第2章　整除関係

2.1　整除

整数全体の集合 $\boldsymbol{Z}$ では，足し算と掛け算が定義されていて通常の演算規則，すなわち，結合法則，交換法則，分配法則が成り立っている．

$$\begin{aligned}&\text{結合法則}\quad (a+b)+c=a+(b+c),\quad (ab)c=a(bc),\\ &\text{交換法則}\quad a+b=b+a,\quad ab=ba,\\ &\text{分配法則}\quad a(b+c)=ab+ac.\end{aligned}$$

さらに，$\boldsymbol{Z}$ は 0 と負の数を含むので，引き算もいつでもできる．このように，加減乗除のうち除（割り算）を除く 3 つの演算が自由にできて通常の演算規則が成り立つ集合は，一般に**可換環**とよばれ,「代数 I」で詳しく学ぶ．除法が必ずしもできない可換環においては,「割り切れる」かどうかが最初の問題として浮上する．

定義 2.1　2 つの整数 a,b に対して $a=bc$ をみたす $c\in\boldsymbol{Z}$ がとれるとき，a は b の**倍数**である，または，b は a の**約数**であるといい，

$$b\mid a$$

で表す．$b\mid a$ でないときは $b\nmid a$ と書く．

たとえば $2\mid 6,\ 4\nmid 10,\ 17\mid 51$ である．次の命題は今後たびたび使われる．

命題 2.2　$a,b,c\in\boldsymbol{Z}$ について次が成り立つ．

(1) $c\mid a$ かつ $c\mid b$ ならば $c\mid(a+b)$.

(2) $c\mid a$ ならば，任意の $x\in\boldsymbol{Z}$ に対して $c\mid ax$.

(3) $c\mid a$ かつ $c\mid b$ ならば，任意の $x,y\in\boldsymbol{Z}$ に対して $c\mid(ax+by)$.

証明は演習とする．

1 はすべての $a\in\boldsymbol{Z}$ の約数であり，0 はすべての $a\in\boldsymbol{Z}$ の倍数である．

$$\text{任意の } a\in\boldsymbol{Z} \text{ に対して, } 1\mid a \text{ かつ } a\mid 0.$$

-1 もすべての $a \in \boldsymbol{Z}$ の約数である．一方，1 の約数は 1 または -1 だけであり，0 の倍数は 0 だけである．

$$a \mid 1 \text{ ならば } a = \pm 1, \qquad 0 \mid a \text{ ならば } a = 0.$$

以上は，0 と 1 に関係する極端な性質である．

定義 2.3 a, b をともに 0 でない整数とする．a, b どちらの約数でもある整数を a, b の**公約数**という．また，a, b どちらの倍数でもある整数を a, b の**公倍数**という．a, b の公約数で最大のものを**最大公約数**といい $\gcd(a, b)$ で表す．a, b の正の公倍数のうち最小のものを**最小公倍数**といい $\operatorname{lcm}(a, b)$ で表す．すなわち，$ab \neq 0$ のとき

$$\gcd(a, b) = \max\left\{ c \in \boldsymbol{N} \,\middle|\, c \mid a,\ c \mid b \right\},$$
$$\operatorname{lcm}(a, b) = \min\left\{ c \in \boldsymbol{N} \,\middle|\, a \mid c,\ b \mid c \right\}.$$

a, b どちらかが 0 のときは，$\gcd(a, 0) = \gcd(0, a) = |a|$，$\operatorname{lcm}(a, 0) = \operatorname{lcm}(0, a) = 0$ と定める．

命題 2.4 整数を成分とする 2 次正方行列 A と，$a, b \in \boldsymbol{Z}$ に対して

$$\begin{pmatrix} c \\ d \end{pmatrix} = A \begin{pmatrix} a \\ b \end{pmatrix}$$

によって $c, d \in \boldsymbol{Z}$ を定める．もし $c = d = 0$ でないならば，次が成り立つ．

(1) $\gcd(a, b) \leq \gcd(c, d)$.

(2) $\det A = \pm 1$ ならば $\gcd(a, b) = \gcd(c, d)$.

証明 $A = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$ とおくと，$c = ax + by$, $d = az + bw$ である．$g = \gcd(a, b)$ ならば $g \mid a$, $g \mid b$ だから，命題 2.2 を使って $g \mid c$, $g \mid d$．したがって g は c, d の公約数となるから $g \leq \gcd(c, d)$ となり (1) が示された．(2) を示すために $\det A = \pm 1$ とすると，A の逆行列 $B = A^{-1}$ も整数を成分とする 2 次正方行列で $\left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right) = B\left(\begin{smallmatrix} c \\ d \end{smallmatrix}\right)$ をみたすから，(1) より $\gcd(c, d) \leq \gcd(a, b)$ となる． □

整数 a の倍数全体の集合を $a\boldsymbol{Z}$ で表す．

命題 2.5 $a, b \in \boldsymbol{Z}$ に対して以下が成り立つ．

(1) $b \mid a \iff a \in b\boldsymbol{Z} \iff a\boldsymbol{Z} \subset b\boldsymbol{Z}$.

(2) $m = \operatorname{lcm}(a, b)$ ならば $m\boldsymbol{Z} = a\boldsymbol{Z} \cap b\boldsymbol{Z}$.

(3) $d = \gcd(a, b)$ ならば $d\boldsymbol{Z} \supset a\boldsymbol{Z} \cup b\boldsymbol{Z}$.

証明は演習とする．性質 (2) は次節の「割り算の定理」を用いて示される．なお，性質 (3) は “イデアル” の概念を用いて精密化されるが，詳しくは「代数 I」でね．

2.2 ユークリッドの互除法

$\boldsymbol{Z}$ で割り算を試みると，割り切れない，つまり割り算の値が整数の範囲に納まらないことがある．しかし，小学校で学んだように「余り」付きの割り算はいつも可能である． すなわち，２つの整数 a, b に対して，商 q と余り r が定まり，関係式 $a = qb + r$ が成り立つ． この事実を次の定理として精密に定式化しておく．

定理 2.6 (割り算の定理) 任意の $a, b \in \boldsymbol{Z}$（ただし $b \neq 0$）に対して，

$$a = qb + r, \quad 0 \leq r < |b|$$

をみたす $q, r \in \boldsymbol{Z}$ の組が一意的に存在する．

証明 はじめに，上のような q, r が存在することを示す． まず $b > 0$ として証明する．集合

$$R = \left\{ a - qb \,\middle|\, q \in \boldsymbol{Z},\, a - qb \geq 0 \right\}$$

を考える． q を十分小さくとれば，$a - qb \geq 0$ となることから，$R \neq \phi$ であることがわかる． そこで R の最小元 r をとる． $r = \min R$. この $r \in R$ を実現する $q \in \boldsymbol{Z}$ をとれば，$a = qb + r$ である． いま，$b \leq r$ とすると，

$$0 \leq r - b = a - qb - b = a - (q+1)b \in R$$

であるが，$r - b < r$ なので，$r = \min R$ に矛盾する． したがって $0 \leq r < b$ が成り立つ．$b < 0$ のときは，a, $-b$ に対して定理は証明されているから，$a = q'(-b) + r'$, $0 \leq r' < -b$ をみたす q', $r' \in \boldsymbol{Z}$ が存在する． そこで $q = -q'$, $r = r'$ とおけばよい．

次に一意性を示すために

$$a = qb + r = q'b + r', \quad 0 \leq r, r' < |b|$$

として，$q = q'$, $r = r'$ を示そう． もし $q \neq q'$ ならば $|q - q'| \geq 1$ であるから，

$$|r - r'| = |q - q'|\,|b| \geq |b|$$

となって $0 \leq r, r' < |b|$ に矛盾する． したがって $q = q'$ であり，これから $r = r'$ も導かれる． □

この証明はもちろん “正しい” 証明であるが，より厳密に見ると一ヶ所不満が残る部分がある（オレだけか？）． それは，R の最小元をとるところである． 本当に最小元はとれるのか？ これにまつわる話を次回の講義で詳述予定，乞うご期待．

２つの整数 a, b の最大公約数を効率よく求める方法が次に述べるユークリッドの互除法である． まず，$\gcd(b, a) = \gcd(a, b)$ であり，$a = 0$ ならば $\gcd(0, b) = |b|$，さらに $a < 0$ ならば $\gcd(a, b) = \gcd(-a, b)$ が成り立つので，はじめから $a > 0, b > 0$ すなわち a, b は自然数として考えればよいことに注意する．

定理 2.7 (ユークリッドの互除法) $a, b \in \boldsymbol{N}$ に対して，$a_0 = a$, $a_1 = b$ とし，数列 $\{a_n\}_{n=0,1,\cdots}$ を $a_n \neq 0$ である限り

$$a_{n-1} = q_n a_n + a_{n+1}, \quad 0 \leq a_{n+1} < a_n$$

によって定めることができる． さらに，ある N に対して $a_{N+1} = 0$ となり，そのとき $a_N = \gcd(a, b)$ である．

証明　まず，数列 $\{a_n\}_{n=0,1,\cdots}$ が定まることは前定理よりわかる． また，

$$0 \leq \cdots < a_{n+1} < a_n < \cdots < a_2 < a_1$$

だから，この操作を（多くとも a_1 回）繰り返せば $a_{N+1} = 0$ となる N が得られることがわかる． 一方，

$$\begin{pmatrix} a_{n-1} \\ a_n \end{pmatrix} = \begin{pmatrix} q_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_n \\ a_{n+1} \end{pmatrix}, \qquad \begin{vmatrix} q_n & 1 \\ 1 & 0 \end{vmatrix} = -1$$

なので，命題 2.4 によって $\gcd(a_{n-1}, a_n) = \gcd(a_n, a_{n+1})$ であり，これを繰り返せば，

$$\gcd(a, b) = \gcd(a_0, a_1) = \gcd(a_1, a_2) = \cdots = \gcd(a_N, a_{N+1}) = \gcd(a_N, 0) = a_N$$

となる． □

例として，12305 と 10379 の最大公約数を求めてみよう。

$$\begin{aligned} 12305 &= 1 \cdot 10379 + 1926, & 10379 &= 5 \cdot 1926 + 749, & 1926 &= 2 \cdot 749 + 428, \\ 749 &= 1 \cdot 428 + 321, & 428 &= 1 \cdot 321 + 107, & 321 &= 3 \cdot 107 + 0 \end{aligned}$$

より $\gcd(12305, 10379) = 107$ を得る．

定理 2.8 $a, b \in \boldsymbol{Z}$ の最大公約数を d とすると，

$$ax + by = d$$

をみたす $x, y \in \boldsymbol{Z}$ が存在する．

証明　$a, b > 0$ のときにのみ確かめれば十分であることはすぐにわかる． このとき，前定理の証明から $\binom{a}{b} = A\binom{d}{0}$, $\det A = \pm 1$ をみたす 2 次正方行列 A がとれる． そこで，A^{-1} の第 1 行を $(x,\ y)$ とすれば，$x, y \in \boldsymbol{Z}$ であり $ax + by = d$ が得られる． □

証明中の A^{-1} は，定理 2.7 の証明に現れる行列 $\begin{pmatrix} q_n & 1 \\ 1 & 0 \end{pmatrix}$ の逆行列 $\begin{pmatrix} 0 & 1 \\ 1 & -q_n \end{pmatrix}$ を用いて

$$A^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & -q_N \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_{N-1} \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix}$$

のようにして計算でき，これから x, y を求めることができる．