

§2 整除理论及其代数语言描述.

§2.1. 整除

\mathbb{Z} 上不能作除法, 即给定 $a, b (\neq 0) \in \mathbb{Z}$, 不一定存在 c 使得 $a = bc$. 于是引出如下定义:

定义1: $a, b \in \mathbb{Z}, b \neq 0$

若 $\exists c \in \mathbb{Z}$ s.t. $a = bc$, 则称

- b 整除 a , 记为 $b|a$ (否则称 b 不整除 a , 记 $b \nmid a$)
- b 为 a 的因子/约数 (factor/divisor)
- a 为 b 的倍数 (multiple)

整除有如下基本性质

性质2: 若 $a, b, c \in \mathbb{Z}$, 则

$$1) \quad b|a \xLeftrightarrow{c \neq 0} bc|ac$$

$$2) \quad a|b \text{ 且 } b|c \Rightarrow a|c \quad \text{传递性}$$

$$3) \quad a|b \text{ 且 } a|c \Rightarrow a|bx+cy \quad (\forall x, y \in \mathbb{Z}).$$

$$4) \quad b|a \neq 0 \Rightarrow |b| \leq |a|$$

$$\text{特别地 } b|a \text{ 且 } a|b \Rightarrow a = \pm b$$

$$\text{Pf: } 1). \quad b|a \Leftrightarrow \exists k \in \mathbb{Z} \text{ s.t. } a = bk \xLeftrightarrow{c \neq 0} \exists k \in \mathbb{Z} \text{ s.t. } ac = bck \Leftrightarrow bc|ac.$$

$$2). \quad \left. \begin{array}{l} a|b \Rightarrow b = ak_1 \\ b|c \Rightarrow c = bk_2 \end{array} \right\} \Rightarrow c = (ak_1)k_2 = a(k_1k_2) \Rightarrow a|c.$$

$$3). \quad \left. \begin{array}{l} a|b \Rightarrow b = ak_1 \\ a|c \Rightarrow c = ak_2 \end{array} \right\} \Rightarrow bx+cy = ak_1x+ak_2y = a(k_1x+k_2y) \Rightarrow a|bx+cy.$$

$$4). \quad b|a \ (a \neq 0) \Rightarrow a = bk \ (k \in \mathbb{Z} \setminus \{0\}) \Rightarrow |a| = |b| \cdot |k| \geq |b|$$

定理3 (带余除法) $\forall a, b \in \mathbb{Z}, b \neq 0. \exists ! q, r \in \mathbb{Z}$ s.t.

$$a = bq + r \quad \text{其中 } 0 \leq r < |b|$$

\downarrow 商 quotient \quad \downarrow 余数 remainder

注: 1) $a \div b = q \cdots r$, 即 a 除以 b 等于 q 余 r .

2) 小学时, 只要求知道结论, 会计算就行. 现在要求会证明.

证: 存在性: $I := \{a - bk \mid k \in \mathbb{Z}\} \Rightarrow I \cap \mathbb{N}_+ \neq \emptyset \Rightarrow I \cap \mathbb{N}_+$ 有最小 r .

即 r 为形如 $a - bk$ 的最小非负整数.

$\Rightarrow 0 \leq r < |b|$ (否则, $r' := r - |b| \in I \cap \mathbb{N}_+$ 且 $r' < r$ \downarrow)

$\Rightarrow r = a - bq$ (即 $a = bq + r$) 满足要求.

唯一性: $a = bq_1 + r_1 = bq_2 + r_2 \Rightarrow |r_1 - r_2| = |b(q_2 - q_1)|$

$\Rightarrow q_2 = q_1$ (否则, $|b| \mid r_1 - r_2$ 且 $r_1 - r_2 \neq 0$,
因此, $|b| \leq |r_1 - r_2|$
 $0 \leq r_1, r_2 < |b| \Rightarrow |r_1 - r_2| < |b|$ \downarrow)
 $\Rightarrow r_1 = r_2$ \square

注: 任意给定正整数 n , 根据除以 n 后得到的余数, 我们可以将 \mathbb{Z} 分解为 n 个子集的无交并.

$$\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\} \sqcup \{nk+1 \mid k \in \mathbb{Z}\} \sqcup \cdots \sqcup \{nk+(n-1) \mid k \in \mathbb{Z}\}$$

余数 0 1 ... $n-1$.

e.g. $n=2$. $\mathbb{Z} = \{\text{偶数}\} \sqcup \{\text{奇数}\}$

$n=3$, $\mathbb{Z} = \{3k \mid k \in \mathbb{Z}\} \sqcup \{3k+1 \mid k \in \mathbb{Z}\} \sqcup \{3k+2 \mid k \in \mathbb{Z}\}$.

§ 2.2. 最大公因子

定义4: $a, b \in \mathbb{Z}$ 不全为0. 称 $d \in \mathbb{Z}$ 为 a 与 b 的 **最大公因子** (greatest common divisor), 若

$$1) \quad d|a \text{ 且 } d|b$$

$$2) \quad \forall d' \text{ 满足 } d'|a \text{ 且 } d'|b \Rightarrow d' \leq d.$$

$$\text{即 } d = \max\{d' \in \mathbb{Z} \mid d'|a \text{ 且 } d'|b\}$$

注: 1) 公因子集有限 \Rightarrow 最大公因子 $\exists!$ 记为 $\gcd(a, b)$. 或 (a, b)

2) 称 a 与 b **互素** (coprime), 若 $\gcd(a, b) = 1$.

最大公因子的基本性质:

性质5: 设 $a, b \in \mathbb{Z}$. 则

$$1) \quad \gcd(\pm a, \pm b) = \gcd(a, b)$$

$$2) \quad \gcd(a, b) = \gcd(b, a)$$

$$3) \quad a \neq 0 \Rightarrow \gcd(a, a) = \gcd(a, 0) = |a|$$

$$4) \quad \gcd(a, b) = \gcd(a+by, b) = \gcd(a, b+ax) \quad (\forall x, y \in \mathbb{Z})$$

$$\text{pf: } 1) \quad d|a \Leftrightarrow d|(-a) \text{ 且 } d|b \Leftrightarrow d|(-b)$$

$$\begin{aligned} \gcd(a, b) &:= \max\{d \in \mathbb{Z} \mid d|a \text{ 且 } d|b\} \\ &= \max\{d \in \mathbb{Z} \mid d|\pm a \text{ 且 } d|\pm b\} =: \gcd(\pm a, \pm b) \end{aligned}$$

$$2) \quad \gcd(a, b) := \max\{d \in \mathbb{Z} \mid d|a \text{ 且 } d|b\} =: \gcd(b, a)$$

$$3) \quad \left. \begin{array}{l} \forall d|a \xrightarrow{a \neq 0} d \leq |a| \\ \text{显然 } |a| | a \end{array} \right\} \Rightarrow \gcd(a, a) = \max\{d \in \mathbb{Z} \mid d|a\} = |a|$$

$$4) \quad d|a, d|b \Rightarrow d|a+by$$

$$d|a+by, d|b \Rightarrow d|(a+by)-by=a$$

$$\text{因此 } \{d \mid d|a, d|b\} = \{d \mid d|a+by, d|b\}.$$

$$\Rightarrow \gcd(a, b) = \gcd(a+by, b)$$

$$\text{同理 } \gcd(a, b) = \gcd(a, b+ax)$$

定理6 (贝祖等式) 设 $a, b \in \mathbb{Z}$ 不全为0. 则

1) 存在 $x, y \in \mathbb{Z}$ 使得 $\gcd(a, b) = ax + by$.

2) 若 $d > 0$ 为 a, b 的公因子且存在 $x, y \in \mathbb{Z}$ 使得 $d = ax + by$, 则 $d = \gcd(a, b)$.

Pf: (1) $I := \{ax + by > 0 \mid x, y \in \mathbb{Z}\} \neq \emptyset$ (e.g. $|a| \in I$)

从而 I 中有最小元, 记作 d . 设 $d = ax + by$

断言: $d = \gcd(a, b)$.

显然 $\gcd(a, b) \mid d$, 只需证明: $d \mid a$ 且 $d \mid b$.

• $d \mid a$:

$$\text{带余除法} \Rightarrow a = qd + r \quad (0 \leq r < d)$$

$$\Rightarrow a = q(ax + by) + r$$

$$\Rightarrow r = (1 - qx)a + (-qy)b$$

$$\Rightarrow r = 0 \text{ 即 } d \mid a. \quad (\text{否则, } r \in I \text{ 与 } d \text{ 的取法矛盾})$$

• 同理 $d \mid b$.

$$(2). \text{ 若 } d' \mid a \text{ 且 } d' \mid b, \text{ 则 } d' \mid d = ax + by \Rightarrow d' \leq |d| = d. \left. \begin{array}{l} d' \mid a \text{ 且 } d' \mid b \end{array} \right\} \Rightarrow d = \gcd(a, b)$$

推论7: a 与 b 互素 $\Leftrightarrow \exists x, y \in \mathbb{Z}$ s.t. $ax + by = 1$.

\Rightarrow : \checkmark

-2-4- \Leftarrow : 记 $d = \gcd(a, b)$. 则 $d \mid ax + by \Rightarrow d \mid 1 \Rightarrow d = 1 \Rightarrow \checkmark$.

最大公因子的基本性质:

1) $d|a$ & $d|b \Rightarrow d|\gcd(a,b)$

2) $m>0 \Rightarrow m\gcd(a,b) = \gcd(ma, mb)$

3) $\gcd(a,b)=d \Rightarrow \gcd\left(\frac{a}{d}, \frac{b}{d}\right)=1$

4) $\gcd(a,m)=1 = \gcd(b,m) \Rightarrow \gcd(ab,m)=1$

5) $c|ab$ & $\gcd(c,b)=1 \Rightarrow c|a$

Pf: 1). 设 $\gcd(a,b)=ax+by$, 则 $d|ax+by \Rightarrow d|\gcd(a,b)$.

2). $m \cdot \gcd(a,b) | ma$ & $m \cdot \gcd(a,b) | mb$
 $\left. \begin{array}{l} \gcd(a,b)=ax+by \Rightarrow m \cdot \gcd(a,b) = ma \cdot x + mb \cdot y \end{array} \right\} \Rightarrow m \cdot \gcd(a,b) = \gcd(ma, mb)$

3). $d \cdot \gcd\left(\frac{a}{d}, \frac{b}{d}\right) \stackrel{2)}{=} \gcd(a,b) = d \Rightarrow \gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

4). $\left. \begin{array}{l} (a,m)=1 \Rightarrow ax_1+my_1=1 \\ (b,m)=1 \Rightarrow bx_2+my_2=1 \end{array} \right\} \Rightarrow (ax_1+my_1)(bx_2+my_2)=1$
 $\Rightarrow ab \cdot x_1x_2 + m(y_1bx_2 + ax_1y_2 + my_1y_2) = 1$
 $\Rightarrow (ab, m)=1$

5). $(c,b)=1 \Rightarrow \exists x,y \text{ s.t. } cx+by=1 \Rightarrow by=1-cx$.

$c|ab \Rightarrow c|aby \Rightarrow c|a(1-cx) \Rightarrow c|a$

注: 可归纳定义 $\gcd(a_1, \dots, a_n) := \gcd(\gcd(a_1, \dots, a_{n-1}), a_n)$

推论 9: $d|a_i \ (\forall i=1, \dots, n) \Leftrightarrow d|\gcd(a_1, \dots, a_n)$.

§2.3 欧氏算法

输入: $a, b \in \mathbb{Z}$ 不全为 0

输出: $\gcd(a, b)$ 及 x, y s.t. $\gcd(a, b) = ax + by$

反复应用带余除法

$$r_{-1} = a \quad r_0 = b$$

$$r_{-1} = q_0 r_0 + r_1 \quad 0 \leq r_1 < |r_0|$$

$$r_0 = q_1 r_1 + r_2 \quad 0 \leq r_2 < r_1$$

\vdots

$$r_{n-2} = q_{n-1} r_{n-1} + r_n \quad 0 \leq r_n < r_{n-1}$$

$$r_{n-1} = q_n r_n$$

$$\Rightarrow \begin{cases} \bullet r_1, r_0, \dots, r_n \text{ 均为 } a, b \text{ 的整线性组合} \\ \bullet r_n \mid r_{n-1}, r_{n-2}, \dots, r_0, r_{-1} \end{cases}$$

$$\Rightarrow r_n = \gcd(a, b).$$

Step	quotient	remainder	x	y
$r_i = ax_i + by_i$		r_{-1}	$x_{-1} = 1$	$y_{-1} = 0$
	q_0	r_0	$x_0 = 0$	$y_0 = 1$
	q_1	r_1	$x_1 = x_{-1} - q_0 x_0$	$y_1 = y_{-1} - q_0 y_0$
	\vdots	\vdots	\vdots	\vdots
	q_{i+1}	r_{i+1}	$x_{i+1} = x_{i-1} - q_i x_i$	$y_{i+1} = y_{i-1} - q_i y_i$
	\vdots	\vdots	\vdots	\vdots
	q_n	r_n	$x_n = x_{n-2} - q_{n-1} x_{n-1}$	$y_n = y_{n-2} - q_{n-1} y_{n-1}$
		0		

$$\Rightarrow \gcd(r_{-1}, r_0) = r_n = x_n \cdot a + y_n \cdot b$$

e.g.

	1517	1	0
3	481	0	1
6	74	1	-3
2	37	-6	19
	0		

-2-6-

$$37 = \gcd(1517, 481) = -6 \times 1517 + 19 \times 481$$

§2.4 最小公倍数

定义 1: $a, b \in \mathbb{Z} \setminus \{0\}$. 称 $m \in \mathbb{N}$ 为 a, b 的 **最小公倍数** (least common multiple)

1) $m > 0, a|m, b|m$ [公倍]

2) 设 m' 为 a, b 公倍数 $\Rightarrow m \leq |m'|$ [最小]

记 $m = [a, b]$ 或 $\text{lcm}(a, b)$.

注: 1) $m = \min \{ m' > 0 \mid a|m' \text{ 且 } b|m' \}$

2) 存在且唯一.

最小公倍数的基本性质:

性质 II: $a, b \in \mathbb{Z} \setminus \{0\}$. 则

1) $a|m, b|m \Leftrightarrow \text{lcm}(a, b) | m$

2) $\text{lcm}(ma, mb) = |m| \cdot \text{lcm}(a, b)$

3) $\text{lcm}(a, b) \cdot \gcd(a, b) = |ab|$

特别地 $\gcd(a, b) = 1 \Rightarrow \text{lcm}(a, b) = |ab|$

Pf: 1). $a|m \text{ 且 } b|m \xRightarrow{m \neq 0} \text{lcm}(a, b) \leq |m|$

设 $|m| = q \cdot \text{lcm}(a, b) + r, (0 \leq r < \text{lcm}(a, b))$

$\Rightarrow a|r \text{ 且 } b|r \Rightarrow r=0$ (否则, $\text{lcm}(a, b) \leq r < \text{lcm}(a, b)$)

$\Rightarrow \text{lcm}(a, b) | m$

2). $ma | m \cdot \text{lcm}(a, b) \text{ 且 } mb | m \cdot \text{lcm}(a, b) \Rightarrow \text{lcm}(ma, mb) | m \cdot \text{lcm}(a, b)$

$ma | \text{lcm}(ma, mb) \Rightarrow a | \frac{\text{lcm}(ma, mb)}{m}$

$mb | \text{lcm}(ma, mb) \Rightarrow b | \frac{\text{lcm}(ma, mb)}{m}$

$\Rightarrow \text{lcm}(a, b) | \frac{\text{lcm}(ma, mb)}{m}$

$\Rightarrow m \cdot \text{lcm}(a, b) | \text{lcm}(ma, mb)$

$$3). d := \gcd(a, b)$$

$$a \mid a \cdot \frac{b}{d} \text{ \& } b \mid \frac{a}{d} \cdot b \Rightarrow \text{lcm}(a, b) \mid \frac{ab}{d} \Rightarrow d \cdot \text{lcm}(a, b) \mid ab.$$

$$\text{又, 设 } d = \gcd(a, b) = ax + by, \mathbb{Z}$$

$$\left. \begin{array}{l} ab \mid a \cdot \text{lcm}(a, b) \\ ab \mid b \cdot \text{lcm}(a, b) \end{array} \right\} \Rightarrow ab \mid (ax + by) \text{lcm}(a, b) = d \cdot \text{lcm}(a, b)$$

$$\Rightarrow d \cdot \text{lcm}(a, b) = |ab|$$

□

$$\text{归纳定义: } \text{lcm}(a_1, \dots, a_n) := \text{lcm}(\text{lcm}(a_1, \dots, a_{n-1}), a_n)$$

$$\text{性质 12: } a_i \mid b \ (\forall i=1, \dots, n) \Leftrightarrow \text{lcm}(a_1, \dots, a_n) \mid b.$$

§2.5 理想

考虑 \mathbb{Z} 的子集 $I = \{0, \pm n, \pm 2n, \pm 3n, \dots\}$ 由 n 的全体倍数组成.

显然 $(I, +)$ 为 $(\mathbb{Z}, +)$ 的子群, 且 I 对其中的元素取倍数封闭.

定义B: 设 R 为环, $\phi \neq I \subseteq R$. 若 I 满足

$$1) \forall a, b \in I \quad a - b \in I \quad (\text{减法封闭})$$

$$2) \forall a \in I, \forall r \in R \quad ra, ar \in I \quad (\text{数乘封闭})$$

则称 I 为 R 的一个理想, 记为 $I \triangleleft R$. 取倍数

注: $1) \Leftrightarrow (I, +)$ 形成 $(R, +)$ 的子群

性质14: 设 I_1, I_2 为环 R 的理想, 则

$$I_1 + I_2 := \{r_1 + r_2 \mid r_1 \in I_1, r_2 \in I_2\}$$

$$I_1 \cap I_2 := \{r \in R \mid r \in I_1 \text{ 且 } r \in I_2\}$$

$$I_1 \cdot I_2 := \left\{ \sum_{i=1}^n a_i b_i \mid a_i \in I_1, b_i \in I_2 \right\}$$

均为 R 的理想.

例15: 设 R 为交换环, $a, a_1, \dots, a_n \in R$, 则

1) $(a) := aR := \{ar \mid r \in R\}$ 为包含 a 的最小理想, 称为由 a 生成的主理想;

2) $(a_1, \dots, a_n) = \{a_1 r_1 + \dots + a_n r_n \mid r_1, \dots, r_n \in R\}$ 为包含 a_1, \dots, a_n 的最小理想, 称为由 a_1, \dots, a_n 生成的理想.

Pf: 只需证明 2).

• (a_1, \dots, a_n) 为理想.

$$\forall x = a_1 r_1 + \dots + a_n r_n, y = a_1 r'_1 + \dots + a_n r'_n \in (a_1, \dots, a_n) \quad \forall r \in R. \text{ 则}$$

$$\bullet x - y = a_1(r_1 - r'_1) + \dots + a_n(r_n - r'_n) \in (a_1, \dots, a_n)$$

$$\bullet rx = r(a_1 r_1 + \dots + a_n r_n) = a_1(r r_1) + \dots + a_n(r r_n) \in (a_1, \dots, a_n)$$

· 最小性:

若 I 为理想, 且 $a_1, \dots, a_n \in I$, 则 $\forall r_1, \dots, r_n \in R$ 有

$$a_1 r_1 + a_2 r_2 + \dots + a_n r_n \in I$$

因此 $(a_1, \dots, a_n) \subseteq I$ 从而 (a_1, \dots, a_n) 为最小的.

注: 设 R 为交换环. $a, a_1, \dots, a_n \in R$.

1) $aR = 0 \Leftrightarrow a = 0$

2) $aR = R \Leftrightarrow a$ 为 R 中乘法可逆元.

3) $(a_1, \dots, a_n) = (a_1) + (a_2) + \dots + (a_n)$

↙ d 的全体倍数组成的集合.

定理 16. 1) $\forall d \in \mathbb{N} = \mathbb{Z}_{\geq 0}$. 则 $d\mathbb{Z}$ 为 \mathbb{Z} 的理想.

2) 在 \mathbb{Z} 的理想 I , 存在 $d \in \mathbb{N}$ 使得 $I = d\mathbb{Z}$.

$$\begin{array}{ccc} \mathbb{N} & \xrightarrow{1:1} & \{I \mid I \triangleleft \mathbb{Z}\} \\ d & \longmapsto & d\mathbb{Z} \end{array}$$

pf: 1) 显然

2) 若 $I = 0$, 则取 $d = 0$

若 $I \neq 0$. 则 $I_+ := I \cap \mathbb{Z}_{>0} \neq \emptyset$ ($0 \neq a \in I \Rightarrow |a| \in I_+$)

取 $d = \min I_+$ 断言: $I = d\mathbb{Z}$

· $d\mathbb{Z} \subseteq I$ 显然

· $\forall n \in I \Rightarrow n = dq + r$ ($0 \leq r < d$) $\Rightarrow r = n - dq \in I$
 $\Rightarrow r = 0$ (否则与 d 的取法矛盾) $\Rightarrow n = dq \in d\mathbb{Z}$

注: 1) $d\mathbb{Z} (\neq 0)$ 有两个生成元 $\pm d$, 其中一正一负. $|d|$ 为其唯一的正生成元.

2)* 整环 + 带余除法 \leadsto ED 欧几里得整环

整环 + 理想都为主理想 \leadsto PID 主理想整环

-2-10-

ED \Rightarrow PID.

§2.6. 用理想语言来描述整除理论.

$$\mathbb{Z} \xrightarrow{n \mapsto n\mathbb{Z}} \{I \mid I \triangleleft \mathbb{Z}\} \xrightarrow[n\mathbb{Z} \mapsto |n|]{\varphi} \mathbb{N}$$

整除理论 理想论

- 引理: 1) $a \mid b \iff b \in a\mathbb{Z} \iff b\mathbb{Z} \subseteq a\mathbb{Z}$
 2) $a = \pm b \iff a\mathbb{Z} = b\mathbb{Z}$
 3) a 与 b 互素 $\iff (a, b) = \mathbb{Z}$.

推论 2': 若 $a, b, c \in \mathbb{Z}$, 则

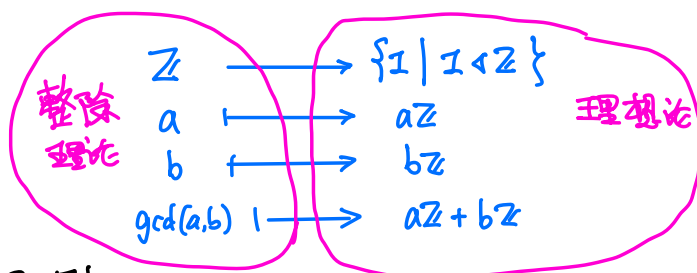
- 1) $a\mathbb{Z} \subseteq b\mathbb{Z} \iff ac\mathbb{Z} \subseteq bc\mathbb{Z}$
- 2) $c\mathbb{Z} \subseteq b\mathbb{Z} \text{ 且 } b\mathbb{Z} \subseteq a\mathbb{Z} \Rightarrow c\mathbb{Z} \subseteq a\mathbb{Z}$
- 3) $b\mathbb{Z} \subseteq a\mathbb{Z} \text{ 且 } c\mathbb{Z} \subseteq a\mathbb{Z} \Rightarrow b\mathbb{Z} + c\mathbb{Z} \subseteq a\mathbb{Z}$
- 4)* $a\mathbb{Z} \subseteq b\mathbb{Z} \text{ 且 } b\mathbb{Z} \mid a\mathbb{Z} \Rightarrow a\mathbb{Z} = b\mathbb{Z}$.

用理想语言无法描述大小关系

定理 6': 设 $a, b \in \mathbb{Z}$ 不全为零. 记 $d = \gcd(a, b)$, 则 $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$.

即 $\gcd(a, b)$ 可解释为理想 $a\mathbb{Z} + b\mathbb{Z}$ 的正生成元.

从理想角度看, 取最大公因子, 相当于对理想作加法.



推论 5': 设 $a, b \in \mathbb{Z}$ 则

- 1) $(\pm a, \pm b) = (a, b) \triangleleft \mathbb{Z}$ (作为理想相等)
- 2) $(a, b) = (b, a) \triangleleft \mathbb{Z}$
- 3) $(a, a) = (a, 0) = (|a|) \triangleleft \mathbb{Z}$
- 4) $(a+by, b) = (a, b) = (a, b+ax) \triangleleft \mathbb{Z}$.

推论 7': $(a, b) = \mathbb{Z} \iff 1 \in (a, b)$.

性质 8':

- 1) $(a) \subseteq (d), (b) \subseteq (d) \Rightarrow (a, b) \subseteq (d)$
- 2) $(m) \cdot (a, b) = (ma, mb)$
- 3) $(a, b) = (d) \Rightarrow (\frac{a}{d}, \frac{b}{d}) = \mathbb{Z}$
- 4) $(a, m) = \mathbb{Z} = (b, m) \Rightarrow (ab, m) = \mathbb{Z}$
- 5) $(ab) \subseteq (c), (c, b) = \mathbb{Z} \Rightarrow (a) \subseteq (c)$

4) $\mathbb{Z} = \mathbb{Z} \cdot \mathbb{Z} = (a, m)(b, m)$
 $\subseteq (ab, m)$
 $\Rightarrow (ab, m) = \mathbb{Z}$

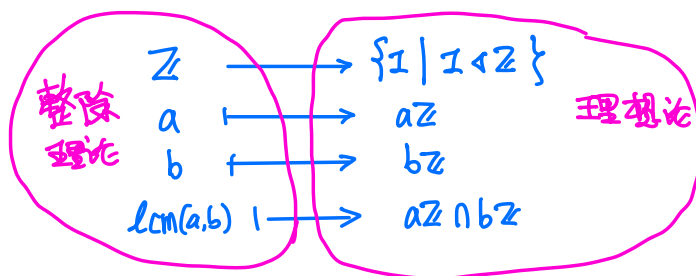
5) $(a) = (a) \cdot \mathbb{Z}$
 $= (a) \cdot (c, b)$
 $= (ac, ab) \subseteq (c)$

推广: $\gcd(a_1, a_2, \dots, a_n)$ 为理想 (a_1, a_2, \dots, a_n) 的非负生成元.

定理: 设 $a, b \in \mathbb{Z} \setminus \{0\}$. 记 $m = \text{lcm}(a, b)$, 则 $m\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$.

即 $\text{lcm}(a, b)$ 可解释为理想 $a\mathbb{Z} \cap b\mathbb{Z}$ 的正生成元.

从理想角度看, 取最小公倍数相当于对理想作交



推广 11': $a, b \in \mathbb{Z} \setminus \{0\}$. 则

- 1) $(m) \subseteq (a), (m) \subseteq (b)$, 则 $(m) \subseteq (a) \cap (b)$
- 2) $(ma) \cap (mb) = (m) \cdot ((a) \cap (b))$
- 3) $((a) \cap (b)) \cdot (a, b) = (a) \cdot (b)$

特别地若 $(a, b) = \mathbb{Z}$, 则 $(a) \cap (b) = (a) \cdot (b)$.

推广: $\text{lcm}(a_1, a_2, \dots, a_n)$ 为理想 $(a_1) \cap (a_2) \cap \dots \cap (a_n)$ 的非负生成元.

2.7 算术基本定理

定义: $p \in \mathbb{Z}_{\geq 2}$. 若 p 的正因子仅有 1 和 p . 则称 p 为 **素数/质数** (prime number)
否则称之为 **合数** (composite number)

性质: 1) $\gcd(p, a) = \begin{cases} 1 & p \nmid a \\ p & p \mid a \end{cases}$

2) $n \in \mathbb{Z}_{\geq 2} \Rightarrow n$ 有素因子. pf: $\min \{d \geq 2 \mid d \mid n\}$ 为素数

欧几里得引理: $p = \text{素数}$. $p \mid ab \Rightarrow p \mid a$ 或 $p \mid b$.

pf: $d := \gcd(p, a)$,
1° $d = 1$. $p \mid ab \Rightarrow p \mid b$ ✓
2° $d = p \Rightarrow p \mid a$ ✓

推论: $p = \text{素数}$. $p \mid a_1 a_2 \cdots a_n$. 则 $\exists i$ s.t. $p \mid a_i$.

欧几里得定理: 素数有无穷多个.

pf: 否则, 记 $\{p_1, \dots, p_n\}$ 为全体素数. 则 $N = p_1 \cdots p_n + 1 \geq 2$ 设 p 为 N 的素因子. 则

$$p \mid p_1 \cdots p_n \text{ 且 } p \mid N \Rightarrow p \mid 1 = N - p_1 \cdots p_n \quad \downarrow$$

算术基本定理: $\forall n \in \mathbb{Z}_{\geq 2}$.

- 1) \exists 素数 p_1, \dots, p_r s.t. $n = p_1 p_2 \cdots p_r$
- 2) 不记次序下, 表达唯一.

pf: 1) 存在性 对 n 归纳: $n=2$ ✓ $n = \text{素数}$ ✓

$n = \text{合数}$ ($n = ab, a, b < n$) \Rightarrow ✓ (将 a 与 b 的分解乘在一起)

2) 唯一性 对 n 归纳: $n=2$ ✓ 设 $n = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t$

$$p_1 \mid n \Rightarrow p_1 \mid q_1 \cdots q_t \Rightarrow \exists i \text{ s.t. } p_1 \mid q_i \Rightarrow p_2 \cdots p_s = q_1 \cdots q_{i-1} q_{i+1} \cdots q_t$$

归纳假设

$\Rightarrow s = t$, p_2, \dots, p_s 为 $q_1, \dots, q_{i-1}, q_{i+1}, \dots, q_t$ 的一个排列.

$\Rightarrow p_1, p_2, \dots, p_s$ 为 q_1, q_2, \dots, q_t 的一个排列. \Rightarrow ✓

变形: $\forall n \in \mathbb{Z} \setminus \{0\}$. $\exists!$ $v_p(n) \in \mathbb{N}$ (对所有的素数 p) s.t.
 $n = \text{sgn}(n) \cdot \prod_{p: \text{素数}} p^{v_p(n)}$ ← 因式分解

- 其中 1) $\text{sgn}(n) = \frac{n}{|n|} = \begin{cases} 1 & n > 0 \\ -1 & n < 0 \end{cases}$
- 2) $p \gg 0 \Rightarrow v_p(n) = 0$ ($\forall p \exists N$ s.t. $\forall p > N$ $v_p(n) = 0$)
- 3) $p | n \Leftrightarrow v_p(n) > 0$
- 4) 表达唯一.

变形: $n = \text{sgn}(n) p_1^{v_{p_1}(n)} \dots p_s^{v_{p_s}(n)}$, $p_i \neq p_j$, $v_{p_i}(n) > 0$.

推论: $\forall a \in \mathbb{Q} \setminus \{0\}$. $a = \frac{m}{n} = \text{sgn}(a) \prod_{p: \text{素数}} p^{v_p(a)}$

- 1) $\text{sgn}(a) = \frac{a}{|a|}$
- 2) $v_p(a) \in \mathbb{Z}$ & $v_p(a) = 0$ for $p \gg 0$.
- 3). $|a| = \frac{m}{n}$ & $\gcd(m, n) = 1$ \Rightarrow

$$m = \prod_{p: v_p(a) > 0} p^{v_p(a)} \quad n = \prod_{p: v_p(a) < 0} p^{-v_p(a)}$$

4). 若 $a = \frac{\alpha}{\beta}$ 则 $\forall p$ 素数 $v_p(a) = v_p(\alpha) - v_p(\beta)$

应用: 1) $n \in \mathbb{Z}_{>0}$. $d = \prod_p p^{v_p(d)} \in \mathbb{Z}_{>0}$

$$d | n \Leftrightarrow v_p(d) \leq v_p(n) \quad \forall p.$$

$$\begin{aligned} 2) \quad \gcd(a, b) &= \prod_p p^{\min\{v_p(a), v_p(b)\}} \\ \text{lcm}(a, b) &= \prod_p p^{\max\{v_p(a), v_p(b)\}} \end{aligned}$$

注: 若已知因式分解, 则很容易求得 \gcd & lcm
但实际应用中一般因式分解非常困难

e.g. $1517 = 37 \times 41, 481 = 13 \times 37$

$$\Rightarrow \gcd(1517, 481) = 37, \text{lcm}(1517, 481) = 13 \times 37 \times 41$$

性质: $v_p: (\mathbb{Q}^\times, \cdot) \rightarrow (\mathbb{Z}, +)$ 为群同态.

$$a \mapsto v_p(a)$$

§2.8. 唯一分解整环.

回顾整环定义:

定义: 设 $(R, +, \cdot)$ 为交换环. 若对任意 $a, b \in R \setminus \{0\}$ 有 $ab \neq 0$, 则称 R 为 **整环**.

性质: **整环 = 交换环 + 消去律**

问题: 一般的整环上有没有算术基本定理? 其上的“素数”怎么定义?

$(R, +, \cdot) = \text{整环}, \forall a, b, p \in R$

• 整除/因子: $a|b \stackrel{\Delta}{\Leftrightarrow} \exists c \in R \text{ s.t. } b = ac \Leftrightarrow b \in (a) \triangleleft R \Leftrightarrow (b) \subseteq (a) \triangleleft R$

• 不可约元: p 不可约 $\stackrel{\Delta}{\Leftrightarrow} \begin{cases} (1) p \notin R^\times \\ (2) p = ab \Rightarrow a \in R^\times \text{ 或 } b \in R^\times \end{cases}$

定义: 称整环 R 为 **唯一分解整环 (UFD)**, 若它满足, 对任意 $a \in R$ 非零非单位

1) (存在性) \exists 不可约元 p_1, \dots, p_r s.t. $a = p_1 p_2 \dots p_r$

2) (唯一性) 若 $a = p_1 p_2 \dots p_s = q_1 q_2 \dots q_t$ (p_i, q_j 不可约), 则

$s = t$, 且适当交换次序后有 $q_i = u_i p_i$ (其中 $u_i \in R^\times$)

定义: 称整环 R 为欧几里得环 (ED). 若存在映射 $\delta: R \setminus \{0\} \rightarrow \mathbb{Z}_{>0}$

满足: $\forall a, b \in R, b \neq 0, \exists q, r \in R$ s.t.

$$a = qb + r$$

其中 $r=0$ 或 $\delta(r) < \delta(b)$.

定理: $ED \Rightarrow PID \Rightarrow UFD \Rightarrow \text{Domain}$

↓
有带余除法

↓
所有理想均为主理想

↘
有唯一分解性定理.

注: 1). 整数的整除理论 $\simeq \mathbb{Z}$ 为 ED, PID, & UFD

2). 问环 R 上是否有整除理论 \simeq 问 R 是否为 ED, PID or UFD.

3). e.g. $\mathbb{Z}, \mathbb{Z}[i], \mathbb{Z}[\sqrt{2}], \mathbb{Z}[\sqrt{3}], k[x] = ED$

e.g. $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right], \mathbb{Z}\left[\frac{1+\sqrt{63}}{2}\right], \mathbb{Z}\left[\frac{1+\sqrt{67}}{2}\right], \mathbb{Z}\left[\frac{1+\sqrt{163}}{2}\right] = PID (\neq ED)$

e.g. $\mathbb{Z}[x], k[x, y] = UFD (\neq PID)$

e.g. $\mathbb{Z}[\sqrt{-5}] = \text{Domain} (\neq UFD)$