4/5

def: ED (Euclidean Domain): 在ID, map $v: D\setminus\{0\} \to \mathbb{Z}^+$ is valuation if:

$\forall x,y\in D, y\neq 0, \exists q,r\in D$ s.t. $x=qy+r$, $r=0$ or $v(r)<v(y)$; D is ED if v exist

即ED可以做除法 (D中可以用 Euclidean algorithm)

例: $R=\mathbb{Z}[\sqrt{3}]=\{m+n\sqrt{3}: m,n\in\mathbb{Z}\}$, R is ED

例: $Q[x]$ is ED, valuation: degree

$\mathbb{Z}$ is ED, valuation: Abs

Th: ED is a PID (thus UFD)

D is ED, I is an ideal

take $b\in I$ s.t. $v(b)$ is the smallest in I, 证明 $I=(b)$ → 即 $\forall a\in I.\ a\in(b)$, $a=bq$ some q

$\forall a\in I.\ b\in I$ then $ab\in I$; $\exists q,r\in D$ s.t. $a=qb+r$ $r=0$ or $v(r)<v(b)$

$r=a-qb\in I$ ∴ $r=0$, $a=qb$

a is arbitary 即 $\forall a\in I$, $a=qb$ some $q\in D$ ∴ $I=(b)$

例: $\mathbb{Z}[\sqrt{-1}]=\{a+bi: a,b\in\mathbb{Z}\}$, $\mathbb{Z}[\sqrt{-1}]$ is ED

let $v(a+bi)=a^2+b^2=|a+bi|^2$

对于 $\forall x,y\in R$, $y\neq 0$, $yR=\{(a+bi)r: r\in R\}$ $v((a+bi)r)=v(a+bi)\cdot v(r)$

∴ yR可以认为是边长 $v(y)=|y|^2$ 正方形网格的格点

设与x最近的格点为 $(a+bi)r=y(c+di)$, let $q=c+di$ $r=x-qy$

(正方形上一点到4个顶点距离最小值 < 边长)

例: HW9 T8: algebraic integer ring of $\mathbb{Q}(\sqrt{5})$ is ED

最高为整系数多项式的根, 在 $\mathbb{Q}(\sqrt{5})=\{a+b\sqrt{5}: a,b\in\mathbb{Q}\}$ 中

① $D=\{a+b\frac{1+\sqrt{d}}{2}: a,b\in\mathbb{Z}\}$, $d\equiv 1 \pmod 4$ is alg-integer ring in $\mathbb{Q}(\sqrt{d})$

$(a+b\frac{1+\sqrt{d}}{2})(a+b\frac{1-\sqrt{d}}{2})=(a+\frac{1}{2}b)^2-(\frac{1}{2}b\sqrt{d})^2=a^2+ab+\frac{1}{4}b^2(1-d)\in\mathbb{Z}$ since $d\equiv 1 \pmod 4$

∴ $f(x)=x(2a+b-x)-(a^2+ab+\frac{1}{4}b^2(1-d))\in\mathbb{Z}[x]$, $f(a+b\frac{1+\sqrt{d}}{2})=0$,

∴ $\forall q\in D$, q a.i. ring of $\mathbb{Q}(\sqrt{5})$ ···①'

另一个方向: 反面;

recall: K is fraction field of R, f irreducible in $R[x] \nRightarrow$ in $F[x]$

lem: irreducible $\Rightarrow$ primitive 设 $f = c(f)\cdot f_1$ (c=c, f_1=pri) 若 $c \neq 1$: c invertible in R f reducible 分解为2个不可逆的

若 $\exists \frac{1}{c}$ in R:

$\because$ gcd(a,b)=d, then gcd(a,b)=cd ; gcd(a,b)=gcd(a,cb)"

$d|a$ $d|b$ $dx=a$ $dy=b$

$cd\cdot xc^{-1}=a$, $cd\cdot yc^{-1}=b$ $\therefore cd|a,b$ $c(f)=c(cf_1)=cf_1=1$

proof: $f(x)=g(x)\cdot h(x)$, $g,h\in F[x]$.

$\exists r$ (把g系数的最小公倍数), s s.t. $rg\in R[x]$, $sh\in R[x]$, $rsf=rg\cdot sh$

$c(rg)=r_1$, $c(sh)=s_1$, then let $g_1r_1=gr$, $hs_1=hs$; h_1和g_1均 primitive

$\therefore rsf=r_1g_1\times s_1h_1$ $c(rsf)=c(r_1g_1\times s_1h_1)$ $\therefore rs=r_1s_1\cdot u^{-1}$ unit in R

$\therefore r_1s_1f=r_1s_1u\cdot g_1\cdot h_1$, $f=ug_1\cdot u'h_1$

① $c(rg)=r_1$, 若 $r_1\neq 1$, g系数为 $a_0a_1\cdots$

$gcd(ra_0,\cdots ra_n)=1\times r_1$

then $gcd(ra_0,\cdots ra_n)=1\times r_1\times r_1^{-1}=1$

rg primitive, 将 r_1 改写成 identity "1"

↓

proof前先说明一下 unit 不影响

② primitive function 一定在R[x]中吗, ? 违背Hilbert

Th: D is UFD, then D[x] is also UFD

WTS: $f(x)=p_1(x)p_2(x)\cdots p_s(x)=q_1(x)q_2(x)\cdots q_t(x)$, then $s=t$ $p_i(x)=q_i(x)$

{Finite factor chain ($f(x)=0$ 时 $r_1r_2\cdots$) ✓

⇑

f is irr, then f is prime

$f(x)\in D[x]$ irreducible, $f|gh$, $\exists fy=gh$ a

- 若 deg f=0, 即 $f(x)=a\in D$, 代回 $a|gh$, $c(a)|c(gh)$

D is UFD $\therefore a|c(g)c(h) \Rightarrow a|c(g)$ or $a|c(h) \Rightarrow a|g$ or $a|h$

- deg f>0, find fraction field of D: 记为 K, f irr in D[x] $\therefore$ f irr in F[x] 上个定理 → pri在上面证过

F[x]是域 $\therefore$ 是UFD, then f is prime in F[x].

$f|gh$, $g,h\in D[x]\subseteq F[x]$ $\therefore f|g$ 或 $f|h$, 设 $f|g$ 即 $\exists fd=g$ $d\in F[x]$

$g=fd$, $\exists r\in R$ s.t $rd\in R[x]$, $rg=rd\cdot f$

设 $c(g)=s$, $c(rd)=t$, g和d可得到 primitive g_1,d_1 $rsg_1=td_1\cdot f$ $rs=tu^{-1}$ $g_1=d_1u^{-1}\cdot f$