L14. 这节笔记中记R为integral domain (可交换, 有unity, 无zero-divisor)

R^* = {R中invertible元素} ↘ 若无说明则默认有说明看说明

def1: $a=bc$, b是a的factor, a是b的multiple; 若c invertible, 则a可以写成 $a=bc \Rightarrow b=ac^{-1}$, 称为a,b associate, $a\sim b$

def2: $d\in R$, d is irreducible if: $ab=d$ then a or b is invertible

def3: $d\in R$, d is prime if $d|ab$ then $d|a$, or $d|b$

prop: ID, prime $\Rightarrow$ irreducible

$d\in R$ is prime $d=ab$,

then $d|ab$, $\therefore d|a$ or $d|b$ (设 $a=dc$)

即回 $d=ab=dcb$, $d(cb-1)=0$

ID中无zero-divisor $\Rightarrow cb=1$ $\therefore$ b invertible d可分

(a,b中没法再分出d的因数)

即可以通过a'd或db'回到b或a

d是factor也是multiple

Rmk. 不在ID中, prime, irr是双向不完等的

例: $R=\{a+b\sqrt{5}: a,b\in\mathbb{Z}\}$ (1) not prime ($2\in R$) (2) reducible ($2\in R$)

(1) $(1-\sqrt{5})(1+\sqrt{5})=6=2\times3$ 这也说明了not PID, 6不可逆, 但有不同的不可约分解

$2|(1-\sqrt{5})(1+\sqrt{5})$, 但 $2\nmid 1-\sqrt{5}$, $2\nmid 1+\sqrt{5}$

(2) 设 $2=(a+b\sqrt{5})(c+d\sqrt{5})$

then $2=\bar{2}=(a-b\sqrt{5})(c-d\sqrt{5})$ $\therefore 4=(a^2+5b^2)(c^2+5d^2)$ b,d$\in\mathbb{Z}$

$\therefore b=d=0$. can be $a=\pm2, c=\pm1$ or $a=\pm1, c=\pm2$ a有逆元或c有

def4: D is ID, D is "unique factorization domain" (UFD) 若:

(1): $\forall$ 不可逆元素 in D, 可以写成 finite irreducible 元素的 product

(2): (不管order, unit multiplication) 此分解唯一

Th: D is ID, then D is UFD 若(1)(chain condition)+若$\forall$ irr element is prime

$\Leftarrow$ $a\in D$ $a=p_1p_2\cdots p_s=q_1q_2\cdots q_t$, a invertible, p_i,q_i irr; 且 gcd$(p_i,p_j)=1$

then: $p_i|q_1q_2\cdots q_t$, $p_i|q_j$ some j $\Rightarrow p_i|p_k$ $\therefore p_i=p_k=q_j$

同样有 $q_j|p_k$ some k,

即每个 p_i, 唯一 $q_j=p_i$ $\Rightarrow$ 总之 $\Pi p_i=\Pi q_j$ 分解相同

⇒: 设 $\exists d \in R$, d irreducible, d not prime; $\exists d \mid ab$, $d \nmid a$, $d \nmid b$

$\therefore \exists a' \mid a, b' \mid b$ s.t. $d = a'b'$

then 设 a' invertible; $a'a'' = a$ $b'b' = b$

设 a invertible, then a'' invertible $d = a'b' = aa''^{-1}b' = a(a''^{-1}b')$ 分解不唯一

$\therefore a$ ~~同理 b~~ not invertible

D is UFD $\therefore a' = p_1 p_2 \cdots p_s$ $b = q_1 q_2 \cdots q_t$

设 d irreducible, not prime

$\exists d \mid ab$ $d \nmid a$, $d \nmid b$

$a \mid b$ 即: $\exists c \in R$ $ac = b$

$\Downarrow$

a, b not invertible, 否则: $d \mid ab \Rightarrow a^{-1}d \mid b$, $\Rightarrow a^{-1} \mid b$. $d \mid b$ --①

设 $a = p_1 p_2 \cdots p_s$, $b = q_1 q_2 \cdots q_t$, 其中 p_i, q_j 不可约

$\therefore d = p_1 p_2 \cdots p_s q_1 q_2 \cdots q_t$

由于不可约分解具有唯一性, 不妨设 $d \sim p_1$ (即 $d \mid p_1$, $p_1 \mid d$) --②

而 $p_1 \mid a \therefore d \mid a$

~~(1)(2)为什么, 说明白~~

和整除关系一一对应

def5: ID is PID principle ideal domain 若: $\forall$ ideal is principal

principle: 由单个元素和 R 生成的 ideal, 如

$RaR = \{\sum^{\text{finite}} r_i a s_i : r_i, s_i \in R\}$ 是由 a 和 R 生成的 2-sided principle ideal

$\Downarrow$ 在ID中即 $\{\sum r_i a : r_i \in R\}$ 且在 a 可逆时 $\langle a \rangle = D$

Th: PID is UFD

CAAP308 lem1: in PID, irreducible $\nRightarrow$ prime

已知在ID中, prime $\Rightarrow$ irreducible

设 a irreducible, $a \mid bc$

Consider ideal $I = \{ax + by : x, y \in D\}$ (是ideal因为ID中的对换, 且是ring) 吸收性

in PID, $\exists d$ s.t. $\langle d \rangle = I = \{\sum r_i d s_i : r_i s_i \in R\} = \{\sum r_i d : r_i \in R\}$

$a \in I \therefore a = dr$, d 或 r invertible

① 若 $\exists d^{-1}$, then $I = D$ since $\forall x \in D$ $\exists (d^{-1}x) d \in I$

(lem直接证出Th)

∴ ∃ x,y s.t. 1 = ax + by thus c = cax + cby

a|bc. a|a ∴ a| LHS 即 a|c

② 存在 n, ⟨a⟩ ⊋ ⟨a²⟩ ⊋ ⋯ ⊋ ⟨aⁿ⟩ = I

∵ b∈I ∴ ∃ t∈D s.t. at = b. 即 a|b

还有要证明：PID满足 chain condition 的证明

下证 a ≠ finite product of irr

a = a₁b₁; 若 a₁ not irr, a₁ = a₂b₂ 不可逆

∴ a = a₂b₂b₁ ⋯

∴ (a) ⊊ (a₂) ⊊ (a₃) ⊊ ⋯ 设 I = ⋃(aᵢ) ⋯

I is ideal of D

D is PID ∴ I = (b) some b

b ∈ (aᵢ) ∴ I = (b) ⊆ (aᵢ) ∈ (aᵢ₊₁) ⊂ I

Rmk: · ring 的定义 (R,+) Abelian group, (R,·) semi group

0∈R 作为加法的 e, 1 不定, inverse 不一定

ID ⇒ UFD, ID + principle ⇒ PID, 均在 ID 基础上考虑

· ideal (a) = {Σ rᵢ a sᵢ : rᵢ, sᵢ ∈ R}

在 ID 中可交换 (a) = {Σ rᵢ a : rᵢ ∈ R} = {Σ a rᵢ : rᵢ ∈ R}; a 可逆则 |: (a) = D

在 ID 中 a = dr, r 可逆则 (a) = (d) (不在 ID 中也行)

a|b 的定义为 ∃ c∈R ac = b

例：ℤ[x] is a UFD. ℤ[x] not a PID 整系数多项式

consider I = (2, x). if I = (h(x)) some h

I = {Σ 2fᵢ + x f₂ : fᵢ f₂ ∈ ℤ[x]} 2∈I, x∈I

∴ 2 = h(x) f₁(x) x = h(x) f₂(x)

∴ h 和 fᵢ 为常数 2 = (±1)(±2)

1 ∉ I, h ∈ I ∴ 只能 f₁ = ±1, h = ±2 (f 在 D 中不是在 I 中)

∴ f₂(x) = ±x ∉ D

Rmk: 涉及 PID 的，一般会用极小性写法表示出 ideal, { I = (d) ; I = {ax + cy : c, y ∈ D} 均是

要从两个 I 分别找信息拼在一起

Th: D is PID, p∈D−{0}, (p) is prime ideal ⇔ (p) is maximal ideal

lem: p is prime, ⇔ irreducible, in PID

lem: in PID, a irreducible ⇔ (a) maximal ideal

⇒: 不妨设 a ≠ 0,

设 ideal I ⊋ (a), I = (b) since D is PID

∴ ∃ a = bt, t∈D, then b 或 t invertible { ∃ b⁻¹ (b) = D ; ∃ t⁻¹ (b) = (a)

$\Leftarrow$ (a) is maximal prime ideal (要求 proper. 设 $\exists a^{-1}$, $(a)=D$)

$\therefore a \neq 0$ 且 a 不可逆

PID is UFD $\therefore a$ 分解为 irr 之积 $a=a_1a_2\cdots a_n$, $(a_i)\subseteq(a)$ WTS: 有 a_i 可逆

a_1 irr $\therefore (a_1)$ maximal 由"$\Rightarrow$"知

$(a_1)\subseteq(a)$ $\therefore (a)=(a_1)$

$\therefore a_2 \cdots a_n$ invertible a irr

Rmk: 若 $(p)=(px)$, $\Rightarrow x$ invertible

lem: PID中 prime ideal (a) 和 a prime ($\Leftrightarrow$ irr in PID) 的关系

定义: 在 commutative ring R 中, I is prime if: $ab\in I \Rightarrow a\in I$ or $b\in I$, 且 $I\neq R$

proof: $\Rightarrow$ if (a) prime $(a)=\{\sum ar_i : r_i\in R\}$

设: if: $bc=a$, $bc\in(a)$ then $b\in(a)$ 或 $c\in(a)$

$\therefore c=ar_i$ 代回

$\therefore bc=br_ia=a$, $(br_i-1)a=0$

在 ID 中无 zero divisor $\therefore br_i=1$ 即 b 可逆 $\therefore a$ irr $\Leftrightarrow$ prime

$\Leftarrow$ ~~a irr. $a=bc$ $\exists b^{-1}$ 或 c^{-1}, $(a)=(b)$~~ 设

if $xy\in(a)$ $xy=ar_i$

~~设 $\exists x^{-1}$ or y^{-1}, 则完成证明; 设 x,y invertible~~, $a|xy$ a prime

设 $a|x$ or $a|y$, $x=at\in(a)$

Rmk: 在 ID 中, (a) primal $\Rightarrow$ a irreducible $\overset{PID}{\Leftarrow}$

夜操 在 ID 中, a prime $\Rightarrow$ (a) primal (a) maximal

$\therefore$ 在 PID 中 irr $\Leftrightarrow$ prime (必定 ID), maximal $\Leftrightarrow$ primal 悄悄了!

T例: (chain cel) ID $\mathbb{Z}[\frac{1}{2}]=\{\frac{m}{2^n} : m,n\in\mathbb{Z}\}$ finite

2 不可逆, 但不存在不可约分解