = 0$ ✓. So assume $N \neq 0$.

Let $\Sigma = \{\varphi(N) \mid \varphi : F \to R$ is R-linear map$\}$.

The Σ is a collection of ideals of R. Since R is noeth & Σ is nonempty, it has a maximal element say $\nu(N)$ for some $\nu : F \to R$ R-linear. i.e. $\nu \in \operatorname{Hom}_R(F, R)$.

$\nu(N)$ is a principal ideal generated by say a_1

i.e. $(a_1) = \nu(N) = a_1 R$.

Note $a_1 \neq 0$ $\left(\because \pi_i : F \longrightarrow R \quad 1 \leq i \leq n \right.$

$F = R^n$

$\left. \pi_i(N) = 0 \ \forall \ i \Rightarrow N = 0 \right)$

$\exists\, x \in N$ s.t. $\nu(x) = a_1$ ←

Claim: $a_1 \mid \varphi(x) \ \forall \ \varphi \in \mathrm{Hom}_R(F, R)$

Pf: Let $d = \gcd(a_1, \varphi(x))$

$d = r_1 a_1 + r_2 \varphi(x)$ for some $r_1, r_2 \in R$.

$\psi : F \longrightarrow R$ is R-lin

$\psi = r_1 \nu + r_2 \varphi$

$\Rightarrow \psi(N) \ni \psi(x) = r_1 \nu(x) + r_2 \varphi(x)$

$= d$

$\Rightarrow \psi(N) \in \Sigma$ & $a_1 \in (d)$

$\Rightarrow (a_1) = \nu(N) \subseteq (d) \subseteq \psi(N)$

By maximality of $\nu(N)$

$\Rightarrow (a_1) = (d)$

$\Rightarrow a_1 \mid \varphi(x)$.

$a_1 \mid \pi_i(x) \quad \forall\ 1 \le i \le n$ $\quad \pi_i : F \to R$ are projection maps.

Let $b_i = \pi_i(x) \quad 1 \le i \le n$

$b_i = a_1 c_i \quad 1 \le i \le n$ for some $c_i \in R$

Note $x = \sum b_i e_i = \sum_{i=1}^{n} a_1 c_i e_i$ where e_i are the std basis $F = R^n$.

$= a_1 \sum_{i=1}^{n} c_i e_i$

Let $x_1 = \sum_{i=1}^{n} c_i e_i \Rightarrow a_1 x_1 = x$

Claim: (i) $F = R x_1 \oplus \ker(\nu)$

(ii) $N = R a_1 x_1 \oplus (\ker(\nu) \cap N)$

Let $y \in F$ then

$y = \underbrace{\nu(y) x_1}_{R x_1} + \underbrace{y - \nu(y) x_1}_{\in \ker(\nu)}$

$\nu(y - \nu(y) x_1)$

$= \nu(y) - \nu(y)\,\nu(x_1)$

$\left(\because a_1 = \nu(x) = \nu(a_1 x_1) = a_1 \nu(x_1) \Rightarrow \nu(x_1) = 1 \ (\because a_1 \neq 0) \right)$

$= 0$

$\Rightarrow F = R x_1 + \ker(\nu)$

Let $y \in R x_1 \cap \ker(\nu)$

$\Rightarrow y = r x_1$ for some $r \in R$

& $\nu(y) = 0 \Rightarrow \nu(r x_1) = 0$

$\Rightarrow r\,\nu(x_1) = 0 \Rightarrow r = 0 \ (\because \nu(x_1) = 1)$

$\Rightarrow y = 0$. Hence (i)

$y \in N$ then

$$y = v(y)x_1 + y - v(y)x_1$$

$$v(y - v(y)x_1) = v(y) - v(y)v(x_1) = 0 \quad (\because v(x_1)=1)$$

$$\Rightarrow \quad y - v(y)x_1 \in \ker(v)$$

So enough to show $v(y)x_1 \in Ra_1x_1$

$$\left(\because \quad Ra_1x_1 = Rx \subseteq N \;\&\; y \in N \Rightarrow y - v(y) \in N\right)$$

$$v(y) \in v(N) \quad (\because y \in N)$$

$$\| \; a_1R$$

$$\Rightarrow v(y)x_1 \in a_1Rx_1 = Ra_1x_1$$

$$\Rightarrow N = Ra_1x_1 + (\ker(v) \cap N)$$

$$y \in Ra_1x_1 \cap (\ker(v) \cap N)$$

$$\Rightarrow y = ra_1x_1 \quad \text{for some } r \in R$$

and $v(y) = 0 \Rightarrow v(ra_1x_1) = 0$

$$\Rightarrow ra_1 = 0 \text{ in } R$$

$$\Rightarrow r = 0 \cdot (\because a_1 \neq 0)$$

$$\Rightarrow y = 0 \cdot \text{ Hence (ii)} \cdot$$

Note that $N = Ra_1x_1 \oplus (\ker(\nu) \cap N)$

$\Rightarrow \operatorname{rank}(N) = 1 + \operatorname{rank}(\ker(\nu) \cap N)$ -- (*)

Induct on rank of N.

(*) $\operatorname{rank}(\ker(\nu) \cap N) < \operatorname{rank}(N) = m$

and $\ker(\nu) \cap N$ is a R-submod of F.

Hence ind hyp $\ker(\nu) \cap N$ is free R-mod of rank $\operatorname{rank}(N) - 1$.

Also $Ra_1x_1 \cong R$ as R-module

$\Rightarrow N$ is free as N is direct sum of Ra_1x_1 & $\ker(\nu) \cap N$.

$Ra_1x_1 \cong R$; $\ker(\nu) \cap N \cong R^{m-1}$

Now for the remaining part.

We induct on $n = \text{rank}(F)$.

$\ker(\nu) \oplus R x_1 = F$.

$\Rightarrow \text{rank}(\ker(\nu)) = n-1$ & $\ker(\nu)$ is free

(since we showed every submod of F is free)

$\Rightarrow$ $\ker(\nu)$ is free of rank $n-1$

and $N \cap \ker(\nu) \subseteq \ker(\nu)$

So by ind hyp, $\ker(\nu)$ has a basis $\{x_2, \dots, x_n\}$ and $\exists a_2, \dots, a_m \in R^\times$ s.t. $a_2 | a_3 | \cdots | a_m$

$\{a_2 x_2, \dots, a_m x_m\}$ is a basis of $N \cap \ker(\nu)$.

claim ⊛

$\Rightarrow$ $\{x_1, \dots, x_n\}$ is a basis of F

& $\{a_1 x_1, a_2 x_2, \dots, a_n x_n\}$ is a basis of N.

$$\Sigma = \{\varphi(N) \mid \varphi \in \mathrm{Hom}(F, R)\}$$

& (a_1) is the maximal element of Σ.

a_2 is s.t.

the maximal element of

$$\{\varphi(N \cap \ker(\nu)) \mid \varphi \in \mathrm{Hom}(\ker(\nu), R)\}$$

$$a_2 = \nu_2(N \cap \ker(\nu))$$

$\mu : Rx_1 \oplus \ker(\nu) \longrightarrow R$

$\mu(x_1) = \nu(x_1)$ & $\mu|_{\ker(\nu)} = \nu_2$

Then $\mu : F \to R$ is R-lin. $\mu(rx_1 + \kappa) = r\nu(x_1) + \nu_2(\kappa)$

$$\mu(N) \ni \mu(a_1 x_1) = \nu(\underbrace{a_1 x_1}_{x}) = a_1$$

$$\Rightarrow (a_1) \subseteq \mu(N) \Rightarrow (a_1) = \mu(N)$$

$$\mu(N) \supseteq \nu_2(\ker(\nu)) = (a_2)$$

$$\Rightarrow a_2 \in (a_1) \Rightarrow a_1 \mid a_2.$$

Lecture 33: Applications of structure theorem

01 December 2020
11:48

Prop: Let R be a PID and F be a free R-module of rank n. Let N be a submodule of F. Then N is a free R-mod of rank $m \leq n$. Moreover there is a basis $x_1, \dots, x_n$ of F and $\exists\, a_1, \dots, a_m \in R^\times$ s.t. $a_1 | a_2 | \cdots | a_m$ and $\{a_1 x_1, a_2 x_2, \dots, a_m x_m\}$ is a basis of N.

Thm (Str thm): Let R be a PID and M be a f.g. R-mod. Then

$$M \cong R^k \oplus R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m)$$

where $k = \text{rank}(M)$ and $a_1, \dots, a_m \in R$ are nonzero nonunits s.t. $a_1 | a_2 | a_3 | \cdots | a_m$. Here k and m could be 0.

Thm: (Str thm version 2) Let R be a PID and M be a f.g. R-mod. Then

$$M \cong R^k \oplus R/p_1^{r_{11}} \oplus R/p_1^{r_{12}} \oplus R/p_1^{r_{13}} \oplus \cdots \oplus R/p_1^{r_{1n_1}}$$
$$\oplus R/p_2^{r_{21}} \oplus R/p_2^{r_{22}} \oplus \cdots \oplus R/p_2^{r_{2n_2}} \qquad k = \text{rank}(M)$$
$$\vdots$$
$$\oplus R/p_m^{r_{m1}} \oplus R/p_m^{r_{m2}} \oplus \cdots \oplus R/p_m^{r_{mn_m}}$$

where $p_1, \dots, p_m$ are irreducible elements of R, $r_{ij} \geq r_{i(j-1)}$ $\forall_{1 \leq i \leq m,\ 2 \leq j \leq n_i}$ are **positive** integers.

Cor ⊗ G is a f.g. abelian group then

$$G \cong \mathbb{Z}^k \oplus \mathbb{Z}/p_1^{r_{11}} \oplus \cdots \oplus \mathbb{Z}/p_1^{r_{1n_1}}$$

$$\vdots$$

$p_1, \ldots, p_m$ are prime nos.

$|G| = 36$, G is abelian

$\mathbb{Z}/36\mathbb{Z}$

$36 = 3^2 \cdot 2^2$

$G \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$

$n_1 = 2$, $p_1 = 2$, $p_2 = 3$

$n_2 = 2$

& $r_{11} = r_{12} = 1 = r_{21} = r_{22}$

$\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/9$

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$ or $\mathbb{Z}/4 \times \mathbb{Z}/3 \times \mathbb{Z}/3$

$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$

Version 1 & 2 are equivalent

Let $a_m = p_1^{r_{11}} p_2^{r_{21}} \cdots p_m^{r_{m1}}$ $\quad r_{ij} \geq 1 \; \forall \; j \leq m$

$a_{m-1} = p_1^{r_{12}} p_2^{r_{22}} p_3^{r_{32}} \cdots p_m^{r_{m2}}$ (upto unit)

where $r_{ij} \geq 0$.

$\vdots$

$a_2 = p_1^{r_{1m-1}} p_2^{r_{2m-1}} \cdots p_m^{r_{mm-1}}$

$a_1 = p_1^{r_{1m}} p_2^{r_{2m}} \cdots p_m^{r_{mm}}$

Since $a_j \mid a_{j+1}$ we have $r_{i,m-j+1} \leq r_{i,m-j}$

$\forall \; 1 \leq i \leq m$

$1 \leq j \leq m-1$

Note that some r_{ij} may be 0.

Now $R/(a_m) \xrightarrow{\text{CRT}} R/(p_1^{r_{11}}) \oplus \cdots \oplus R/(p_m^{r_{m1}})$

$(\because (p_i^{r_{ii}}, p_j^{r_{ij}}) = 1$ if $i \neq j)$

Now rearrange

$$M \cong R^k \oplus R/(a_1) \oplus \cdots \oplus R/(a_m)$$

$$\cong R^k \oplus R/(p_1^{r_{11}}) \oplus R/(p_2^{r_{21}}) \cdots \oplus R/(p_m^{r_{m1}})$$

$$\oplus R/(p_1^{r_{12}}) \oplus R/(p_2^{r_{22}}) \oplus \cdots \oplus R/(p_m^{r_{m2}})$$

$$\vdots$$

$$\oplus R/(p_1^{r_{1m}}) \oplus R/(p_2^{r_{2m}}) \oplus \cdots \oplus R/(p_m^{r_{mm}})$$

Note that r_{1m}, r_{2m} may be 0.

Write the transpose of above and ignore the terms when $r_{ij} = 0$ to obtain version 2.

Version 2 $\Rightarrow$ version 1

$$M \cong R^k \oplus R/(p_1^{r_{11}}) \oplus \cdots \oplus R/(p_1^{r_{1n_1}})$$

$$\vdots$$

$$R/(p_m^{r_{m1}}) \oplus \cdots \oplus R/(p_m^{r_{mn_m}})$$

$r_{ij} \geq r_{ij-1}$

Let $l = \max(n_1, \ldots, n_m)$

$$M \cong R^k \oplus 0 \oplus \cdots \oplus 0 \oplus R/(p_1^{r_{11}}) \oplus \cdots \oplus R/(p_1^{r_{1n_1}})$$

$$0 \oplus \cdots \oplus 0 \oplus R/(p_2^{r_{21}}) \oplus R/(p_2^{r_{2n_2}})$$

$$0 \oplus \cdots \oplus 0 \oplus R/(p_3^{r_{31}}) \oplus R/(p_3^{r_{3n_3}})$$

$$\vdots$$

$$0 \oplus \cdots \oplus 0 \oplus R/(p_m^{r_{m1}}) \oplus \cdots \oplus R/(p_m^{r_{mn_m}})$$

Let $a_m = p_1^{r_{1n_1}} p_2^{r_{2n_2}} \cdots p_m^{r_{mn_m}}$

$a_{m-1} = p_1^{r_{1(n_1-1)}} p_2^{r_{2n_2-1}} \cdots p_m^{r_{mn_m-1}}$

$\vdots$

$a_1 = p_1^{r_{1,n_1-m+1}} p_2^{r_{2,n_2-m+1}} \cdots p_m^{r_{m,n_m-m+1}}$

$\supseteq R/(a_m)$

CRT $M \cong R^k \oplus R/(a_1) \oplus \cdots \oplus R/(a_m)$

Also condition $r_{ij} \geq r_{ij-1}$

$\Rightarrow a_1 | a_2 | \cdots | a_m$.

convention is $r_{ij} = 0$ if $j \leq 0$

Thm: (Rational form)
$A \in M_{n\times n}(k)$ k a field.

A is similar to
$$\begin{bmatrix} R_{a_1} & & 0 \\ & \ddots & \\ 0 & & R_{a_m} \end{bmatrix}$$
where $a_i = x^{n_i} + b_{n_i-1}x^{n_i-1} + \cdots + b_1 x^1 + b_0$, $1 \le i \le m$

$\sum_{i=1}^{m} n_i = n$

$a_1 | a_2 | \cdots | a_m$

where $R_{a_i} = \begin{bmatrix} 0 & & & -b_0 \\ 1 & \ddots & & \vdots \\ & \ddots & 0 & -b_{n_i-1} \\ 0 & & 1 & \end{bmatrix}$ $n_i \times n_i$ matrix

$\exists P$ nonsing s.t. $P^{-1}AP = R$

Pf: $A : k^n \longrightarrow k^n$ k-lin map.
V V

This gives V a $k[x]$-mod sts.

via $v \in V$
$x \cdot v = Av$ $\quad f(x) = a_n x^n + \cdots + a_1 x + a_0$

In general $f(x)\cdot v = f(A)v$
$= (a_n A^n + \cdots + a_1 A + a_0 I)v$

$k[x]$ is a PID and V is f.g. $k[x]$-mod

What is $\operatorname{rank}(V)$ as a $k[x]$-mod?

$m_A(x) \in k[x]$ minimal poly $\quad m_A(x)\cdot v = m_A(A)v = 0$ (Caley-Hamilton)

$\Rightarrow$ V is torsion $k[x]$-mod

So by str. thm

$$V \cong R/(a_1) \oplus \cdots \oplus R/(a_m) \quad \text{as } R\text{-mod}$$

where $R = k[x]$

$a_1 | a_2 | \cdots | a_m \quad a_i \in k[x]$

May assume a_i are monic

$A \cdot v = x \cdot v \qquad a_i(x) = x^{n_i} + b_{n_i-1} x^{n_i-1} + \cdots + b_0$

So choose the basis

$$R/(a_i) \cong k[x]/(a_i(x)) \cong k \oplus k\bar{x} \oplus k\bar{x}^2 \oplus \cdots \oplus k\bar{x}^{n_i-1}$$

$$B = \{1, \bar{x}, \bar{x}^2, \bar{x}^3, \ldots, \bar{x}^{n_i-1}, \ldots\}$$

What is the matrix of A w.r.t B.

$$x \cdot 1 = 0 \cdot 1 + 1\bar{x} + 0\bar{x}^2 + \cdots$$

$$x \cdot \bar{x} = \bar{x}^2 = 0 \cdot 1 + 0 \cdot \bar{x} + 1 \cdot \bar{x}^2 + \cdots$$

$$x \cdot \bar{x}^{n-2} = \bar{x}^{n-1} = 0 \cdot 1 + 0 \cdot \bar{x} + \cdots + 0 \cdot \bar{x}^{n-2} + 1\bar{x}^{n-1}$$

$$x \cdot \bar{x}^{n-1} = \bar{x}^n = -b_0 1 - b_1 \bar{x} + -b_2 \bar{x}^2$$

$$\begin{bmatrix} 0 & & & -b_{n-1} \\ 1 & 0 & & \vdots \\ 0 & 1 & \ddots & \\ \vdots & 0 & 0 & -b_1 \\ 0 & 0 & 1 & -b_0 \end{bmatrix}$$

Lecture 34: Rational canonical form and Jordan form

03 December 2020
19:20

Thm (Rat'l canonical form): Let V be a n-dimensional vector space over a field k and $\varphi: V \to V$ be a k-linear map. Then $\exists$ a basis $\mathcal{B}$ of V s.t. that the matrix of φ w.r.t $\mathcal{B}$ is of the form

$$R_\varphi = \begin{bmatrix} R_{a_1} & & \\ & R_{a_2} & \\ & & \ddots \\ & & & R_{a_m} \end{bmatrix}$$

where for a monic poly $a(x) = x^l + b_{l-1}x^{l-1} + \cdots + b_0$ of deg l, R_a is the $l \times l$ matrix

$$\begin{bmatrix} 0 & & & -b_0 \\ 1 & 0 & & -b_1 \\ & 1 & \ddots & \vdots \\ & & 0 & \vdots \\ & & 1 & -b_{l-1} \end{bmatrix}$$

$a_1(x), \ldots, a_m(x) \in k[x]$ are nonconstant monic poly s.t. $a_1 | a_2 | \cdots | a_m$.

Equivalently, $A \in M_{n\times n}(k)$ then $\exists$ a nonsingular matrix P s.t. $P^{-1}AP = R_\varphi$ for some $a_1, \ldots, a_m \in k[x]$ nonconst. monic poly with $a_1 | a_2 | \cdots | a_m$.

Pf: $\varphi: V \to V$ is a k-lin map

$\Rightarrow$ V is a $k[x]$-mod s.t. $X \cdot v = \varphi(v)$ $\forall v \in V$.

$f(x)\cdot v = f(\varphi)(v)$ Note $f(\varphi) \in \mathrm{End}_k(V)$

By str thm for f.g. mod over PID.

$$V \overset{\theta}{\cong} R/(a_1) \oplus \cdots \oplus R/(a_m)$$

where $R = k[x]$ and $a_1, \ldots, a_m$ are monic nonconst. poly and $a_1 | a_2 | \cdots | a_m$ as R-modules

(since $\mathrm{rank}(V) = 0$ as $k[x]$-mod as $m_\varphi(x)$ annihilates V)

$m_\varphi(x)$: minimal poly of φ.

Note

$$\begin{array}{ccc} V & \xrightarrow{\varphi} & V \\ \uparrow\theta & \circlearrowright & \downarrow\theta^{-1} \\ \bigoplus_{i=1}^m R/(a_i) & \longrightarrow & \bigoplus_{i=1}^m R/(a_i) \end{array}$$

Claim: $\theta^{-1}\circ\varphi\circ\theta = \mu_X$ ← mult by X

Let $\alpha \in \bigoplus_{i=1}^m R/(a_i)$

θ^{-1} is $k[x]$-linear

$$\theta^{-1}\circ\varphi\circ\theta(\alpha) = \theta^{-1}(X\cdot\theta(\alpha)) = X\cdot\theta^{-1}(\theta(\alpha)) = X\cdot\alpha = \mu_X(\alpha)$$

So enough to show that the matrix of μ_X w.r.t some basis is R_φ.

Note that $R/(a_i)$ is invariant under μ_X as

$$X \cdot (\kappa_1, \dots, \kappa_m) = (X \cdot \kappa_1, \dots, X \cdot \kappa_m) \quad \text{for } \kappa_i \in R/(a_i)$$

$1 \le i \le m$.

Also $B_i = \{[1]_i, [X]_i, [X]_i^2, \dots, [X]_i^{n_i - 1}\}$ is a basis of $R/(a_i)$ where a_i is a poly of deg n_i.

$[X^j]_i = X^j + (a_i)$

Let B be the ordered basis $B_1 \cup B_2 \cup \dots \cup B_m$. Then the matrix of μ_X w.r.t. B is

$$\begin{bmatrix} R_1 & & 0 \\ & \ddots & \\ 0 & & R_m \end{bmatrix}$$ where

R_i is the matrix of $\mu_X|_{R/(a_i)}$ w.r.t. the ordered basis B_i. (Since $R/(a_i)$ is invariant under μ_X)

So enough to show $R_i = R_{a_i}$

matrix of $\mu_X|_{R/(a_i)}$ w.r.t $B_i = \{[1]_i, [X]_i, \dots, [X^{n_i-1}]_i\}$

Recall matrix of $\psi \in End(V)$ w.r.t a ordered basis $\{v_1, \dots, v_n\}$ is $((c_{ij})) \in M_{n\times n}(k)$ where $\psi(v_j) = \sum_{i=1}^{n} c_{ij} v_i$ $1 \le j \le n$.

$$\mu_X([1]_i) = X\cdot[1]_i = [X]_i = 0[1]_i + 1[X]_i + 0[X^2]_i + \dots + 0[X^{n_i-1}]_i$$

$$\mu_X([X]_i) = X\cdot[X]_i = [X^2]_i = 0[1]_i + 0[X]_i + 1[X^2]_i + \dots + 0[X^{n_i-1}]_i$$

$$\mu_X([X^{n_i-2}]_i) = [X^{n_i-1}]_i = 0[1]_i + 0[X]_i + \dots + 0[X^{n_i-2}]_i + 1[X^{n_i-1}]_i$$

$$\mu_X([X^{n_i-1}]_i) = [X^{n_i}]_i = -b_0[1]_i - b_1[X]_i + \dots + -b_{n_i-1}[X^{n_i-1}]_i$$

if $a_i(X) = X^{n_i} + b_{n_i-1}X^{n_i-1} + b_{n_i-2}X^{n_i-2} + \dots + b_1X + b_0$

Hence $R_i = R_{a_i} = \begin{pmatrix} 0 & 0 & & & -b_0 \\ 1 & 0 & & 0 & -b_1 \\ 0 & 1 & & & \vdots \\ & 0 & 1 & & \\ & & & \ddots & \\ 0 & 0 & & 0 & -b_{n_i-2} \\ & & & 1 & -b_{n_i-1} \end{pmatrix}$

Hence the matrix of μ_X w.r.t the ordered basis B is R_φ.

Thm: (Jordan form) Let V be a n-dim'l vs over $\mathbb{C}$ (or any alg closed field). Let $\varphi: V \to V$ be a $\mathbb{C}$-linear map. Then there exist a basis $\mathcal{B}$ of V s.t. the matrix of φ w.r.t. $\mathcal{B}$ is of the form.

$$J_\varphi = \begin{bmatrix} J_{\lambda_1}^{r_{11}} & & & & & & \\ & J_{\lambda_1}^{r_{12}} & & & & & \\ & & \ddots & & & & \\ & & & J_{\lambda_1}^{r_{1m_1}} & & & \\ & & & & J_{\lambda_2}^{r_{21}} & & \\ & & & & & \ddots & \\ & & & & & & J_{\lambda_m}^{r_{mm_m}} \end{bmatrix}$$

where $\lambda_i \in \mathbb{C}$, $1 \le i \le m$; r_{ij} are positive integers.

$$J_\lambda^r = \begin{bmatrix} \lambda & & 0 \\ 1 & \ddots & \\ 0 & & 1 \lambda \end{bmatrix}$$ is a $r \times r$ matrix $\lambda \in \mathbb{C}$.

Equivalently, $A \in M_{n\times n}(\mathbb{C})$ then A is similar to J_φ for some $\lambda_1, \dots, \lambda_m \in \mathbb{C}$ & r_{ij} positive integers.

str thm as $\mathbb{C}[x]$-mod

$$V \cong R/p_1^{a_{11}} \oplus R/p_1^{a_{12}} \oplus \cdots \oplus R/p_1^{a_{1m_1}}$$
$$\oplus R/p_2^{a_{21}} \cdots \oplus R/p_2^{a_{2m_2}}$$
$$\vdots$$
$$\oplus R/p_m^{a_{m1}} \oplus \cdots \oplus R/p_m^{a_{mm_m}}$$

$p_i(x)$ are irred in $\mathbb{C}[x]$

(R) Every non const poly in $\mathbb{C}[x]$ is prod of linear factors (FTA).

$\Rightarrow p_i(x) = (x-\lambda_i)$ for some $\lambda_i \in \mathbb{C}$.

So $R/(p_i^{a_{ij}}) = \dfrac{\mathbb{C}[x]}{(x-\lambda_i)^{a_{ij}}}$

So we will choose a basis B_{ij} of $\dfrac{\mathbb{C}[x]}{(x-\lambda_i)^{a_{ij}}}$ s.t. the matrix of μ_x on $R/p_i^{a_{ij}}$ is $J_{\lambda_i}^{a_{ij}}$.

And this will complete the proof.

$$B_{ij} = \left\{1,\ x-\lambda_i,\ (x-\lambda_i)^2,\ \dots,\ (x-\lambda_i)^{\alpha_{ij}-1}\right\}$$

$$\mu_X(1) = X\cdot 1 = \lambda_i 1 + 1(x-\lambda_i) + 0\cdot(x-\lambda_i)^2 + \dots + 0(x-\lambda_i)^{\alpha_{ij}-1}$$

$$\mu_X(x-\lambda_i) = X^2 - \lambda_i X = 0\cdot 1 + \lambda_i(x-\lambda_i) + 1(x-\lambda_i)^2 + 0\dots$$

$$\vdots$$

$$\mu_X\left((x-\lambda_i)^{\alpha_{ij}-2}\right) = X(x-\lambda_i)^{\alpha_{ij}-2} = (x-\lambda_i)^{\alpha_{ij}-1} + \lambda_i(x-\lambda_i)^{\alpha_{ij}-2}$$

$$= 0\cdot 1 + 0\cdot(x-\lambda_i) + \dots + \lambda_i(x-\lambda_i)^{\alpha_{ij}-2} + 1(x-\lambda_i)^{\alpha_{ij}-1}$$

$$\mu_X\left((x-\lambda_i)^{\alpha_{ij}-1}\right) = X(x-\lambda_i)^{\alpha_{ij}-1} = (x-\lambda_i)^{\alpha_{ij}} + \lambda_i(x-\lambda_i)^{\alpha_{ij}-1}$$

$$= 0\cdot 1 + 0\cdot(x-\lambda_i) + \dots + 0(x-\lambda_i)^{\alpha_{ij}-2} + \lambda_i(x-\lambda_i)^{\alpha_{ij}-1}$$

$$J_\lambda^{\alpha_{ij}} = \begin{pmatrix} \lambda_i & 0 & & & 0 & 0 \\ 1 & \lambda_i & & & & \\ 0 & 1 & \lambda_i & & & \\ & 0 & 1 & \ddots & & \\ & & 0 & & \lambda_i & 0 \\ 0 & 0 & & 0 & 1 & \lambda_i \end{pmatrix}$$

Hence the matrix of μ_X w.r.t. $B = B_1^{\alpha_{11}} \cup B_1^{\alpha_{12}} \cup \dots \cup B_1^{\alpha_{1m_1}} \cup B_2^{\alpha_{21}} \cup B_2^{\alpha_{22}} \dots \cup B_m^{\alpha_{nnm}}$ is

J_φ .

Lecture 35: Rational form and Jordan form - Examples

07 December 2020
14:37

Thm (Rat'l canonical form): Let V be a n-dimensional vector space over a field k and $\varphi: V \to V$ be a k-linear map. Then $\exists$ a basis $\mathcal{B}$ of V s.t. that the matrix of φ w.r.t $\mathcal{B}$ is of the form.

$$R_\varphi = \begin{bmatrix} R_{a_1} & & \\ & R_{a_2} & \\ & & \ddots \\ & & & R_{a_m} \end{bmatrix}$$

where for a monic poly $a(x) = x^l + b_{l-1}x^{l-1} + \dots + b_0$ of deg l, R_a is the $l \times l$ matrix

$$\begin{bmatrix} 0 & & & -b_0 \\ 1 & 0 & & -b_1 \\ & \ddots & \ddots & \vdots \\ & & 1 & -b_{l-1} \end{bmatrix}$$

$a_1(x), \dots, a_m(x) \in k[x]$ are nonconstant monic poly s.t. $a_1 | a_2 | \dots | a_m$.

Equivalently, $A \in M_{n\times n}(k)$ then $\exists$ a nonsingular matrix P s.t. $P^{-1}AP = R_\varphi$ for some $a_1, \dots, a_m \in k[x]$ nonconst, monic poly with $a_1 | a_2 | \dots | a_m$.

Thm: (Jordan form) Let V be a n-dim'l vs over $\mathbb{C}$ (or alg closed field). Let $\varphi: V \to V$ be a $\mathbb{C}$-linear map. Then there exist a basis of $\mathcal{B}$ of V s.t. the matrix of φ w.r.t. $\mathcal{B}$ is of the form.

$$J_\varphi = \begin{bmatrix} J_{\lambda_1}^{r_{11}} & & & & & \\ & J_{\lambda_1}^{r_{12}} & & & & \\ & & \ddots & & & \\ & & & J_{\lambda_2}^{r_{21}} & & \\ & & & & \ddots & \\ & & & & & J_{\lambda_m}^{r_{mn_m}} \end{bmatrix}$$

where $\lambda_i \in \mathbb{C}$, $1 \le i \le m$, r_{ij} are positive integers.

$$J_\lambda^r = \begin{bmatrix} \lambda & & 0 \\ 1 & \ddots & \\ 0 & \ddots & 1 \lambda \end{bmatrix}$$ is a $r \times r$ matrix $\lambda \in \mathbb{C}$. $\leftarrow \mathbb{C}[x]/(x-\lambda)^r$

Equivalently, $A \in M_{n\times n}(\mathbb{C})$ then A is similar to J_φ for some $\lambda_1, \dots, \lambda_m \in \mathbb{C}$ & r_{ij} positive integers.

⊛ What is the minimal poly of φ? Char poly of φ?

⊛ What are eigen values of φ?

⊛ Note that $V \cong k[X]/(a_1) \oplus \cdots \oplus k[X]/(a_m)$

$a_1 | a_2 | \cdots | a_m$ $\quad a_i \in k[X]$ non const monic poly.

minimal poly of φ is the least deg monic poly $m_\varphi(X) \in k[X]$, s.t. $m_\varphi(\varphi)$ is the zero endo of V. $\quad m_A(A)=0$

i.e. $m_\varphi(X) \cdot v = 0 \quad \forall v \in V$

i.e. $(m_\varphi(X)) = Ann(V)$ $\quad r(\bar{1}, \bar{1}, \bar{1}, \ldots, \bar{1}) = \underset{\sim}{0}$

But $Ann(V) = (a_m(X))$. Hence $a_m(X)$ is the minimal poly of φ. ← as a $k[X]$-module

Char poly of $R_a = \det(XI - R_a)$

$$= \begin{pmatrix} X & 0 & & b_0 \\ -1 & X & & \vdots \\ & -1 & & b_{n-2} \\ 0 & & -1 & X+b_{n-1} \end{pmatrix}$$

$$= (X+b_{n-1})X^{n-1} - b_{n-2}\det\begin{pmatrix} X & 0 & & 1 \\ -1 & \ddots & & 0 \\ & -1 & X & 0 \\ 0 & & 0 & -1 \end{pmatrix}$$

$$+ b_{n-3}\det\begin{pmatrix} X & 0 & & 0 \\ -1 & \ddots & & \vdots \\ & -1 & X & 0 \\ 0 & & -1 & X \\ & & 0 & -1 \end{pmatrix} - \cdots$$

$$= X^n + b_{n-1}X^{n-1} + b_{n-2}X^{n-2} + \cdots + b_0$$

$$= a(X)$$

So char of R_φ $ch_\varphi(X) = a_1(X)\, a_2(X) \cdots a_m(X)$

* minimal poly of R_a is $a(X)$

* minimal poly, char poly J_λ^r is $(X-\lambda)^r$

Eigen value of φ are $\lambda_1, \dots, \lambda_m$ of Jordan form.

Example: $V = \mathbb{C}^3$

$A : \mathbb{C}^3 \longrightarrow \mathbb{C}^3$ — V is a $\mathbb{C}[X]$-mod

$$A = \begin{pmatrix} 1 & 2 & 0 \\ 3 & 4 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

$$V \overset{\theta}{\cong} \mathbb{C}[X]/(a_1) \oplus \frac{\mathbb{C}[X]}{(a_2)} \quad \text{or} \quad \frac{\mathbb{C}[X]}{(a_1(x))}$$

or $\mathbb{C}[X]/(a_1) \oplus \frac{\mathbb{C}[X]}{(a_4)} \oplus \mathbb{C}[X]/(a_3)$ X

$\Downarrow \Uparrow \; a_1 = a_2 = a_3$

If $m_A(x) = (x-\lambda) \Rightarrow A = \lambda I$ (contra!)

$$ch_A(x) = (x-2)\left[(x-1)(x-4)-6\right] = \det \begin{pmatrix} x-1 & -2 & 0 \\ -3 & x-4 & 0 \\ 0 & 0 & x-2 \end{pmatrix}$$

$$= (x-2)(x^2-5x+4-6)$$

$$= (x-2)(x^2-5x-2) = x^3-5x^2-2x \\ -2x^2+10x+4$$

$$= x^3-7x^2+8x+4$$

$$\frac{5 \pm \sqrt{33}}{2}$$

$m_A(x) = ch_A(x)$

$\Rightarrow a_3(x) = ch_A(x) = m_A(x)$

$$\begin{pmatrix} 0 & 0 & -4 \\ 1 & 0 & -8 \\ 0 & 1 & 7 \end{pmatrix}$$ rat'l form A

Jordan form

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & \frac{5+\sqrt{33}}{2} & 0 \\ 0 & 0 & \frac{5-\sqrt{33}}{2} \end{pmatrix}$$