抽象代数学

我们推广 $\mathbb{Z}$上整除性理论

定义1 设R是整环(含幺交换), $a,b\in R$, 若存在 $c\in R$, 使得 $b=ac$, 则称a是b的因子, a整除b, 记作 $a|b$. 若 $a,b\neq 0$ 且 $a|b$, $b|a$, 则a与b相伴 (associates of each other)

性质: (1) $a|b$, $b|a$ ($b\neq 0$) $\Leftrightarrow$ 存在可逆元 $c\in R$, $a=bc$. (c也称为单位)

(2) $a|b, a|c \Rightarrow a|b+c$, $a|b, b|c \Rightarrow a|c$

(3) $a|b \Leftrightarrow (b)\subseteq(a)$, $a\sim b \Leftrightarrow (a)=(b)$

证明: (1) $a|b \Rightarrow \exists d$, $b=ad$, $b|a \Rightarrow \exists e$, $a=be$

$\Rightarrow b=bed \Rightarrow ed=1$

定义2 设R是整区, $a_1,\cdots,a_n,b\in R$. 若 $b|a_i$ $i=1,\cdots,n$ 则称b是 $a_1,\cdots,a_n$ 的公因子. 若d是 $a_1,\cdots,a_n$ 的公因子且任一公因子整除d, 则称d是 $a_1,\cdots,a_n$ 的最大公因子. 记作 $d=g.c.d(a_1,\cdots,a_n)$ 或 $d=(a_1,\cdots,a_n)$.

同理, 定义 $a_1,\cdots,a_n$ 的公倍式和最小公倍式, 记作 $c=l.c.m(a_1,\cdots,a_n)$ 或 $c=[a_1,\cdots,a_n]$

例 $R=\mathbb{Z}[i]=\{a+bi \mid a,b\in\mathbb{Z}\}$ 5有真因子:

$1\pm 2i$, $-1\pm 2i$, $2\pm i$, $-2\pm i$

R的单位是 $1, -1, i, -i$

上述真因子 $2\pm i = i(-1\pm 2i)$ $\quad -1\pm 2i = -(1\mp 2i)$

不相伴真因子：$1\pm 2i$

例 $R=\mathbb{Z}[\sqrt{-5}]$ $\quad 9 = 3\cdot 3 = (2+\sqrt{-5})(2-\sqrt{-5})$

3的因子：设 $3=(a+b\sqrt{-5})(c+d\sqrt{-5})$ 两边取共轭

$3=(a-b\sqrt{-5})(c-d\sqrt{-5})$

$\Rightarrow 9 = (a^2+5b^2)(c^2+5d^2) = 25b^2d^2+\cdots$

$\Rightarrow bd=0$，设 $b\neq 0, d=0$，$5b^2<9 \Rightarrow b=\pm 1 \Rightarrow a=\pm 2$

$\Rightarrow c=\pm 1$ 即 $3=\pm(a+b\sqrt{-5})$ 矛盾. 同理 $d\neq 0$ 也

得到矛盾. $\Rightarrow$ 3只有平凡因子 $\pm 1, \pm 3$.

同理 $2\pm\sqrt{-5}$ 只有平凡因子.

定义 设R整区，$a\in R$称为不可约元(irreducible element)

$\Leftrightarrow a\neq 0$，a不是单位且 $a=bc$ 暗示b或c是单位.

a称为素元(prime element) 若 $a\neq 0$，不是单位，若$a|bc$

则$a|b$或$a|c$.

性质：(1) 非零素元是不可约元. 设$p\in R$是素元，且

$p=rs$，$\Rightarrow p|rs \Rightarrow p|r$或$p|s$ 假设$p|r$ 则$r=pa$

$\exists a\in R$，$p=pas \Rightarrow as=1 \Rightarrow s$是单位.

(2) 不可约元未必是素元

例如 $R=\mathbb{Z}[\sqrt{-5}]$ 3是不可约元 $3 \mid 9=(2+\sqrt{-5})(2-\sqrt{-5})$

但 $3 \nmid 2\pm\sqrt{-5} \Rightarrow$ 3不是素元

定义 R整区，R满足下列条件

(1) $\forall a\neq 0\in R$，a非单位，则a可以写成R中有限个不可约元的乘积

(2) 若 $a=p_1p_2\cdots p_r=q_1q_2\cdots q_s$，$p_i, q_j$ 均为不可约元，则 $s=r$ 且 $q_1,\cdots,q_s$ 是 $p_1,\cdots,p_s$ 的一个重排的相伴元.

则R称为唯一分解整环(unique factorization domain)

UFD

例 $\mathbb{Z}$是一个UFD

$\mathbb{Z}[\sqrt{-5}]$不是一个UFD　　$9=(2+\sqrt{-5})(2-\sqrt{-5})=3\cdot 3$

定理 设R是整区，则R是唯一分解整环 $\Longleftrightarrow$

(1) $\forall a\neq 0\in R$，a非单位，则a可表示为有限个不可约元的乘积 (2) R中不可约元是素元.

证明："$\Rightarrow$" 设 $a\in R$ 是不可约元，且 $a\mid bc$，$b,c\neq 0$ 均不是单位，因为R是一个UFD. $b=b_1\cdots b_m$，$c=c_1\cdots c_m$ b_i, c_j 均是不可约元，$a\mid b_1\cdots b_m c_1\cdots c_n$，$\exists\, d=d_1\cdots d_l$ d_i 是不可约

元、$i=1,\cdots,l$　　$ad=bc$

即 $ad_1\cdots d_l=b_1\cdots b_m c_1\cdots c_n$ 由分解唯一性，a和某个b_i或c_j相伴，则$a|b$或$a|c$.

"$\Leftarrow$" 设$a\neq 0\in R$，a不是单位．设a的所有分解中不可约因子最少的个数为n.

若$n=1$，则a不可约，若$a=q_1\cdots q_m$　q_i不可约，则 $a|q_1\cdots q_m$ 由于a也是素元，存在q_j，$a|q_j$，$q_j|a$

即 $a\sim q_j$ 此时$m=1$.（否则其余q_t是单位）

假设对于$n-1$，a分解唯一 $\to$ p_i,q_j不可约

当 $a=p_1p_2\cdots p_n=q_1\cdots q_m$ $(m\geq n)$，$p_1|q_1\cdots q_m$

p_1是素元，存在q_i　$p_1|q_i$　$\exists c$　$q_i=p_1c$　但q_i不可约

c是单位$\Rightarrow p_1\sim q_i$　两边消去p_1,q_i

$b=p_2\cdots p_n=cq_1\cdots q_{i-1}q_{i+1}\cdots q_m$　由假设，$n-1=m-1$

调换位置，可得$p_j\sim q_j$.

例 $\mathbb{Z}[\sqrt{-3}]$　　$4=2\times 2=(1+\sqrt{-3})(1-\sqrt{-3})$

2是不可约元：设$2=(a+b\sqrt{-3})(c+d\sqrt{-3})\Rightarrow 4=(a^2+3b^2)(c^2+3d^2)$

$a^2+3b^2\leq 4\Rightarrow b=0,a\leq 2$ 或 $b=1,a=1\Rightarrow c=\pm 1,d=0$.

2不是素元　$2|4$ 但 $2\nmid 1\pm\sqrt{-3}\Rightarrow\mathbb{Z}[\sqrt{-3}]$非UFD.

定理 R整区，R是UFD ~~当~~ R是任意两非零元$a, b\in R$ a, b不是单位，则$g.c.d(a,b)$存在，同样地，$l.c.m(a,b)$存在.

证明：设$a=up_1^{e_1}p_2^{e_2}\cdots p_n^{e_n}$，$b=vp_1^{f_1}p_2^{f_2}\cdots p_n^{f_n}$

$u, v\in R$是单位，$p_1,\cdots,p_n$互异素元 $e_i, f_i\geq 0$

则 $(a,b)=p_1^{\min(e_1,f_1)}p_2^{\min(e_2,f_2)}\cdots p_n^{\min(e_n,f_n)}$

例 $R=\mathbb{Z}[\sqrt{-5}]$中 $a=3(2+\sqrt{-5})$，$b=9$ 不存在$gcd(a,b)$

否则 设$d=gcd(a,b)$ $3|d$，$2+\sqrt{-5}|d$

$d=3e$ $e\in R$，$d|9\Rightarrow e|3$，前面展示3不可约.

$e=\pm 3$或± 1. 若$e=\pm 1$ $\Rightarrow d=\pm 3$ 但$2+\sqrt{-5}|\pm 3$ 不可能!

若$e=\pm 3$ $d=\pm 9\Rightarrow d|a\Rightarrow 3|2+\sqrt{-5}$ 不可能!

例 $R=\dfrac{\mathbb{Q}[x,y]}{(f(x,y))}$ $f(x,y)$是$\mathbb{Q}[x,y]$中不可约多项式

$\mathbb{Q}[x,y]$唯一分解整环$\Rightarrow f(x,y)$是素元$\Rightarrow R$是整区

例 设R是UFD，若$a,b,c\in R$满足$(a,b)=1$，$a|bc$ 则$a|c$.

证明：设 $b=p_1p_2\cdots p_r$，$c=p_1'p_2'\cdots p_s'$，$a=q_1q_2\cdots q_t$

其中 p_i, p_j', q_k　　$a|bc \Rightarrow \exists\, d$；$bc=ad$

$$p_1p_2\cdots p_r p_1'\cdots p_s' = q_1q_2\cdots q_t d$$

$(a,b)=1 \Rightarrow q_k$ 不能与 $p_i\ (i=1,\cdots,r)$ 相伴，只能与 $p_1',\cdots,p_s'$

相伴 $\Rightarrow a|c$.

例 $\mathbb{Z}[i]$ 中　$\forall\, a+bi\in\mathbb{Z}[i]$，若 $a^2+b^2=p$ 是素数，

则 $a+bi$ 是 $\mathbb{Z}[i]$ 的不可约元.

证明：设 $a+bi=(x+yi)(x'+y'i)$　两边取共轭

$$a^2+b^2=(x^2+y^2)(x'^2+y'^2)=p$$

$\Rightarrow x^2+y^2=\pm1$ 或 $x'^2+y'^2=\pm1 \Rightarrow x+yi$ 或 $x'+y'i$ 是单位.

反之，不成立. $7i$ 是不可约元　但 $7^2=49$

最大公因子的性质：R 是整区，任意两个元素有最大公因子，

(1) $((a,b),c)\sim(a,(b,c))$

(2) $c(a,b)\sim(ca,cb)$

证明：$c(a,b)|ca$，$c(a,b)|cb \Rightarrow c(a,b)|(ca,cb)$

令 $(ca,cb)=c(a,b)x$　　$cx|ca$，$cx|cb \Rightarrow x|a$，$x|b$

$(a,b)x|a$，$(a,b)x|b \Rightarrow (a,b)x|(a,b) \Rightarrow x$ 是单位

(3) $(a,b)\sim 1$, $(a,c)\sim 1$, 则 $(a,bc)\sim 1$

证明: $(1,c)\sim 1 \xRightarrow{\text{由(2)}} (a,ac)\sim a$ 同理 $(ac,bc)\sim c$

$(a,bc)\sim((a,ac),bc)\sim(a,(ac,bc))\sim(a,c)\sim 1$

定理 R 整区, R 是 UFD $\Longleftrightarrow$ (1) $\forall a\neq 0\in R$, a 非单位, a 可写成有限个不可约元乘积.

(2) $\forall x,y\in R$, 存在最大公因子.

证明: 只需证不可约元是素元.

设 $P\in R$ 不可约, 且 $P\nmid a$, $P\nmid b$, 设 $(P,a)=d$, $d\mid P$

$d\mid a$, P 不可约 $\Rightarrow d\sim 1$, 同理 $(P,b)\sim 1$, 由以上性质(3)

$(P,ab)\sim 1$, 即 $P\nmid ab$.

作业: Page 103 ~~2~~, 3, 4, 5, 6, 7, 8, 9