2-26-25 (WEEK 2) Shun/翔海 (@shun4midx)

EUCLIDEAN DOMAINS

Today, R is an integral domain.

DEFINITION

- Any function $N: R \to \mathbb{N}$ with $N(0)=0$ is called a **norm** on R
- N is **positive** if $N(a)>0$ $\forall a \neq 0$
- R is called a **Euclidean domain** if $\exists$ a norm N on R, s.t. $\forall a, 0\neq b \in R$, $\exists q, r \in R$, s.t. $a=qb+r$ and $r=0$ or $N(r)<N(b)$

  For example: $R=\mathbb{Z}$, $F[x]$, $\underline{F} \leftarrow N(a)=0\ \forall a \in F$, $\forall a, 0\neq b \in F$, $a=ab^{-1}b+0$
- **Euclidean Algorithm** for R being a ED: For $a, 0\neq b \in R$, $a=q_1 b+r_1, \dots, r_1=q_3r_2+r_3, \dots \Rightarrow \exists k$, s.t. $r_{k+1}=0$ otherwise $0 \leq N(b) > N(r_1) > N(r_2) > \dots$

FACT

$r_k = \gcd(a,b)$

Proof

Let $A(x)=\begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix}$, $A(x)^{-1}=\begin{pmatrix} 0 & 1 \\ 1 & -x \end{pmatrix}$. We find that $(a\ b)=(b\ r_1)A(q_1)$, $(b\ r_1)=(r_1\ r_2)A(q_2)$, $\dots$, $(r_{k-1}\ r_k)=(0\ k)A(q_{k+1})$

$\therefore$ We have $(a\ b)=(r_k\ 0)A(q_{k+1})A(q_k)\dots A(q_1) \Rightarrow (r_k\ 0)=(a\ b)A(q_1)^{-1}A(q_2)^{-1}\dots A(q_{k+1})^{-1}$

From the LHS, we can deduce $r_k | a$, $r_k | b$. From the RHS, we can deduce $r_k = ta+sb$ and "$c|a, c|b \Rightarrow c | ta+sb = r_k$"

DEFINITION

$A_D :=$ the ring of integers in the quadratic field $\mathbb{Q}(\sqrt{D})$ with $D\neq 1$, D being square-free.

$= \{\alpha \in \underbrace{\mathbb{Q}(\sqrt{D})}_{p+q\sqrt{D},\ p,q\in\mathbb{Q}} \mid \alpha$ is **integral** over $\mathbb{Z}\}$, i.e. $\underbrace{\alpha^n + a_1\alpha^{n-1} + \dots + a_n}_{f(b)} = 0$, $a_i \in \mathbb{Z}$

THEOREM

- If $D \equiv 1 \pmod 4$, $A_D = \{a+b(\frac{1+\sqrt{D}}{2}) = \frac{2a+b}{2} + \frac{b}{2}\sqrt{D}\}$
- If $D \equiv 2,3 \pmod 4$, $A_D = \{a+b\sqrt{D} \mid a,b \in \mathbb{Z}\}$

Proof

Let $\alpha = p+q\sqrt{D} \in A_D$, $\underline{p, 0\neq q \in \mathbb{Q}}$ — $q=0$, $x-p$

Notice, $\alpha - p \in q\sqrt{D} \Rightarrow (\alpha-p)^2 = \underbrace{\alpha^2 - 2\alpha p + p^2}_{g(\alpha)} = q^2 D \Rightarrow \alpha^2 - 2\alpha p + (p^2-q^2D)$

Note: In $\mathbb{Q}[x]$, $\mathbb{Z}[x] \ni f(x) = q(x)g(x) + (ax+b)$

$f(\alpha)=0$, $g(\alpha)=0 \Rightarrow a\alpha+b=0 \Rightarrow a=0, b=0$, i.e. $f(x)=q(x)g(x)$. All are monic $\Rightarrow g(x)\in\mathbb{Z}[x]$ by Gauss Lemma

If p is even $\Rightarrow p \in \mathbb{Z} \Rightarrow q \in \mathbb{Z}$. Since $p^2-q^2D \in \mathbb{Z}$, D is square-free, $\therefore q^2D \in \mathbb{Z}$

If p is odd, say $2p=2m+1 \Rightarrow (2p)^2 \equiv (2m+1)^2 \pmod 4 \Rightarrow 4(\underbrace{p^2-q^2D}_{\in\mathbb{Z}}) \equiv 0 \pmod 4$ $\therefore 4p^2 \equiv 4q^2D \equiv 1 \pmod 4 \Rightarrow q \notin \mathbb{Z}$, $q=\frac{2n+1}{2}$. Also, $4q^2D = (2n+1)^2 D \equiv 0 \pmod 4$

THEOREM

A_D is an ED if $D=2,3,5,-1,-2,-3,-7,-11$

Proof

Define $N': \mathbb{Q}(\sqrt{D}) \longrightarrow \mathbb{Q}$ and $N: A_D \longrightarrow \mathbb{N}$

$\alpha = p+q\sqrt{D} \longmapsto (p+q\sqrt{D})(p-q\sqrt{D}) = p^2-q^2D$ $\qquad \alpha \longmapsto |N'(\alpha)| = |p^2-q^2D|$ — prevent negative values

Now, for $\alpha, 0\neq\beta \in A_D$, $\frac{\alpha}{\beta} = x+y\sqrt{D}$, $x,y \in \mathbb{Q}$

- $D=2,3,-2,-1$: Choose $a,b \in \mathbb{Z}$, s.t. $|x-a| \leq \frac{1}{2}$, $|y-b| \leq \frac{1}{2}$

  If $\lambda = a+b\sqrt{D}$, then $|N'(\frac{\alpha}{\beta}-\lambda)| = |(x-a)^2-(y-b)^2D|$.

  $D=2,3$: $\leq (y-b)^2 D \leq \frac{D}{4} < 1$

  $D=-2,-1$: $\leq (x-a)^2 + (y-b)^2|D| \leq \frac{1}{4} + \frac{|D|}{4} \leq \frac{3}{4} < 1$

Shun/羊羽海(@shun4midx)

KEY: We need $|N'(\frac{\alpha}{\beta}-\lambda)|<1$, then we can divide easily

Let $w=\alpha-\lambda\beta$, $N(w)=|N'(\beta)N'(\frac{\alpha}{\beta}-\lambda)|<|N'(\beta)|=N(\beta)$

$|y-\frac{b}{2}|\le\frac{1}{4}$

- $D=5,-3,-7,-11$: Choose $a,b\in\mathbb{Z}$, s.t. $|2y-b|\le\frac{1}{2}$, $|x-a-\frac{b}{2}|\le\frac{1}{2}$.
  If $\lambda=a+b(\frac{1+\sqrt{D}}{2})$, then $|N'(\frac{\alpha}{\beta}-\lambda)|=|(x-a-\frac{b}{2})^2-(y-\frac{b}{2})^2D|\le\frac{1}{4}+\frac{|D|}{16}<1$

DEFINITION

Let $N:R\longrightarrow\mathbb{N}$ be a norm. N is a **Dedekind-Hasse norm** if N is positive and $\forall a, 0\ne b\in R$, either $b|a$ or $\exists s,t\in R$, s.t. $0<N(sa-tb)<N(b)$

FACT

R is a ED with N being positive $\Rightarrow$ N is a Dedekind-Hasse norm ($s=1$, $t=q$)

THEOREM

generated by 1 element (i.e. the ring version of cyclic groups)

R has a D-H norm $\Rightarrow$ R is a PID

Proof

Let $I\ne\{0\}$ and $d\in I$, $N(d)=\min\{N(a)\,|\,0\ne a\in I\}$

Claim: $I=\langle d\rangle$

Proof

$\forall 0\ne a\in I$, $\forall s,t\in R$, $sa-td\in I\Rightarrow N(sa-td)\ge N(d)$ $\therefore$ By def of D-H norm, then $d|a$, i.e. $a\in\langle d\rangle$ $\square$

DEFINITION

$\tilde{R}:=\underbrace{R^\times}_{\text{units}}\cup\{0\}$, $u\in R\setminus\tilde{R}$ is called a **universal side divisor** if $\forall x\in R$, $\exists r\in\tilde{R}$, s.t. $u|x-r$

FACT

$R\ne\tilde{R}$

R is a ED but not a field $\Rightarrow$ R has a universal side divisor

Proof

Define $N(u):=\min\{N(a)\,|\,a\in R\setminus\tilde{R}\}$. $\forall x\in R$, $\exists q,r$, s.t. $x=qu+r$
- If $r=0$, then $u|x-0$ ✓
- If $r\ne0$, then $r=x-qu\notin R\setminus\tilde{R}$ since $N(r)<N(u)\Rightarrow r\in\tilde{R}$

KEY EXAMPLE

A_{-19} is a PID but not a ED

Proof

TL;DR, we need "A_{-19} has a D-H norm" (PID) and "A_{-19} has no universal side divisor" (ED 否)

Claim: A_{-19} has a D-H norm

Proof

Recall: $N: A_{-19}\longrightarrow\mathbb{N}$

$$a+b(\tfrac{1+\sqrt{-19}}{2})\longmapsto|(a+\tfrac{b}{2})^2+\tfrac{b^2}{4}(19)|=|a^2+ab+5b^2|$$

$\because -19\equiv1\pmod 4$

Given $0\ne\alpha$, $0\ne\beta\in A_{-19}$, suppose $\beta\nmid\alpha$, i.e. $\frac{\alpha}{\beta}\notin A_{-19}$. We hope "$\exists s,t\in A_{-19}$, s.t. $0<N(s\alpha-t\beta)<N(\beta)$, i.e. $0<|N'(s(\frac{\alpha}{\beta}-t))|<1$"

We write $\frac{\alpha}{\beta}=\frac{a+b\sqrt{-19}}{c}$, $a,b,c\in\mathbb{Z}$, $c>1$, $\gcd(a,b,c)=1$.

$\Rightarrow\begin{cases}\exists x,y,w\in\mathbb{Z}, \text{ s.t. } ya+xb-wc=1\\ \exists z,r\in\mathbb{Z}, \text{ s.t. } xa-19yb=cz+r \text{ with } |r|\le\frac{c}{2}\end{cases}$

i.e. instead of $7=1\times4+3$, we write $7=2\times4+(-1)$, since $3>\frac{4}{2}$

Let $s=x+y\sqrt{-19}$, $t=z+w\sqrt{-19}$, we get $0<|N'(s(\frac{\alpha}{\beta})-t)|=\frac{(xa-19yb-cz)^2}{c^2}+\frac{19(ya+xb-wc)^2}{c^2}\le\frac{1}{4}+\frac{19}{c^2}<1$ for $c<5$

For $c=5$, $|r|\le2$, then $\frac{r^2}{c^2}+\frac{19}{c^2}\le\frac{4+19}{25}<1$

For $c=2$, $a\not\equiv b\pmod 2$ (coprime) $\Rightarrow(a-1)\equiv b\pmod 2$. Take $s=1$, $t=\frac{(a-1)+b\sqrt{-19}}{c}\in A_{-19}\Rightarrow|N'(\frac{\alpha}{\beta}-t)|=\frac{1}{4}<1$

For $c=3$, $a\equiv b\equiv0\pmod 3$ is false $\Rightarrow a^2+b^2\not\equiv0\pmod 3\Rightarrow a^2+19b^2\not\equiv0\pmod 3$, say $a^2+19b^2=3q+r$, $r=1$ or 2.
  Set $s=a-b\sqrt{-19}$, $t=q$, then $0<|N'(s(\frac{\alpha}{\beta})-t)|=|(\frac{a^2+19b^2}{3}-q)|^2=(\frac{r}{3})^2<1$

For $c=4$, One of a,b is odd, the other is even. $\therefore a^2+19b^2$ is odd. Write $a^2+19b^2=4q+r$, $r=1$ or 3.
  Set $s=a-b\sqrt{-19}$, $t=q$. Then, $|N'(s(\frac{\alpha}{\beta})-t)|=(\frac{a^2+19b^2}{4}-q)^2=(\frac{r}{4})^2<1$
  a and b are both odd. $\therefore a^2+19b^2\equiv4\pm3\pmod 8$. Set $s=\frac{a}{2}-\frac{b}{2}\sqrt{-19}$, $t=q$. Then, $0<|N'(s(\frac{\alpha}{\beta})-t)|=(\frac{a^2+19b^2}{8}-q)^2=(\frac{4}{8})^2<1$

$\therefore$ In conclusion, A_{-19} has a D-H norm. $\square$

Shun/翔海(@shun4midx)

Claim: A_{-19} has no universal side divisor

Proof

Suppose that u is a usd.

Let $\overset{\text{cannot for } x=2 \Rightarrow \text{ not OK for some } x}{\underline{x=2}}$. Then, $u \mid 2 \pm \underline{0}$ or $u \mid 2 \pm \overset{\text{unit}}{\underline{1}}$ in A_{-19}, i.e. $u \mid 2$ or $u \mid 3$

↳ If $u \mid 2$, then we have $2 = u\alpha \Rightarrow N(2) = N(u)N(\alpha) \Rightarrow 4 = N(u)N(\alpha)$ with $N(\alpha) \geq 5$ ($\because \alpha$ is not a unit) $\therefore N(u) \leq 4 \Rightarrow u = \pm 2$

↳ If $u \mid 3$, then we have $3 = u\alpha \Rightarrow 9 = N(u)N(\alpha) \Rightarrow N(u) = 3$ or $9 \Rightarrow u = \pm 3$

However, for $x = \frac{1+\sqrt{-19}}{2} \in A_{-19}$, we must have "$\underbrace{\pm 2, \pm 3}_{\text{Possible } u} \mid x, x \pm 1$", but $N(x) = \frac{1}{4} + \frac{19}{4} = 5$, $N(x+1) = \frac{9}{4} + \frac{19}{4} = 7$, but $N(\pm 2) = 4$, $N(\pm 3) = 9$ ※

$\therefore$ By contradiction, A_{-19} has no universal side divisor. $\square$