第5章 整环内的因子分解理论

第5.1节 唯一分解整环的概念

1. 自反性：显然 $a \sim a$

对称性 显然 $a \sim b \Leftrightarrow b \sim a$

传递性：若 $a,b,c \neq 0$，$a \sim b$，$b \sim c$ 则 $a|b$，$b|c$，$b|a$，$c|b$

故 $a|c$，$c|a$ 故 $a \sim c$。

2. 证明 $\Rightarrow$ 若 $a \sim b$，则 $a|b$，故存在 $u \in R$ 使得 $b = au$ 故 $b = bcu$

由 R 是整环有消去律，因此 $cu = 1$，故 u 可逆。

[另由命题5.1.1，由 $a \sim b \Leftrightarrow$ 存在 $u \in R^\times$，使得 $a = bu$ 故 $bu = bc$

$\Rightarrow u = c \in R^\times$ 故 c 是可逆元]

$\Leftarrow$ 由 c 是可逆元，$a = bc$，$ac^{-1} = bcc^{-1} = b$ 故 $b|a$，$a|b$

因此 $a \sim b$。

3. 由高斯整环 $\mathbb{Z}[i]$ 的乘法单位群 $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$

由命题5.1.1(1)知 $a+bi$ 相伴的所有元素为 $\begin{cases} \pm(a+bi) \\ \pm i(a+bi) = \mp(b+ai) \end{cases}$

4. 的证明：设 $\alpha = a+b\sqrt{-3}$ $(a,b \in \mathbb{Z})$，$\in \mathbb{Z}[\sqrt{-3}]$，$N(\alpha) = a^2+3b^2$ 为非负整数 $(\in \mathbb{Z}_{\geq 0})$

由命题5.1.4，α 可逆 $\Leftrightarrow N(\alpha) = 1$ 解得 R 能有 $a = \pm 1$，$b = 0$，故 $R^\times = \{\pm 1\}$

由 $N(2) = N(1+\sqrt{-3}) = N(1-\sqrt{-3}) = 4$，假设2可约，则 R 中存在不可逆元 s.t. 使得 $2 = \xi\eta$ 由命题5.1.4得 $N(2) = 4 = N(\xi)N(\eta)$，$N(\xi) > 1$，$N(\eta) > 1$。

R 能有 $N(\xi) = N(\eta) = 2$，但不存在整数 a,b，使得 $a^2+3b^2 = 2$，故 R 中不存在范数为2的元素，矛盾，故2是不可约元。

$1+\sqrt{-3}$，$1-\sqrt{-3}$ 同理

用为 2，$1+\sqrt{3}$ 是不可约元，故 2 的全部因子为 $\pm 1, \pm 2$，$1+\sqrt{3}$ 的全部因子为 $\{\pm 1, \pm(1+\sqrt{3})\}$

$1-\sqrt{3}$ 的全部因子为 $\{\pm 1, \pm(1-\sqrt{3})\}$. 于是 $2 \nmid 1+\sqrt{3}$，$1+\sqrt{3} \nmid 2$.

而由 $4=2\cdot 2=(1+\sqrt{3})(1-\sqrt{3})$ 知 $2 \mid (1+\sqrt{3})(1-\sqrt{3})$，$1+\sqrt{3} \mid 2\cdot 2$

故 2，$1+\sqrt{3}$ 不为素元.

(2). 由(1) $4=2\cdot 2=(1+\sqrt{3})(1-\sqrt{3})$ (不相伴)

右两乘为不可约元乘积的方式不唯一，故 R 不是唯一分解整环

(3). 假设最大公因子为 d. 由 $4=2\cdot 2=(1+\sqrt{3})(1-\sqrt{3})$

易知 4 与 $2(1+\sqrt{3})$ 有公因子 2 和 $(1+\sqrt{3})$，从而有

$2 \mid d$，$(1+\sqrt{3}) \mid d$，$d \mid 4$，$d \mid 2(1+\sqrt{3})$

$[\because d=(4, 2(1+\sqrt{3}))]$

由 $2 \mid d$；令 $d=2t$ $(t \in R)$，由 $d \mid 4$ 知 $t \mid 2$.

由 2 是 R 的不可约元，知 $t=\pm 1$，或 ± 2.

若 $t=\pm 1$，则 $d=\pm 2$，于是 $(1+\sqrt{3}) \mid 2$ 与 2 是不可约元矛盾.

若 $t=\pm 2$ 则 $d=\pm 4$ 于是 $4 \mid 2(1+\sqrt{3}) \Rightarrow 2 \mid (1+\sqrt{3})$，与 $(1+\sqrt{3})$ 为不可约元矛盾.

故无中不存在 4 和 $2(1+\sqrt{3})$ 的最大公因子

5. 证明：d 是 $\mathbb{Z}[\sqrt{2}]$ 的可约元，则存在 s, t (不可逆)

使得 $d=st$. 由命题 5.1.4，$N(s)$ 和 $N(t)$ 为不等于 ± 1 的整数.

且 $N(s)N(t)=N(d)=p$ 其 p 为素数. 显存 $N(s), N(t)$ 均有一为 ± 1 矛盾.

故 d 为 $\mathbb{Z}[\sqrt{2}]$ 的不可约元

6. 同上一题. $\mathbb{Z}[i]=\mathbb{Z}[\sqrt{-1}]$ $N(1+i)=2$ 为素数 故 $1+i$ 是不可约元

7. 反证. 若 $f(x)$ 可约，则存在 $g(x), h(x)$ 为 $F_3[x]$ 中不可逆元素，使得 $f(x)=g(x)h(x)$.

易知 $\deg g(x)=\deg h(x)=1$. 不妨设 $g(x)=x-a$. $a \in F_3$. 则有 $f(a)=0$.

由 $a \in \{0,1,2\}$ $f(0)=1$、$f(1)=2$，$f(2)=2$，均不为 0，矛盾.

故 $f(x)$ 在 $F_3[x]$ 中不可约

8. (1) 若 $p(x)$ 是零次不可约元，设 $p(x)=c$ 比是 >1 的.

若 c 不是素数，则 $c=mn$，$p(x)$ 有非平凡分解. 故 $p(x)$ 不是不可约元.

若 c 是素数 设 $p(x)=c=f(x)g(x)$，只能 $\deg f(x)=\deg g(x)=0$. 由 c 是素数.

故有 $f(x)=\pm 1$ 或 $g(x)=\pm 1$，因此 $p(x)$ 为 0 次不可约元从而 $p(x)=\pm p$ p 为素数.

若 $p(x)$ 是次数 ≥ 1 的不可约元，设 $p(x)=a_nx^n+\cdots+a_1x+a_0$ $(n\geq 1)$.

若 $(a_0,a_1,\cdots a_n)=d>1$. 则 $p(x)=d\left(\frac{a_n}{d}x^n+\cdots+\frac{a_1}{d}x+\frac{a_0}{d}\right)$ 是 $p(x)$ 的一个非平凡分解，每 $p(x)$ 是不可约元矛盾，从而 $(a_0,a_1,\cdots,a_n)=1$ 故 $p(x)$ 是本原多项式.

(2). 显然 $\times$ 满且不可逆，若 $x\mid f(x)g(x)$，$f(x),g(x)\in\mathbb{Z}[x]$.

设 $f(x)$，$g(x)$ 的常数项分别为 a,b，则 $f(x)g(x)$ 的常数项 $ab=0$.

故 $a=0$ 或 $b=0$. 故 $x\mid f(x)$ 或 $x\mid g(x)$. 因此 x 是 $\mathbb{Z}[x]$ 的素元.

9. (1) 证明 ~~要~~ 当 $f(x)=0$ 时 显然成立. ~~要证~~

令 $f(x)=b_nx^n+b_{n-1}x^{n-1}+\cdots+b_1x+b_0$

令 $q(x)=c_{n-1}x^{n-1}+c_{n-2}x^{n-2}+\cdots+c_1x+c_0$

则 $q(x)(x-a)+f(a)=c_{n-1}x^n+c_{n-2}x^{n-1}+\cdots+c_1x^2+c_0x$

$\quad -ac_{n-1}x^{n-1}-c_{n-2}x^{n-2}+\cdots-ac_1x-ac_0+f(a)$

$=c_{n-1}x^n+(c_{n-2}-ac_{n-1})x^{n-1}+\cdots+(c_1-ac_2)x^2+(c_0-ac_1)x+f(a)-ac_0$

$=b_nx^n+b_{n-1}x^{n-1}+\cdots+b_1x+b_0$

故令 $c_{n-1}=b_n$，$c_{n-2}=b_{n-1}+ac_{n-1}$，$\cdots$，$c_0=b_1+ac_1$，$f(a)-ac_0=b_0$

故 $q(x)\in F(x)$ 存在

故 $(x-a)\mid f(x)$ 的充要条件是 a 是 $f(x)$ 的一个根. (显然) □

$f(a)=ac_0+b_0$

$=a(b_1+ac_1)+b_0$

$=a^2c_1+ab+b_0$

$\vdots$

$=f(a)$ √

12). 由(1) 若 $(x-a)\mid f(x)$ 的充要条件是 a 是 $f(x)$ 的 k 个根

若 $f(x)$ 有 $n+1$ 个根 $a_1, a_2, \cdots, a_{n+1}$, 则 $(x-a_k)\mid f(x)$ $(k\le n+1)$

故 $f(x)=(x-a_1)(x-a_2)\cdots(x-a_{n+1})\cdot q(x)$

故 $\deg f(x)\ge n+1$ 与 $\deg f(x)=n$ 矛盾. 故 $f(x)$ 在 F 内最多有 n 个根 □

10: 证明 设 $d=(a_1, a_2, \cdots, a_n)$ 且 r 是与 d 相伴的数 $r\sim d$.

故存在可逆元 $u\in R$ 使得 $r=du$

(故对任意 $a_1, a_2 \cdots a_n$ 的公因子 c 由 $c\mid d$, $d\mid du$ 得 $c\mid r$

~~证明~~

由 $d\mid a_i$ $(i\le n)$ 则 $a_i=q_i\cdot d=q_i r\cdot u^{-1}$ 故 $r\mid a_i$)

因此 r 是 $a_1, a_2, \cdots a_n$ 的最大公因子

又若是 $a_1, a_2, \cdots a_n$ 的任一最大公因子, 则由 d 是 $a_1, \cdots a_n$ 的最大公因子.

故 $t\mid d$, $d\mid t$, 因此. d 与 t 相伴, $d\sim t$

因此最大公因子如果存在, 则在相伴的意义下是唯一的 □

11 证明:

(1) 由 R 是唯一分解整环 令 $c\mid a$, $c\mid b$. 则 $c=wp_1^{h_1}p_2^{h_2}\cdots p_t^{h_t}$ $h_i\ge 0$ 且 w 是可逆元

故存在 $z_1, z_2\in R$ 使得

$a=z_1 c$ 即 $up_1^{e_1}\cdots p_t^{e_t}=z_1 w p_1^{h_1}p_2^{h_2}\cdots p_t^{h_t}$

$b=z_2 c$ 即 $vp_1^{f_1}\cdots p_t^{f_t}=z_2 w p_1^{h_1}p_2^{h_2}\cdots p_t^{h_t}$

由 z_1, z_2 均可分解. 故存在 $h_i\le \min\{e_i, f_i\}$

因此 $c\mid \prod_{i=1}^{t} p_i^{\min\{e_i, f_i\}}$ 又因为 $\prod_{i=1}^{t} p_i^{\min\{e_i, f_i\}}\mid a$ 且 $\prod_{i=1}^{t} p_i^{\min\{e_i, f_i\}}\mid b$.

故 $\prod_{i=1}^{t} p_i^{\min\{e_i, f_i\}}=(a,b)$. □

(2) 同理. 令 $a\mid c$, $b\mid c$ $c=wp_1^{h_1}p_2^{h_2}\cdots p_t^{h_t}$ 则可得 $h_i\ge \max\{e_i, f_i\}$.

又因为 $\prod_{i=1}^{t} p_i^{\max\{e_i, f_i\}}\mid c$ 因此 $\prod_{i=1}^{t} p_i^{\max\{e_i, f_i\}}=[a,b]$

□

13). 由 (a,b) 是与 $\prod_{i=1}^{k} p_i^{\min\{e_i,f_i\}}$ 相伴的元素

[a,b] 是与 $\prod_{i=1}^{k} p_i^{\max\{e_i,f_i\}}$ 相伴的元素.

由 $ab = uv\, p_1^{e_1+f_1} p_2^{e_2+f_2} \cdots p_k^{e_k+f_k}$, u,v 是可逆元.

而 (a,b)[a,b] 是与 $\prod_{i=1}^{k} p_i^{e_i+f_i}$ 相伴的元素.

因此 $ab \sim (a,b)[a,b]$ (相伴的传递性)

□

12. 若 a,b,c 中有零元为单元, 易证.

由只是给一个解整环, 故 $a = u\prod_{i=1}^{k} p_i^{r_i}$, $r_i \geq 0$, $i \leq k$

$b = v\prod_{i=1}^{k} p_i^{s_i}$ $s_i \geq 0$ $i \leq k$

$c = w\prod_{i=1}^{k} p_i^{t_i}$ $t_i \geq 0$ $i \leq k$.

其中 u,v,w 为可逆元, p_i 为不可约元.

由题知 $(a,b) = \prod_{i=1}^{k} p_i^{\min\{r_i,s_i\}} = 1$. 故 $\min\{r_i,s_i\} = 0$, $i \leq k$. 即 r_i, s_i 中至少有一个为 0

(1). 若 $a \mid bc$ 则对一切 i 都有 $r_i \leq s_i + t_i$ 对 Given 的 i 若 $r_i = 0$, 则 $r_i = 0 \leq t_i$

若 $s_i = 0$, 则 $r_i \leq t_i$, 故 $r_i \leq t_i$ 对任何都成立 即 $a \mid c$ □

(2) 若 $a \mid c$, $b \mid c$, 则对任何 i 都有 $r_i \leq t_i$, $s_i \leq t_i$, 对任给定的 i, 若 $r_i = 0$. 则 $r_i + s_i = s_i \leq t_i$

若 $s_i = 0$ 则 $r_i + s_i = r_i \leq t_i$, 故 $r_i + s_i \leq t_i$ 对任给的 i 均成立, 即 $ab \mid c$.

(3). 由题知. $(a,c) = \prod_{i=1}^{k} p_i^{\min\{r_i,t_i\}}$, $(b,c) = \prod_{i=1}^{k} p_i^{\min\{s_i,t_i\}}$, $(ab,c) = \prod_{i=1}^{k} p_i^{\min\{r_i+s_i,t_i\}}$

对任给定的 i, 若 $r_i = 0$, 则.

$\min\{r_i,t_i\} + \min\{s_i,t_i\} = 0 + \min\{s_i,t_i\} = \min\{0+s_i,t_i\} = \min\{r_i+s_i,t_i\}$.

若 $s_i = 0$, 同

$\min\{r_i,t_i\} + \min\{s_i,t_i\} = \min\{r_i+s_i,t_i\}$

即 $(a,c)(b,c) = \prod_{i=1}^{k} p_i^{\min\{r_i,t_i\}+\min\{s_i,t_i\}} = \prod_{i=1}^{k} p_i^{\min\{r_i+s_i,t_i\}} = (ab,c)$

□

5.2 主理想整环与欧几里得整环

1. 证明：

(1) (x^2+x+1) 是 $F_2[x]$ 中的不可约元. 若否, 则 x^2+x+1 可以分解为两个一次多项式的乘积. 设为 $x^2+x+1=(ax+b)(cx+d)$, $a,b,c,d\in\{0,1\}$

由 $(ax+b)(cx+d)=acx^2+(ad+bc)x+bd=x^2+x+1 \Rightarrow \begin{cases} ac=1 \\ ad+bc=1 \\ bd=1 \end{cases}$ 无解

因此 x^2+x+1 是 $F_2[x]$ 中的不可约元.

(2) 由 $F_2[x]$ 是主理想整环, 故 (x^2+x+1) 是 $F_2[x]$ 的极大理想

理想 $F_2[x]/(x^2+x+1)$ 是域.

$F_2[x]/(x^2+x+1)=\{ax+b \mid a,b\in F_2\}$ 共有 4 个元素. □

2. $F_3[x]/(x^2+x+1)$ 不为域

$x^2+x+1=(x-1)(x-1)=x^2-2x+1=x^2+x+1$.

故 x^2+x+1 不是不可约元.

由 $F_3[x]$ 是主理想整环 若 $F_3[x]/(x^2+x+1)$ 为域, 则 (x^2+x+1) 是极大理想

由命题 5.2.1 则 x^2+x+1 是不可约元 矛盾. 故 $F_3[x]/(x^2+x+1)$ 是域 □

3. 证明: $\Rightarrow$ 域 F 上的多项式环 $F[x]$ 是主理想整环 (例 5.2.3)

$\Leftarrow$ 令 $\varphi: R[x] \longrightarrow R$

$f(x) \longmapsto f(0)$

故 φ 是同态. 且 $\ker\varphi=(x)$ 由同态基本定理得 $R[x]/(x) \cong R$

(类似于例题 4.5.1)

证明 x 是 $R[x]$ 的不可约元. 设

$x=f(x)g(x)$ $f(x),g(x)\in R[x]$ $\deg f(x)\geq\deg g(x)$

故有 $\deg f(x)=1$, $\deg g(x)=0$. 设 $f(x)=ax+b$ $g(x)=c$ $(a,b,c\in R)$

即 $ac=1$, 故 c 可逆, 即 $g(x)$ 可逆. 于是 x 是 $R[x]$ 的不可约元

$R[x]$ 是主理想整环. 故 (x) 是 $R[x]$ 的极大理想. 故 $R[x]/(x)$ 是域. 故 R 是域 □

4. $\mathbb{Z}[i]=\{a+bi \mid a,b\in\mathbb{Z}\}$

证明：由 $\mathbb{Z}[i]$ 是欧几里德整环，是主理想整环，$a\neq 0$，且 a 不是零元的可逆元

故 a 是不可约元 $\Leftrightarrow$ a 是素元

(1) 若 $1+i$ 可逆，则存在 $a+bi$ 使得 $(1+i)(a+bi)=(a-b)+(a+b)i=1+i$.

$\Rightarrow \begin{cases} a-b=1 \\ a+b=1 \end{cases} \Rightarrow a=1,\ b=0$. 故 $1+i$ 不可逆.

由 $N(1+i)=2$ 为素数 故由引理 5.2.2，$1+i$ 是不可约元.

(2). $(3-2i)(a+bi)=1$ $\begin{cases} 3a+2b=1 \\ -2a+3b=0 \end{cases}$ $2a=3b$, $a=\frac{3}{2}b$ $\Rightarrow \frac{9}{2}b+\frac{b}{2}=1$

$18b+3b=6$ $b\notin\mathbb{Z}$ 不存在

故 $3-2i$ 不可逆

$N(3-2i)=9+4=13$ 素数 故 $3-2i$ 是不可约元.

(3) 由引理 5.2.1，$\pi\in\mathbb{Z}[i]$ 是不可约元. 则存在素数 $p\in\mathbb{Z}$, s.t. $\pi\mid p$.

若 $p=7=p$ 是素数，故 7 是不可约元

(4) ~~$2+5i=7$ 不在 $\mathbb{Z}[i]$ 中~~

~~$=(1+i)(2-3i)$~~

$(2+5i)(a+bi)=1 \Rightarrow \begin{cases} 2a-5b=1 \\ 2b+5a=0 \end{cases}$

$5a=-2b$, $a=-\frac{2}{5}b$ $-\frac{2}{5}b-5b=1$, $(25+4)b=5$, $b\notin\mathbb{Z}$

故 $2+5i$ 是不可逆元.

$N(2+5i)=25+4=29$ 素数 故 $2+5i$ 是不可约元.

5. 由 $\mathbb{Z}[i]=\{a+bi \mid a,b\in\mathbb{Z}\}$ 为主理想整环

$(a+bi)(1+i)=(a-b)+(a+b)i$

故 $(1+i)=\{(a-b)+(a+b)i \mid a,b\in\mathbb{Z}\}$

由 $a-b$ 与 $a+b$ 同奇偶，故得证

$a+b=a-b+2b$，$2b$ 偶数；$a-b$ 与 $a+b$ 同奇偶.

□

6. 由 $\mathbb{Z}[i]$ 是主理想整环，由 4 题知 $1+i$ 是 $\mathbb{Z}[i]$ 的不可约元.

故由命题 5.2.1. $(1+i)$ 是非零素理想.

故 $\mathbb{Z}[i]/(1+i)$ 是域.

$\varphi: \mathbb{Z} \longrightarrow \mathbb{Z}[i]/(1+i)$

$a \longmapsto a+(1+i)\mathbb{Z}[i]$

$\ker\varphi = (1+i)\cdot\mathbb{Z}[i] \cap \mathbb{Z}$

由 $(1+i)(a+bi) = a-b+(a+b)i \in \mathbb{Z} \Leftrightarrow a+b=0 \Leftrightarrow a=-b$

故 $\ker\varphi = \{-2b \mid b\in\mathbb{Z}\} = 2\mathbb{Z}$，由故 φ 是同态；

对 $\forall$ ~~$a+bi \in \mathbb{Z}[i]/(1+i)$~~ $a+bi+(1+i)\mathbb{Z}[i]$，有 $a+bi = a-b+b+bi = a-b+b(1+i)$

$\varphi(a-b) = a+bi+(1+i)\mathbb{Z}[i]$ φ 是满射.

由同态基本定理 $\mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}[i]/(1+i)$ 由 $\mathbb{Z}/2\mathbb{Z} \cong \mathbb{F}_2$ 为 2 元域 得证 □

7. $\Rightarrow$ 若 $(a,b)=(d)$ 则由 $(a,b) = (a)+(b) = \{xa+yb \mid x,y\in R\}$

故存在 $u,v\in R$，使得 $d=au+bv$. 因为 $a,b\in(d)$ 故 $d\mid a$，$d\mid b$

即 d 是 a,b 的公因子，若 d' 是 a,b 的任意公因子 则 $d'\mid(au+bv)$ 即 $d'\mid d$.

故 d 是 a,b 的一个最大公因子.

$\Leftarrow$ 设 a,b 的最大公因子，则 $d\mid a$，$d\mid b$. 且存在 $u,v\in R$，使得 $d=au+bv$.

故 $a,b\in(d)$，$d\in(a,b)$ 故 $(a,b)=(d)$ □

8. 证明：$1 = 0.x + \frac{1}{2}\cdot 2 \in (x,2)$ $\frac{1}{2}\notin\mathbb{Q}$

故 $(x,2) = (1) = \mathbb{Q}[x]$ 由第7题结论 $\gcd(x,2)=1$. □

9. 证明 由例 5.2.2. 在 $\mathbb{Z}[x]$ 中 $(2,x)$ 不是主理想故 $\gcd(x,2)=1$.

若存在 设 $\gcd(x,2)=m(x)$ 则 $m(x)\mid x$，$m(x)\mid 2$. 故 $(2,x)\subseteq(m(x))$

由 $m(x) = u(x)\cdot x + v(x)\cdot 2$ 故 $m(x)\in(2,x)$ 故 $(2,x)=(m(x))$ 矛盾 □

10. 反证：

若 $\mathbb{Z}[\sqrt{d}]$ 是欧几里得整环，则 $\mathbb{Z}[\sqrt{d}]$ 是主理想整环，但 $(2,\sqrt{d})$ 不是主理想（例 3.22）

故矛盾.

若 $\mathbb{Z}[\sqrt{3}]$，$\mathbb{Z}[\sqrt{5}]$ 是欧几里得整环则 其为唯一分解整环，但 $\mathbb{Z}[\sqrt{3}]$，$\mathbb{Z}[\sqrt{5}]$ 不是唯一分解整环，矛盾.（见例 5.1.3）（与习题 5.1.4）

$9=3\cdot 3=(2+\sqrt{5})(2-\sqrt{5})$ 与 $4=2\cdot 2=(1+\sqrt{3})(1-\sqrt{3})$

□

12. 一般的 $\mathbb{Z}[\sqrt{d}]$ 定义：$\delta=a+b\sqrt{d}\to|a-db^2|$ 范数

$\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ 定义为 $\delta=a+b\frac{1+\sqrt{d}}{2}\to a^2+ab+\frac{1+d}{2}b^2$

（见下页）

11. 类似与例 5.2.5.

对任意 $0\neq m+\sqrt{2}n\in\mathbb{Z}[\sqrt{2}]$，定义.

$d(m+\sqrt{2}n)=|N(m+\sqrt{2}n)|=|m^2-2n^2|\in\mathbb{Z}_{\geq 0}$　$d(m+\sqrt{2}n)$ 是 $m+\sqrt{2}n$ 的范数的绝对值

$\forall a=m+\sqrt{2}n$，$b=s+\sqrt{2}t\in\mathbb{Z}[\sqrt{2}]$，$s+\sqrt{2}t\neq 0$，

$\frac{a}{b}=x+\sqrt{2}y$. 其中 $\frac{m+\sqrt{2}n}{s+\sqrt{2}t}=\frac{(m+\sqrt{2}n)(s-\sqrt{2}t)}{(s+\sqrt{2}t)(s-\sqrt{2}t)}=\frac{ms-2tn+ns\sqrt{2}-mt\sqrt{2}}{s^2+2t^2}$

$x=\frac{ms-2tn}{s^2+2t^2}\in\mathbb{Q}$　$y=\frac{ns-mt}{s^2+2t^2}\in\mathbb{Q}$.

取 $g,h\in\mathbb{Z}$ 使 $|x-g|\leq\frac{1}{2}$　$|y-h|\leq\frac{1}{2}$

令 $q=g+h\sqrt{2}$，及 $r=a-qb=(\frac{a}{b}-q)b=(x+\sqrt{2}y-g-\sqrt{2}h)b$

$=((x-g)+(y-h)\sqrt{2})b$.

则 $q,r\in\mathbb{Z}[\sqrt{2}]$ 且 $a=qb+r$

若 $r\neq 0$ 则 $d(r)=|N((x-g)+(y-h)\sqrt{2})N(b)|$

$\leq|(\frac{1}{4}+\frac{2}{4})N(b)|\leq\frac{3}{4}d(b)<d(b)$.

故 $\mathbb{Z}[\sqrt{2}]$ 是欧几里得整环　□

12: 类似证明高斯整数环是Euclid环. 例 5.2.5 此第11题

$\mathbb{Z}[\sqrt{2}]$是$\mathbb{Q}[\sqrt{2}]$的子环.

任取 $\alpha=a+b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, $a,b\in\mathbb{Q}$. 定义 $\delta: \mathbb{Q}[\sqrt{-2}] \longrightarrow \mathbb{N}$

$$a+b\sqrt{2} \longmapsto a^2+2b^2.$$

$\alpha,\beta \in \mathbb{Q}[\sqrt{2}]$, $\Rightarrow \delta(\alpha\beta) = \delta(\alpha)\cdot\delta(\beta)$

任取 $\alpha,\beta \in \mathbb{Z}[\sqrt{2}]$, $\beta\neq 0$, 故 $\delta(\beta)\neq 0$. 即存在 $\beta^{-1}\in\mathbb{Q}[\sqrt{2}]$ 使得.

$\alpha\beta^{-1} = s+t\sqrt{2}$, 这里 $s,t\in\mathbb{Q}$, 显然存在 $m,n\in\mathbb{Z}$, 使得.

$|m-s|\leq\frac{1}{2}$, $|n-t|\leq\frac{1}{2}$.

令 $q=m+n\sqrt{2}$, $r=\beta[(s-m)+(t-n)\sqrt{2}] = \alpha-\beta q$

显然 $q,r\in\mathbb{Z}[\sqrt{2}]$, 并且 $\alpha=\beta q+r$.

同时 $\delta(r)=\delta(\beta)\delta((s-m)+(t-n)\sqrt{2}) = \delta(\beta)((s-m)^2+2(t-n)^2)$

$$\leq \delta(\beta)\left(\left(\frac{1}{2}\right)^2+2\left(\frac{1}{2}\right)^2\right) \leq \frac{3}{4}\delta(\beta) < \delta(\beta)$$

故 δ 是满足要求的 Euclid 函数. $\Rightarrow \mathbb{Z}[\sqrt{2}]$ 是 Euclid 环 □

13: 对任意 $0\neq m+\sqrt{3}n\in\mathbb{Z}[\sqrt{3}]$, 定义.

$d(m+\sqrt{3}n) = |N(m+\sqrt{3}n)| = |m^2-3n^2| \in \mathbb{Z}_{\geq 0}$ 范数的绝对值

对 $a=m+\sqrt{3}n$, $b=s+\sqrt{3}t\in\mathbb{Z}[\sqrt{3}]$, $b\neq 0$

则由 $\frac{a}{b}=x+\sqrt{3}y$, 即 $x=\frac{ms-3tn}{s^2+3t^2}\in\mathbb{Q}$, $y=\frac{ns-mt}{s^2+3t^2}\in\mathbb{Q}$.

先取 $g,h\in\mathbb{Z}$, s.t $|x-g|\leq\frac{1}{2}$, $|y-h|\leq\frac{1}{2}$

令 $q=g+h\sqrt{3}$, 及 $r=a-qb=(\frac{a}{b}-q)b=(x+\sqrt{3}y-g-\sqrt{3}h)b=((x-g)+(y-h)\sqrt{3})b$

于是 $q,r\in\mathbb{Z}[\sqrt{3}]$, 且 $a=qb+r$

若 $r\neq 0$ 则 $d(r)=|N((x-g)+(y-h)\sqrt{3})N(b)| \leq |(\frac{1}{4}+\frac{3}{4})N(b)| \leq |N(b)| = d(b)$.

若等号成立. 则有 $x=g$, $y=h$ 则 $x,y\in\mathbb{Z}$. 且 $r=0$ 与 $r\neq 0$ 矛盾.

若当 $r\neq 0$ 时 $d(r)<d(b)$

于是 $\mathbb{Z}[\sqrt{3}]$ 是欧几里得整环 □

14: 由 d 是 a,b 在 R 中的最大公因子，R 是主理想整环

则 由 $d|a$, $d|b$. 有 $(a,b)\subseteq(d)$.

存在 $u,v\in R\subseteq D$ 使得 $d=ua+vb$ 故 $(d)\subseteq(a,b)$.

因此 $(a,b)=(d)$. 且在主理想整环 D 中 ($D\supseteq R$) 仍成立.

故 d 也是 a,b 在 D 中的最大公因子

□