代数学特講

– 環, 体 –

平成23年度　後期 月曜2限

中川 仁

目標 初等整数論を題材にして，環, 体の基本事項を解説する．

記号 $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ をそれぞれ自然数全体の集合，整数全体の集合，有理数全体の集合，実数全体の集合，複素数全体の集合とする．

目 次

1 環と体

1.1 環の概念

定義 1.1. 2 つ以上の元からなる集合 R が**環** (**単位元を持つ可換環**) であるとは，任意の $a, b \in R$ に対して，和 $a+b$, 積 $ab \in R$ が定義されていて，次の条件 (1)–(8) を満たすことである:

(1) $(a+b)+c = a+(b+c)$;

(2) $\exists 0 \in R$, $\forall a \in R$, $a+0 = 0+a = a$;

(3) $\forall a \in R$, $\exists(-a) \in R$, $a+(-a) = (-a)+a = 0$;

(4) $a+b = b+a$;

(5) $(ab)c = a(bc)$;

(6) $(a+b)c = ac+bc$;

(7) $ab = ba$;

(8) $\exists e \in R, \forall a \in R, ae = ea = a$.

0 を R の**零元**，e を R の**単位元**という．e は通常 1 とかく．

例 1.2. 整数の全体 $\mathbb{Z}$ は環である．自然数の全体 $\mathbb{N}$ は環ではない．$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ も環である．実数係数の 1 変数 x の多項式全体 $\mathbb{R}[x]$ は環である．もっと一般に，R を任意の環とするとき，1 変数 x の R 係数の多項式全体の集合 $R[x]$ は環である．2 変数 x, y の R 係数の多項式全体の集合 $R[x, y]$ も環である．

定義 1.3. 環 R の元 a について，$b \in R$ で $ba = ab = 1$ を満たすものが存在するとき，a を R の**可逆元**という．R の可逆元全体の集合を $R^\times$ で表す．$a_1, a_2 \in R^\times$ ならば，$a_1 a_2 \in R^\times$ である．

例 1.4. $\mathbb{Z}^\times = \{1, -1\}$ である．$(R[x])^\times = R^\times$ である．

定義 1.5. 環 R において，

$$a, b \in R,\ a \neq 0, b \neq 0 \Longrightarrow ab \neq 0$$

が成り立つとき，R は**整域**であるという．

例 1.6. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ は整域である．

定義 1.7. 環 K が $K^\times = K - \{0\}$ をみたすとき，K は**体**であるという．ここで，$K - \{0\} = \{a \in K \mid a \neq 0\}$ である．体は整域であることは容易にわかる．

例 1.8. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ は体である．$\mathbb{Z}$ は体ではない．

1.2 イデアルと剰余環

定義 1.9. 環 R の部分集合 I が次の条件をみたすとき，R の**イデアル**であるという:

$a, b \in I \Longrightarrow a + b \in I$;

$r \in R, a \in I \Longrightarrow ra \in I$.

命題 1.10. I を $\mathbb{Z}$ のイデアルとすると，$\exists m \in \mathbb{Z},\ m \geq 0,\ I = m\mathbb{Z}$.

[証明] I を $\mathbb{Z}$ のイデアルとする．$I = \{0\}$ ならば，$m = 0$ とおけば，$I = m\mathbb{Z}$ である．$I \supsetneq \{0\}$ とする．このとき，$a \in I$ ならば，$-a \in I$ だから，I は必ず正の整数を含む．m を I に含まれる最小の正の整数とする．このとき，任意の $a \in I$ に対して，a を m で割算して，

$$a = mq + r,\ q \in \mathbb{Z},\ 0 \leq r < m$$

とかく．$r = a - mq \in I$ より，m の最小性から，$r = 0$ でなければならない．したがって，$a = mq \in m\mathbb{Z}$ となる．すなわち，$I \subset m\mathbb{Z}$ である．$I \supset m\mathbb{Z}$ は明かであるから，$I = m\mathbb{Z}$ を得る． □

定義 1.11. R を環とし，I をそのイデアルとする．各 $a \in R$ に対して，R の部分集合

$$a + I = \{a + x \,|\, x \in I\}$$

を，a によって代表される I を法とする**剰余類**という．$a+I = b+I \Longleftrightarrow a-b \in I$ である．I を法とする剰余類全体からなる集合を R/I で表す．すなわち，

$$R/I = \{a + I \,|\, a \in I\}.$$

命題 1.12. I を環 R のイデアルとする．このとき，R/I は自然に環になる．R の I による**剰余環**という．

[証明]　R/I に加法，乗法を次のように定義する．$a + I = \bar{a}$ とかく．

$$\bar{a} + \bar{b} = \overline{a+b},$$
$$\bar{a}\bar{b} = \overline{ab}.$$

これは代表元のとりかたによらず矛盾なく定義される．$\bar{0}$ は R/I の零元，$\bar{1}$ は R/I の単位元であり，$-\bar{a} = \overline{-a}$,

$$\begin{aligned}(\bar{a} + \bar{b}) + \bar{c} &= \overline{a+b} + \bar{c} = \overline{(a+b)+c} \\ \bar{a} + (\bar{b} + \bar{c}) &= \bar{a} + \overline{b+c} = \overline{a+(b+c)}\end{aligned}$$

□

定義 1.13. 環 R のイデアル $I \neq R$ について，R/I が整域のとき，I は R の**素イデアル**であるといい，R/I が体のとき，I は R の**極大イデアル**であるという．

命題 1.14. 環 R のイデアル $I \subsetneq R$ について，

$$\begin{aligned}I \text{ が素イデアル} &\iff a, b \in R, ab \in I \text{ ならば } a \in I \text{ または } b \in I; \\ I \text{ が極大イデアル} &\iff I \subsetneq J \subsetneq R \text{ をみたすイデアル } J \text{ は存在しない.}\end{aligned}$$

[証明]　素イデアルについては明らか．J を $I \subsetneq J \subset R$ をみたすイデアルとすると，$a \in J$，$a \notin I$ をとれる．このとき，R/I は体であり，$\bar{a} = a + I \in R/I$，$\bar{a} \neq 0$ だから，$b \in R$ で，$\bar{a}\bar{b} = \bar{1}$ となるものがある．すなわち，$ab = 1 + c$，$c \in I \subset J$ とかける．したがって，$1 = ab - c \in J$，$R \subset J$ となり，$J = R$ を得る．逆に，$I \subsetneq J \subsetneq R$ をみたすイデアル J は存在しないとする．このとき，任意の $a \in R$, $a \notin I$ をとる．

$$J = I + Ra = \{x + ya \,|\, x \in I, y \in R\}$$

とおく．明らかに，J はイデアルであり，$a \in J$ だから $I \subsetneq J \subset R$ である．仮定から，$J = R$ となる．特に，$1 \in R = J$ だから，$1 = x + ya$，$x \in I$，$y \in R$ となる．したがって，R/I において，$\bar{y}\bar{a} = \bar{1}$．ゆえに，R/I は体である．すなわち，I は極大イデアルである．□

例 1.15. $\mathbb{Z}$ の素イデアルは 0 と $p\mathbb{Z}$ (p は素数) である．このうち，$p\mathbb{Z}$ は極大イデアルである．$m = ab,\ 1 < a, b < m$ ならば，$a \notin I,\ b \notin I$ であるが，$ab = m \in I$ であるから，$I = m\mathbb{Z}$ は素イデアルではない．また，$p\mathbb{Z} \subset J \subset \mathbb{Z}$ となるイデアル J が存在したとすれば，$J = m\mathbb{Z}$ より，$p = mt$ となるが，p は素数であるから，$m = 1$ または $m = p$，すなわち，$J = \mathbb{Z}$ または $J = p\mathbb{Z}$ である．ゆえに，$p\mathbb{Z}$ は極大イデアルであり，したがって，$\mathbb{Z}/p\mathbb{Z}$ は体である．

体 $\mathbb{Z}/p\mathbb{Z}$ を $\mathbb{F}_p$ とかく．$\mathbb{F}_p$ を p 個の元からなる**有限体**という．

1.3 有理整数環 $\mathbb{Z}$

ここでは，$R = \mathbb{Z},\ I = m\mathbb{Z}$ $(m \in \mathbb{N})$ として，商環 $\mathbb{Z}/m\mathbb{Z}$ を考察する．$a \in \mathbb{Z}$ によって代表される剰余類 $a + m\mathbb{Z}$ を $\bar{a}$ とかくことにする．$\mathbb{Z}/m\mathbb{Z} = \{\bar{0}, \bar{1}, \cdots, \overline{m-1}\}$ である．$\bar{a} = \bar{b}$ を $a \equiv b \pmod{m}$ とかく．

補題 1.16. n 個の整数 $a_1, \cdots, a_n$ に対して，

$$I = \{a_1x_1 + \cdots + a_nx_n \,|\, x_1, \cdots, x_n \in \mathbb{Z}\}$$

とおけば，I は $\mathbb{Z}$ のイデアルであり，m を $I = m\mathbb{Z}$ となる正の整数とすると (命題 1.10)，m は n 個の整数 $a_1, \cdots, a_n$ の最大公約数である．

[証明]　I がイデアルであることは明か．$a_j \in I$ より，$m | a_j$ $(j = 1, \cdots, n)$．すなわち，m は整数 $a_1, \cdots, a_n$ の公約数である．d を整数 $a_1, \cdots, a_n$ の公約数とすると，$a_j = db_j,\ b_j \in \mathbb{Z}$ $(j = 1, \cdots, n)$ とかける．一方，$m = a_1x_1 + \cdots + a_nx_n$ とかけるから，$m = d(b_1x_1 + \cdots + b_nx_n)$．すなわち，$d | m$．したがって，$m$ は整数 $a_1, \cdots, a_n$ の最大公約数である．□

整数 $a_1, \cdots, a_n$ の最大公約数を $\gcd(a_1, \cdots, a_n)$ とかく．

命題 1.17. $\bar{a} \in \mathbb{Z}/m\mathbb{Z}$ に対して，

$$\bar{a} \in (\mathbb{Z}/m\mathbb{Z})^\times \iff \gcd(a, m) = 1.$$

[証明]　$\bar{a} \in (\mathbb{Z}/m\mathbb{Z})^\times$ ならば，$\bar{x} \in (\mathbb{Z}/m\mathbb{Z})$ で $\bar{a}\bar{x} = \bar{1}$ となるものが存在する．すなわち，$ax = 1 + my$ $(\exists y \in \mathbb{Z})$．このとき, 明らかに $\gcd(a, m) = 1$.

逆に，$\gcd(a, m) = 1$ ならば，命題 1.16 より，$ax + my = 1$ となる $x, y \in \mathbb{Z}$ が存在する．すなわち，$\bar{a}\bar{x} = \overline{ax} = \bar{1}$.　□

定義 1.18. $m > 1$ に対して，$(\mathbb{Z}/m\mathbb{Z})^\times$ の元の個数を $\varphi(m)$ とし，$\varphi(1) = 1$ とする．命題 1.17 より，

$$\varphi(m) = \#\{a \in \mathbb{Z} \,|\, 0 \le a \le m-1,\ \gcd(a, m) = 1\}$$

である．この関数 φ を**オイラーの関数**という．p を素数とすれば，$\varphi(p) = p - 1$ である．

定理 1.19 (フェルマーの小定理). p を素数とすると，$\gcd(a,p)=1$ なる $a\in\mathbb{Z}$ に対して，

$$a^{p-1}\equiv 1 \pmod{p}.$$

[証明]　有限体 $\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$ において考える．$a\in\mathbb{F}_p$, $a\neq 0$ をとり固定する．写像 $f:\mathbb{F}_p^\times\longrightarrow\mathbb{F}_p^\times$ を，$f(x)=ax$, $x\in\mathbb{F}_p^\times$ によって定義する．そのとき，f は単射である．実際，$f(x)=f(y)$, $x,y\in\mathbb{F}_p^\times$ とすれば，$ax=ay$, $a(x-y)=0$. $a\neq 0$ だから，$x-y=0$, $x=y$ である．ゆえに，f は単射である．f は有限集合 $\mathbb{F}_p^\times$ から自分自身への単射だから，全単射である．よって，$f(1),f(2),\dots,f(p-1)$ は $\mathbb{F}_p^\times$ の元全体である．特に，これらすべての積をとれば，

$$f(1)f(2)\cdots f(p-1)=1\cdot 2\cdots(p-1)$$

をえる．この左辺は，

$$(a\cdot 1)(a\cdot 2)\cdots(a(p-1))=a^{p-1}\cdot 1\cdot 2\cdots(p-1)$$

に等しい．$1\cdot 2\cdots(p-1)\in\mathbb{F}_p^\times$ だから，$a^{p-1}=1$ を得る．　□

上と全く同様にして，次の定理を得られる．

定理 1.20. $m\geq 2$ とすると，$\gcd(a,m)=1$ なる $a\in\mathbb{Z}$ に対して，

$$a^{\varphi(m)}\equiv 1 \pmod{m}.$$

練習問題 1. 2^{10000} を 13 で割ったときの余りを求めよ．3^{10000} を 17 で割ったときの余りを求めよ．

1.4　ユークリッドの互除法

補題 1.21. 整数 a, b, $b>0$ に対して，r を a を b で割ったときの余りとすれば，$\gcd(a,b)=\gcd(b,r)$.

[証明]　$a=bq+r$ とかける．$m=\gcd(a,b)$, $n=\gcd(b,r)$ とすれば，

$$\begin{aligned}\{ax+by\,|\,x,y\in\mathbb{Z}\} &= m\mathbb{Z},\\ \{bx+ry\,|\,x,y\in\mathbb{Z}\} &= n\mathbb{Z}\end{aligned}$$

である．$m\mathbb{Z}$ の任意の元 z は $z=ax+by$, $x,y\in\mathbb{Z}$ とかける．そのとき，$a=bq+r$ より，

$$z=(bq+r)x+by=b(qx+y)+rx\in n\mathbb{Z}.$$

したがって，$m\mathbb{Z}\subset n\mathbb{Z}$．$n\mathbb{Z}$ の任意の元 w は $w=bx+ry$, $x,y\in\mathbb{Z}$ とかける．そのとき，$a=bq+r$, $r=a-bq$ より，

$$w=bx+(a-bq)y=ay+b(x-qy)\in m\mathbb{Z}.$$

したがって，$n\mathbb{Z}\subset m\mathbb{Z}$．ゆえに，$m\mathbb{Z}=n\mathbb{Z}$, $m=n$ である．　□

定理 1.22 (Euclid の互除法)**.** 自然数 a, b に対して，

$$\begin{aligned} a &= bq_0 + r_1, \quad 0 \le r_1 < b, \\ b &= r_1 q_1 + r_2, \quad 0 \le r_2 < r_1, \\ r_1 &= r_2 q_2 + r_3, \quad 0 \le r_3 < r_2, \\ &\cdots\cdots\cdots \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n, \quad 0 \le r_n < r_{n-1}, \\ r_{n-1} &= r_n q_n \end{aligned}$$

であるとすると，$\gcd(a, b) = r_n$.

[証明]　補題 1.21 によって，$\gcd(a, b) = \gcd(b, r_1)$ である．これを繰り返せば，

$$\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-1}, r_n) = r_n$$

となる． □

練習問題 2. 1995 と 1029 の最大公約数を求める．

$$\begin{aligned} 1995 &= 1029 \times 1 + 966, \\ 1029 &= 966 \times 1 + 63, \\ 966 &= 63 \times 15 + 21, \\ 63 &= 21 \times 3. \end{aligned}$$

したがって，$\gcd(1995, 1029) = 21$ である．

整数 a, b が与えられたとき，$d = \gcd(a, b)$ とすると，

$$ax - by = d$$

を満たすような整数 x, y を見つけることがユークリッドの互除法を応用することによってできる．これを具体例で説明する．

例 1.23. 671 と 237 の最大公約数を求める．

$$\begin{aligned} 671 &= 237 \times 2 + 197, & 40 &= 37 \times 1 + 3, \\ 237 &= 197 \times 1 + 40, & 37 &= 3 \times 12 + 1, \\ 197 &= 40 \times 4 + 37, & 3 &= 1 \times 3. \end{aligned}$$

これから，$\gcd(671, 237) = 1$ となる．この計算を利用して，

$$671x + 237y = 1$$

を満たす整数 x, y をすべて求めることができる．

$$\begin{aligned} 1 &= 37 - 3 \times 12 \\ &= 37 - (40 - 37 \times 1) \times 12 = 37 \times 13 - 40 \times 12 \\ &= (197 - 40 \times 4) \times 13 - 40 \times 12 = 197 \times 13 - 40 \times 64 \\ &= 197 \times 13 - (237 - 197 \times 1) \times 64 = 197 \times 77 - 237 \times 64 \\ &= (671 - 237 \times 2) \times 77 - 237 \times 64 \\ &= 671 \times 77 - 237 \times 218. \end{aligned}$$

したがって，$x_1 = 77$, $y_1 = -218$ とおけば，$671x_1 + 237y_1 = 1$ を満たす．$x = x_1 + 237k$, $y = y_1 - 671k$, $k \in \mathbb{Z}$ は

$$671x + 237y = 1$$

を満たす．逆に，一般解は，このように表せる．実際，

$$671x_1 + 237y_1 = 1, \tag{1.1}$$

$$671x + 237y = 1 \tag{1.2}$$

とするとき，$(1.1) \times x - (1.2) \times x_1$ より，$x - x_1 = 237(xy_1 - x_1y)$, $(1.1) \times y - (1.2) \times y_1$ より，$y - y_1 = 671(x_1y - xy_1) = -671(xy_1 - x_1y)$ である．よって，$xy_1 - x_1y = k$ とおけば，$x - x_1 = 237k$, $y - y_1 = -671k$,

$$\begin{cases} x &= 77 + 237k, \\ y &= -218 - 671k, \quad k \text{ は任意の整数.} \end{cases}$$

練習問題 3. $\mathbb{F}_{37} = \mathbb{Z}/37\mathbb{Z}$ において，1 次方程式

$$13x + 5 = 0$$

を解け (ある自然数 x を 13 倍して 5 を加えたら 37 の倍数になった．このような x で最小のものを求めよ).

1.5 多項式環

ここでは，K を任意の体として，K の元を係数とする 1 変数 x の多項式全体のなす環を $K[x]$ で表す．$f(x) \in K[x]$, $f(x) \neq 0$ を

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n, \quad a_i \in K \ (0 \leq i \leq n), \ a_0 \neq 0$$

とかくとき，n を $f(x)$ の**次数**といい，$\deg f(x)$ で表す．

$$\deg f(x)g(x) = \deg f(x) + \deg g(x)$$

が成り立つ．

命題 1.24. 任意の $g(x) \in K[x]$ と任意の $f(x) \in K[x], f(x) \neq 0$ に対して，$q(x), r(x) \in K[x]$ で，

$$g(x) = f(x)q(x) + r(x), \quad r(x) = 0 \text{ または } \deg r(x) < \deg f(x)$$

を満たすものがただ一組存在する．

[証明]　まず，$q(x)$, $r(x)$ の存在を示す．

$$\begin{aligned} f(x) &= a_0x^n + \cdots + a_{n-1}x + a_n, \\ g(x) &= b_0x^m + \cdots + b_{m-1}x + b_m, \end{aligned}$$

$a_0 \neq 0$, $b_0 \neq 0$ とする．$m - n = l$ とおき，l に関する帰納法を用いる．$l < 0$ ならば，$q(x) = 0$, $r(x) = g(x)$ とすればよい．$l = 0$ のとき，$q(x) = b_0/a_0$,

$$r(x) = g(x) - (b_0/a_0)f(x) = (b_1 - (b_0/a_0)a_1)x^{n-1} + \cdots + (b_n - (b_0/a_0)a_n)$$

とおけば，$g(x) = f(x)q(x) + r(x)$, $r(x) = 0$ または $\deg r(x) < \deg f(x)$ である．$l > 0$ のとき，

$$g_1(x) = g(x) - (b_0/a_0)x^{m-n}f(x) = (b_1 - (b_0/a_0)a_1)x^{m-1} + (\text{低次の項})$$

とおけば，$g_1(x) = 0$ または $\deg g_1(x) - n < m - n = l$ であるから，帰納法の仮定によって，

$$g_1(x) = f(x)q_1(x) + r_1(x), \ r_1(x) = 0 \text{ または } \deg r_1(x) < \deg f(x)$$

となる $q_1(x), r_1(x) \in K[x]$ が存在する．そのとき，

$$q(x) = (b_0/a_0)x^{m-n} + q_1(x), \quad r(x) = r_1(x)$$

とおけばよい．

一意性を示す．

$$g(x) = f(x)Q(x) + R(x), \quad R(x) = 0 \text{ または } \deg R(x) < \deg f(x)$$

ともかけたとする．そのとき，

$$R(x) - r(x) = f(x)(q(x) - Q(x))$$

となる．左辺は 0 または次数が $\deg f(x)$ より小さいが，右辺は $f(x)$ の倍数であるから，両辺とも 0 でなければならない．すなわち，$Q(x) = q(x)$, $R(x) = r(x)$ である． □

系 1.25. $f(x) \in K[x]$, $a \in K$ とする．そのとき，

$$f(x) \text{ が } x - a \text{ で割りきれる} \iff f(a) = 0.$$

[証明]　命題 1.24 より，$\exists q(x), r(x) \in K[x]$,

$$f(x) = (x-a)q(x) + r(x), \quad r(x) = 0 \text{ または } \deg r(x) = 0.$$

$r(x)$ は定数である．$x = a$ を代入して，$f(a) = r(a) = r(x)$ を得る．したがって，

$$f(x) \text{ が } x-a \text{ で割りきれる} \iff r(x) = 0 \iff f(a) = 0$$

である． □

命題 1.26. $f(x) \in K[x]$, $\deg f(x) = n > 0$ とする．そのとき，$f(a) = 0$ を満たす $a \in K$ は高々 n 個しかない．

[証明]　n に関する帰納法を用いる．$n = 1$ のときは明か．$n > 1$ のとき，もし，$f(a) = 0$ となる $a \in K$ がなければ，主張は自明である．$f(a_1) = 0$ となる $a_1 \in K$ があったとする．そのとき，系 1.25 より，$f(x) = (x-a_1)f_1(x)$, $f_1(x) \in K[x]$ とかける．$\deg f_1(x) = n-1$ であるから，帰納法の仮定より，$f_1(a) = 0$ となる $a \in K$ は高々 $n-1$ 個しかない．よって，$f(a) = (a-a_1)f_1(a) = 0$ となる $a \in K$ は高々 n 個しかない． □

命題 1.27 (ウィルソンの定理)**.** p を素数とすると，

$$(p-1)! = (p-1)(p-2)\cdots 2 \cdot 1 \equiv -1 \pmod{p}$$

[証明]　$K = \mathbb{Z}/p\mathbb{Z}$ とおく．フェルマーの小定理によって，任意の $a \in K^\times$ は $a^{p-1} = 1$ を満たす．したがって，$f(x) = x^{p-1} - 1 \in K[x]$ について，系 1.25 を適用すれば，任意の $a \in K^\times$ について，$x - a | x^{p-1} - 1$ である．次数と x^{p-1} の係数を見れば，

$$x^{p-1} - 1 = \prod_{a \in K^\times} (x-a)$$

を得る．その定数項を比べて，$-1 = (-1)^{p-1} \prod_{a \in K^\times} a$ を得る． □

[別証明] $G = (\mathbb{Z}/p\mathbb{Z})^\times$ とおけば，$a \in G$ で，$a = a^{-1}$ すなわち，$a^2 = 1$ を満たすものは，$a = 1, p-1$ だけである．したがって，$\prod_{a \in G} a$ において，$1, p-1$ 以外の $a \in G$ に対しては，a と a^{-1} が現れるから，$\prod_{a \in G} a = p-1$ を得る． □

命題 1.28. $K[x]$ のイデアル I に対して，$\exists f(x) \in K[x]$, $I = f(x)K[x]$.

[証明]　$I \neq \{0\}$ としてよい．$f(x)$ を I に属する 0 でない多項式で次数が最小のものとする．このとき，任意の $g(x) \in I$ に対して，

$$g(x) = q(x)f(x) + r(x), \quad r(x) = 0 \text{ or } \deg r(x) < \deg f(x)$$

とかける．$f(x), g(x) \in I$ より，$r(x) = g(x) + (-q(x))f(x) \in I$．$f(x)$ の次数が最小であることから，$r(x) = 0$ でなければならない．よって，$g(x) \in f(x)K[x]$, $I \subset f(x)K[x]$．$f(x)K[x] \subset I$ は明らかである． □

2　環の準同型

2.1　準同型定理

定義 2.1. 環 R から環 R' への写像 $f : R \longrightarrow R'$ が

$$f(a+b) = f(a) + f(b),\ \ f(ab) = f(a)f(b)\ \ \forall a, b \in R,$$

$$f(1) = 1'\ \ (1'\text{は } R'\text{の単位元})$$

を満たすとき，f は**準同型**であるという．また，環 R から環 R' への準同型 f が全単射であるとき，f を同型といい，$f : R \cong R'$ とかく．

$f : R \longrightarrow R'$ が準同型ならば，$f(0) = 0'$ ($0'$ は R' の零元)，$f(-a) = -f(a), \forall a \in R$ が成立する．$\ker f = \{a \in R \,|\, f(a) = 0'\} \subset R$ を f の**核**という．また，$f(R) = \{f(a) \,|\, a \in R\} \subset R'$ を f の**像**という．容易に，

f が単射 $\Longleftrightarrow \ker f = \{0\}$;

f が全射 $\Longleftrightarrow f(R) = R'$.

がわかる．

定理 2.2 (準同型定理)**.** $f : R \longrightarrow R'$ を環 R から環 R' への準同型とすると，$\ker f$ は R のイデアルであり，$f(R)$ は R' の部分環である．さらに，f は自然な同型 $R/\ker f \cong f(R)$ を引き起こす.

例 2.3. $f : \mathbb{R}[x] \longrightarrow \mathbb{C}$ を $f(g(x)) = g(i)$, i は虚数単位，によって定義する．f は準同型である．$f(a+bx) = a+bi$ より，f は全射である．$g(x) \in \ker f$ とすると，$g(i) = 0$ である．命題 1.24 より，

$$g(x) = (x^2+1)q(x) + a + bx, \quad q(x) \in \mathbb{R}[x],\ a, b \in \mathbb{R}$$

とかけるから，

$$0 = g(i) = (i^2+1)q(i) + a + bi = a + bi$$

である．ゆえに，$a = b = 0$, $g(x) = (x^2+1)q(x) \in (x^2+1)\mathbb{R}[x]$．したがって，$\ker f \subset (x^2+1)\mathbb{R}[x]$ である．逆に，$g(x) \in (x^2+1)\mathbb{R}[x]$ ならば，$f(g(x)) = g(i) = 0$ であるから，$g(x) \in \ker f$, $(x^2+1)\mathbb{R}[x] \subset \ker f$ である．ゆえに，$\ker f = (x^2+1)\mathbb{R}[x]$ である．準同型定理によって，同型

$$\mathbb{R}[x]/(x^2+1)\mathbb{R}[x] \cong \mathbb{C}$$

を得る．$\bar{x} = x + (x^2+1)\mathbb{R}[x]$ が i に対応している．

例 2.4. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \,|\, a, b \in \mathbb{Q}\}$ とおけば，これは $\mathbb{C}$ の部分体であることがわかる．$f : \mathbb{Q}[x] \longrightarrow \mathbb{Q}(\sqrt{2})$ を $f(g(x)) = g(\sqrt{2})$ によって定義する．f は準同型である．$f(a + bx) = a + b\sqrt{2}$ より，f は全射である．$g(x) \in \ker f$ とすると，$g(\sqrt{2}) = 0$ である．命題 1.24 より，

$$g(x) = (x^2 - 2)q(x) + a + bx, \quad q(x) \in \mathbb{Q}[x],\ a, b \in \mathbb{Q}$$

とかけるから，

$$0 = g(\sqrt{2}) = (\sqrt{2}^2 - 2)q(\sqrt{2}) + a + b\sqrt{2} = a + b\sqrt{2}$$

である．$\sqrt{2}$ は無理数であるから，$a = b = 0$,

$$g(x) = (x^2 - 2)q(x) \in (x^2 - 2)\mathbb{Q}[x].$$

したがって，$\ker f \subset (x^2 - 2)\mathbb{Q}[x]$ である．逆に，$g(x) \in (x^2 - 2)\mathbb{Q}[x]$ ならば，$f(g(x)) = g(\sqrt{2}) = 0$ であるから，$g(x) \in \ker f$, $(x^2 - 2)\mathbb{Q}[x] \subset \ker f$ である．ゆえに，$\ker f = (x^2 - 2)\mathbb{Q}[x]$ である．準同型定理によって，同型

$$\mathbb{Q}[x]/(x^2 - 2)\mathbb{Q}[x] \cong \mathbb{Q}(\sqrt{2})$$

を得る．$\bar{x} = x + (x^2 - 2)\mathbb{Q}[x]$ が $\sqrt{2}$ に対応している．

2.2 中国剰余定理

定義 2.5. $R_i, i = 1, \cdots, n$ を環とし $R = R_1 \times \cdots \times R_n$ を集合としての直積とする．今，$x = (x_1, \cdots, x_n), y = (y_1, \cdots, y_n) \in R$ に対して，

$$x + y = (x_1 + y_1, \cdots, x_n + y_n),\ xy = (x_1y_1, \cdots, x_ny_n)$$

によって和と積を定義すれば，R は環になる．

定義 2.6. 環 R のイデアル A, B に対して，その和 $A + B$ を

$$A + B = \{a + b \,|\, a \in A, b \in B\}$$

によって定義すれば，$A + B$ は R のイデアルになる．また，A, B の積 AB を

$$AB = \{\sum_i a_ib_i \,|\, a_i \in A, b_i \in B\}$$

によって定義すれば，AB は R のイデアルである．

定理 2.7 (中国剰余定理). R を環，$A_1, \cdots, A_l$ を R のイデアルで，$A_i + A_j = R$, $(i \neq j)$ を満たすとする．そのとき，$A = \cap_{i=1}^{l} A_i$ とおくと，

$$R/A \cong (R/A_1) \times \cdots \times (R/A_l),$$

$$(R/A)^{\times} \cong (R/A_1)^{\times} \times \cdots \times (R/A_l)^{\times}.$$

[証明] $l = 2$ の場合を示す．A, B を R のイデアルで，$A + B = R$ を満たすものとする．写像 $f : R \longrightarrow (R/A) \times (R/B)$ を $f(\gamma) = (\gamma + A, \gamma + B)$ によって定義する．f は準同型である．実際,

$$\begin{aligned} f(\gamma_1 + \gamma_2) &= (\gamma_1 + \gamma_2 + A, \gamma_1 + \gamma_2 + B) \\ &= (\gamma_1 + A, \gamma_1 + B) + (\gamma_2 + A, \gamma_2 + B) \\ &= f(\gamma_1) + f(\gamma_2), \\ f(\gamma_1\gamma_2) &= (\gamma_1\gamma_2 + A, \gamma_1\gamma_2 + B) \\ &= (\gamma_1 + A, \gamma_1 + B)(\gamma_2 + A, \gamma_2 + B) \\ &= f(\gamma_1)f(\gamma_2), \\ f(1) &= (1 + A, 1 + B) \end{aligned}$$

である．$(A, B) = 1$ より，$a + b = 1$ なる $a \in A, b \in B$ がある．このとき，任意の $\alpha \in R, \beta \in R$ に対して，$\gamma = \alpha b + \beta a$ とおけば,

$$\gamma - \alpha = \alpha(b - 1) + \beta a = (\beta - \alpha)a \in A$$

より，$\gamma + A = \alpha + A$.

$$\gamma - \beta = \alpha b + \beta(a - 1) = (\alpha - \beta)b \in B$$

より，$\gamma + B = \beta + B$．よって，$f(\gamma) = (\alpha + A, \beta + B)$ である．これは，f が全射であることを示している．$\ker f = A \cap B$ は明か．準同型定理によって，$R/(A \cap B) \cong (R/A) \times (R/B)$. さらに，$(A, C) = (B, C) = 1$ ならば，$a' + c = 1, b' + c' = 1$ なる $a' \in A, b' \in B, c \in C, c' \in C$ があるから,

$$1 = a'b' + (b'c + a'c' + cc'),\ a'b' \in A \cap B,\ (b'c + a'c' + cc') \in C,$$

すなわち，$(A \cap B, C) = 1$．よって上の議論から,

$$R/(A \cap B \cap C) \cong (R/(A \cap B)) \times (R/C) \cong (R/A) \times (R/B) \times (R/C).$$

これを繰り返せばよい． □

注意 2.8. 上の命題で，$A = \cap_i A_i = \prod_i A_i$ である．

[証明] $(A,B)=1$ のとき，$A\cap B=AB$ を示せばよい．定義から明らかに，$A\cap B\supset AB$ である．$(A,B)=1$ だから，$a\in A$，$b\in B$ で $a+b=1$ となるものがある．このとき，任意の $c\in A\cap B$ に対して，

$$c=c\cdot 1=c(a+b)=ca+cb\in AB$$

である．よって，$A\cap B\subset AB$．ゆえに，$A\cap B=AB$. □

系 2.9. $m=m_1\cdots m_l$, $m_i>1$, $\gcd(m_i,m_j)=1, i\neq j$，$R=\mathbb{Z}/m\mathbb{Z}$, $R_i=\mathbb{Z}/m_i\mathbb{Z}$ とすると，自然な写像によって

$$R\cong R_1\times\cdots\times R_l,$$

$$R^\times\cong R_1^\times\times\cdots\times R_l^\times,$$

$$\varphi(m)=\varphi(m_1)\cdots\varphi(m_l)$$

が成り立つ.

補題 2.10. p を素数とすると $\varphi(p^e)=p^{e-1}(p-1)$.

[証明] $\varphi(m)$ の定義と命題 1.17 から，

$$\begin{aligned}\varphi(p^e) &= \#\{a\in\mathbb{Z}; 0\le a\le p^e-1,\ (a,p^e)=1\}\\ &= \#\{a\in\mathbb{Z}; 0\le a\le p^e-1,\ (a,p)=1\}\\ &= p^e-p^{e-1}.\end{aligned}$$

□

上の系と補題から直ちに，

命題 2.11. 自然数 m に対して，$m=p_1^{e_1}\cdots p_r^{e_r}$ をその素因数分解とすれば，

$$\varphi(m)=m\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_r}\right).$$

練習問題 4. $m=105=3\times5\times7$ に対して，中国剰余定理を適用すれば，

$$\mathbb{Z}/105\mathbb{Z}\cong(\mathbb{Z}/3\mathbb{Z})\times(\mathbb{Z}/5\mathbb{Z})\times(\mathbb{Z}/7\mathbb{Z})$$

である．$a+m\mathbb{Z}=[a]_m\in\mathbb{Z}/m\mathbb{Z}$ とかくとき，上の同型は $f([x]_{105})=([x]_3,[x]_5,[x]_7)$ によって与えられた．$f([a]_{105})=([1]_3,[0]_5,[0]_7)$，$f([b]_{105})=([0]_3,[1]_5,[0]_7)$，$f([a]_{105})=([0]_3,[0]_5,[1]_7)$，を満たす $[a]_{105},[b]_{105},[c]_{105}$ を求めよ．さらに，これを用いて，

$$f([xa+yb+zc]_{105})=([x]_3,[y]_5,[z]_7)$$

が成り立つことを示せ．特に $([x]_3,[y]_5,[z]_7)=([2]_3,[3]_5,[5]_7)$ として，3 で割った余りが 2，5 で割った余りが 3，7 で割った余りが 5 であるような最小の自然数を求めよ $(a=70,b=21,c=15,\ 68)$.

3　原始根の存在

15 の正の約数は $1, 3, 5, 15$ であり，

$$\varphi(1) + \varphi(3) + \varphi(5) + \varphi(15) = 1 + 2 + 4 + 8 = 15$$

である．一般に，次が成り立つ．

補題 3.1. オイラー関数 φ は任意の自然数 n に対して，

$$\sum_{d|n} \varphi(d) = n$$

を満たす．

[証明]　自然数 n に対して，

$$F(n) = \sum_{d|n} \varphi(d)$$

とおくとき，$F(n) = n$ が成り立つことを示せばよい．$n = p$, p は素数ならば，$n = p$ の約数は 1, p であるから，

$$F(p) = \varphi(1) + \varphi(p) = 1 + p - 1 = p$$

であり，補題の主張は正しい．$n = p^k$ のときは，$n = p^k$ の約数は $1, p, \ldots, p^{k-1}, p^k$ であるから，

$$\begin{aligned} F(p^k) &= \varphi(1) + \varphi(p) + \cdots + \varphi(p^k) \\ &= 1 + p - 1 + p(p-1) + \cdots + p^{k-1}(p-1) \\ &= p^k \end{aligned}$$

であり，この場合も補題の主張は正しい．一般の場合は，$\gcd(m, n) = 1$ ならば，$F(mn) = F(m)F(n)$ が成り立つことを用いる．実際，m の約数の全体を $d_1, \ldots, d_r$, n の約数の全体を $e_1, \ldots, e_s$ とすれば，mn の約数は $d_i e_j$ の形に一意的に表せ，そのとき，$\gcd(d_i, e_j) = 1$ であるから，系 2.9 によって，$\varphi(d_i e_j) = \varphi(d_i)\varphi(e_j)$ である．よって，

$$\begin{aligned} F(mn) &= \sum_{i=1}^{r} \sum_{j=1}^{s} \varphi(d_i e_j) = \sum_{i=1}^{r} \sum_{j=1}^{s} \varphi(d_i)\varphi(e_j) \\ &= \sum_{i=1}^{r} \varphi(d_i) \sum_{j=1}^{s} \varphi(e_j) = \sum_{i=1}^{r} \varphi(d_i) F(n) \\ &= F(n) \sum_{i=1}^{r} \varphi(d_i) = F(n)F(m). \end{aligned}$$

よって，一般に，$n = p_1^{a_1} \cdots p_r^{a_r}$ と素因数分解すれば，

$$F(n) = F(p_1^{a_1}) \cdots F(p_r^{a_r}) = p_1^{a_1} \cdots p_r^{a_r} = n.$$

□

定義 3.2. p を素数とし，$a \in \mathbb{F}_p^\times$ とする．そのとき，$a^n = 1$ となる最小の自然数 n を $e_p(a)$ で表し，a の $\mathbb{F}_p^\times$ における**位数**とよぶ．フェルマーの小定理により，$a^{p-1} = 1$ であるから，$e_p(a) \leq p-1$ である．

例 3.3. $e_p(1) = 1$ である．$p = 7$ とする．$\mathbb{F}_7^\times$ において，$\bar{2}^1 = \bar{2}$, $\bar{2}^2 = \bar{4}$, $\bar{2}^3 = 1$ であるから，$e_7(2) = 3$ である．

$$\bar{3}^1 = \bar{3}, \quad \bar{3}^2 = \bar{2}, \quad \bar{3}^3 = \bar{6}, \quad \bar{3}^4 = \bar{4}, \quad \bar{3}^5 = \bar{5}, \quad \bar{3}^6 = 1$$

より，$e_7(\bar{3}) = 6$ である．

補題 3.4. p を素数とし，$a \in \mathbb{F}_p^\times$ とし，$a^n = 1$ とする．そのとき，n は $e_p(a)$ で割りきれる．特に，$e_p(a)$ は $p-1$ の約数である．

[証明]　$e = e_p(a)$ とおくと，$a^e = 1$ である．$a^n = 1$ とする．n を e で割ったときの商を q，余りを r とすると，

$$n = eq + r, \quad 0 \leq r < e$$

である．そのとき，

$$1 = a^n = a^{eq+r} = (a^e)^q a^r = 1^q a^r = a^r.$$

もし，$r \neq 0$ とすると，r は e より小さな自然数で，$a^r = 1$ を満たすことになる．これは，$e = e_p(a)$ が a の p を法とする位数であることに矛盾する．ゆえに，$r = 0$ であり，$n = eq$ である．また，フェルマーの小定理により，$a^{p-1} = 1$ であるから，上で示したことから，$p-1$ は $e_p(a)$ で割りきれ，$e_p(a)$ は $p-1$ の約数である．□

定義 3.5. 素数 p に対して，$g \in \mathbb{F}_p^\times$ で，$e_p(g) = p-1$ であるようなものを，$\mathbb{F}_p$ の**原始根**という．

$e_7(\bar{3}) = 6$ であったから，$\bar{3}$ は $\mathbb{F}_7$ の原始根である．

補題 3.6. p を素数とする．$n \geq 1$ を $p-1$ の任意の約数とする．そのとき，$a \in \mathbb{F}_p^\times$ で，$X^n - 1 = 0$ の根であるものは丁度 n 個存在する．

[証明]　$p - 1 = nk$ とかく．そのとき，$\mathbb{F}_p$-係数の多項式

$$Y^k - 1 = (Y-1)(Y^{k-1} + Y^{k-2} + \cdots + Y + 1)$$

に $Y = X^n$ を代入すれば，$\mathbb{F}_p$-係数の多項式の等式

$$\underbrace{X^{p-1}-1}_{p-1=nk\text{ 個の根}} = \underbrace{(X^n-1)}_{n\text{ 個以下の根}}\underbrace{((X^n)^{k-1}+(X^n)^{k-2}+\cdots+X^n+1)}_{nk-n\text{ 個以下の根}}$$

を得る．命題 1.26 より，体 $\mathbb{F}_p$ における X^n-1 の根は n 個以下であり，$(X^n)^{k-1}+(X^n)^{k-2}+\cdots+X^n+1$ の根も $n(k-1)$ 個以下である．しかし，フェルマーの小定理によって，$X^{p-1}-1$ の体 $\mathbb{F}_p$ における根の数は丁度 $p-1$ 個である．したがって，X^n-1 の根も丁度 n 個存在しなければならない． □

定理 3.7. 任意の素数 p に対して，$\mathbb{F}_p$ の原始根は丁度 $\varphi(p-1)$ 個存在する．

[証明] $p-1$ の各約数 $d \geq 1$ に対して，$a \in \mathbb{F}_p^\times$ で，$e_p(a) = d$ となるものの個数を $\psi(d)$ で表す．$n \geq 1$ を $p-1$ の任意の約数とする．$a \in \mathbb{F}_p^\times$ が $a^n = 1$ を満たせば，補題 3.4 より，$e_p(a)$ は n の約数である．逆に，$e_p(a)$ が n の約数ならば，$a^n = 1$ である．したがって，補題 3.6 より，

$$\sum_{d|n}\psi(d) = \sum_{d|n}\sum_{\substack{a\in\mathbb{F}_p^\times \\ e_p(a)=d}} 1 = \sum_{\substack{a\in\mathbb{F}_p^\times \\ a^n=1}} 1 = n.$$

一方，補題 3.1 より，

$$\sum_{d|n}\varphi(d) = n.$$

これらの 2 つの等式から，$\psi(n) = \varphi(n)$ であることが次のように導かれる．まず，$n = q$ が素数のとき，

$$\psi(1)+\psi(q) = \varphi(1)+\varphi(q)$$

であるが，$\psi(1) = 1$, $\varphi(1) = 1$ であるから，$\psi(q) = \varphi(q)$ を得る．一般に，$n = q_1^{a_1}\cdots q_r^{a_r}$ と素因数分解する．そのとき，$S(n) = a_1+\cdots+a_r$ とおく．$S(n) = 1$ のときは，$n = q$ は素数であるから，$\psi(n) = \varphi(n)$ が成り立つ．$m \geq 2$ として，$S(n) \leq m-1$ のときは，$\psi(n) = \varphi(n)$ が成り立つと仮定する．$S(n) = m$ とする．n の任意の約数 d については，$d \neq n$ ならば，$S(d) \leq m-1$ であり，帰納法の仮定によって，$\psi(d) = \varphi(d)$ である．

$$\sum_{d|n,\, d\neq n}\psi(d)+\psi(n) = \sum_{d|n,\, d\neq n}\varphi(d)+\varphi(n)$$

より，$\psi(n) = \varphi(n)$ を得る．帰納法によって，$p-1$ のすべての約数 n について，$\psi(n) = \varphi(n)$ が成り立つ．特に，$n = p-1$ に対して，$\psi(p-1) = \varphi(p-1) > 0$ を得る．これは $\mathbb{F}_p$ の原始根が存在することを意味する．a を $\mathbb{F}_p$ の原始根とする． □

系 3.8. g を $\mathbb{F}_p$ の原始根とすれば，$\mathbb{F}_p^\times = \{1, g, g^2, \ldots, g^{p-2}\}$ である．

[証明]　g を $\mathbb{F}_p$ の原始根とすれば，$1,\ g,\ g^2,\ \ldots,\ g^{p-2}$ はすべて相異なる $\mathbb{F}_p^\times$ の元である．実際，$g^i = g^j,\ 0 \leq i < j \leq p-2$ とすると，$g^{j-i} = 1$ となるが，$0 < j-i < p-1$ であるから，これは，$e_p(g) = p-1$ に矛盾する．$\mathbb{F}_p^\times$ の元の個数は $p-1$ であるから，$1,\ g,\ g^2,\ \ldots,\ g^{p-2}$ は $\mathbb{F}_p^\times$ のすべての元を尽している．　□

練習問題 5. $p = 11, 13, 19$ について，$\mathbb{F}_p$ の原始根を求めよ．

4　平方剰余の相互法則

4.1　平方剰余

定義 4.1. p を 3 以上の素数とし，$a \in \mathbb{F}_p^\times$ とする．2 次方程式 $X^2 - a = 0$ が有限体 $\mathbb{F}_p$ において根を持つとき，a を $\mathbb{F}_p$ の**平方剰余**であるといい，そうでないとき，**平方非剰余**であるという．**ルジャンドル記号** $\left(\dfrac{a}{p}\right)$ を

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & a \text{ が平方剰余} \\ -1, & a \text{ が平方非剰余} \end{cases}$$

と定義する．

定理 3.7 と系 3.8 より，$g \in \mathbb{F}_p^\times$ が存在して，

$$\mathbb{F}_p^\times = \{g^k \,|\, 0 \leq k \leq p-2\}.$$

したがって，$a \in \mathbb{F}_p^\times$ が平方剰余ならば，$a = b^2,\ b = g^k$ とかけて，$a = g^{2k}$ とかける．逆に，$a = g^{2k}$ とかければ，$b = g^k$ とおくと，$a = g^{2k} = b^2$ であり，a は平方剰余である．ゆえに，$\mathbb{F}_p$ の平方剰余は，$g^{2k},\ 0 \leq k \leq (p-3)/2$ の $(p-1)/2$ 個あり，平方非剰余は，$g^{2k+1},\ 0 \leq k \leq (p-3)/2$ の $(p-1)/2$ 個ある．また，$a = g^k$ のとき，$\left(\dfrac{a}{p}\right) = (-1)^k$ が成り立つこともわかる．したがって，$a \longmapsto \left(\dfrac{a}{p}\right)$ は写像 $\mathbb{F}_p^\times \longrightarrow \{\pm 1\}$ で，

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

を満たすことがわかる．

命題 4.2. $\mathbb{F}_p$ の平方剰余，平方非剰余の個数はともに，$\dfrac{p-1}{2}$ である．

フェルマーの小定理によって，

$$\left(g^{\frac{p-1}{2}} - 1\right)\left(g^{\frac{p-1}{2}} + 1\right) = g^{p-1} - 1 = 0$$

であるが，g の位数は丁度 $p-1$ であるから，$g^{\frac{p-1}{2}}-1\neq 0$．したがって，$\mathbb{F}_p$ において，$g^{\frac{p-1}{2}}+1=0$, $g^{\frac{p-1}{2}}=-1$ である．よって，$a=g^k$ について，

$$a^{\frac{p-1}{2}}=\left(g^k\right)^{\frac{p-1}{2}}=\left(g^{\frac{p-1}{2}}\right)^k=(-1)^k=\left(\frac{a}{p}\right)$$

が成り立つ．したがって，次の定理を得る．

定理 4.3 (オイラーの規準)**.**

$$a^{\frac{p-1}{2}}=\left(\frac{a}{p}\right).$$

定理 4.4 (平方剰余の第 1 補充法則)**.**

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}=\begin{cases}+1, & p\equiv 1 \pmod 4,\\ -1, & p\equiv 3 \pmod 4.\end{cases}$$

[証明]　オイラーの規準で $a=-1$ とおけばよい．　□

次に，$\left(\frac{2}{p}\right)$ を求めよう．$a=2$ としてオイラーの規準を用いても，$a=-1$ のときと異なり，$2^{\frac{p-1}{2}}$ を簡単に計算できない．フェルマーの小定理の証明を思い出す．

$p=13$, $a=2$ とすると，x が $\mathbb{F}_{13}^{\times}$ の各値を 1 回ずつとるとき，$2x$ も $\mathbb{F}_{13}^{\times}$ の各値を 1 回ずつとる．x が $\mathbb{F}_{13}^{\times}$ の半分の元からなる部分集合 $A=\{1,2,3,4,5,6\}$ をうごくとき，$2x$ は $B=\{2,4,6,8,10,12\}$ をうごく．$A'=\{7,8,9,10,11,12\}$ とおけば，$A\cap B=\{2,4,6\}$ であり，$A'\cap B=\{8,10,12\}$ である．$\mathbb{F}_{13}$ において，$8=13-5=-5$, $10=13-3=-3$, $12=13-1=-1$ であるから，$A'\cap B=\{-5,-3,-1\}$ である．したがって，$\mathbb{F}_{13}$ において，

$$\begin{aligned}(2\cdot 1)(2\cdot 2)(2\cdot\cdots 3)(2\cdot 4)(2\cdot 5)(2\cdot 6)&=2\cdot 4\cdot 6\cdot(-5)\cdot(-3)\cdot(-1),\\ 2^6(1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6)&=(-1)^3(1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6),\\ 2^6&=(-1)^3=-1.\end{aligned}$$

オイラーの規準より，$\left(\frac{2}{13}\right)=2^6=-1$ を得る．

$p=17$, $a=2$ とすると，x が $\mathbb{F}_{17}^{\times}$ の各値を 1 回ずつとるとき，$2x$ も $\mathbb{F}_{17}^{\times}$ の各値を 1 回ずつとる．x が $\mathbb{F}_{17}^{\times}$ の半分の元からなる部分集合 $A=\{1,2,3,4,5,6,7,8\}$ をうごくとき，$2x$ は $B=\{2,4,6,8,10,12,14,16\}$ をうごく．$A'=\{9,10,11,12,13,14,15,16\}$ とおけば，このとき，$A\cap B=\{2,4,6,8\}$ であり，$A'\cap B=\{10,12,14,16\}$ である．$\mathbb{F}_{17}$ において，$10=17-7=-7$, $12=17-5=-5$, $14=17-3=-3$, $16=17-1=-1$ であるから，$A'\cap B=\{-7,-5,-3,-1\}$ である．したがって，$\mathbb{F}_{17}$ において，

$$\begin{aligned}(2\cdot 1)(2\cdot 2)(2\cdot 3)(2\cdot 4)(2\cdot 5)(2\cdot 6)(2\cdot 7)(2\cdot 8)&=2\cdot 4\cdot 6\cdot 8\cdot(-7)\cdot(-5)\cdot(-3)\cdot(-1),\\ 2^8(1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7\cdot 8)&=(-1)^3(1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7\cdot 8),\\ 2^8&=(-1)^4=1.\end{aligned}$$

オイラーの規準より，$\left(\dfrac{2}{17}\right) = 2^8 = 1$ を得る．このような考察を一般化すると，次の結果を得る．

補題 4.5 (ガウスの補題)**.** p を素数，$s = \dfrac{p-1}{2}$ とする．$\mathbb{F}_p^\times$ を次のように s 個の元からなる 2 つの部分集合に分ける．

$$\mathbb{F}_p^\times = A \cup A', \quad A = \{1, 2, \ldots, s\},\ A' = \{s+1, s+2, \ldots, p-1\}.$$

$a \in \mathbb{F}_p^\times$ をとり，$a, 2a, \ldots, sa$ のうちで，A' に属するものの個数を n とすれば，

$$\left(\frac{a}{p}\right) = (-1)^n$$

が成り立つ．

[証明]　$a, 2a, \ldots, sa$ のうちで，A に属するものを，$b_1, b_2, \ldots, b_m$ とし，A' に属するものを $c_1, c_2, \ldots, c_n$ とする．そのとき，

$$\{b_1, b_2, \ldots, b_m\} \cup \{-c_1, -c_2, \ldots, -c_n\} = A$$

である．実際，

$$A' = \{s+1, s+2, \ldots, p-2, p-1\} = \{-s, -(s-1), \ldots, -2, -1\} = \{-x \,|\, x \in A\}$$

であるから，$c_j \in A'$ より，$-c_j \in A$ である．したがって，

$$\{b_1, b_2, \ldots, b_m\} \cup \{-c_1, -c_2, \ldots, -c_n\} \subset A.$$

また，もし，$b_i = -c_j$ とすると，$b_i = ax$, $c_j = ay$, $x, y \in A$ とかける．$ax = -ay$, $a(x+y) = 0$ である．$a \neq 0$ より，$x + y = 0$, $y = -x$ である．$y \in A$, $-x \in A'$ だからこれは矛盾である．ゆえに，

$$\{b_1, b_2, \ldots, b_m\} \cap \{-c_1, -c_2, \ldots, -c_n\} = \emptyset$$

であり，$m + n = s = |A|$ であるから，

$$\{b_1, b_2, \ldots, b_m\} \cup \{p - c_1, p - c_2, \ldots, p - c_n\} = A$$

を得る．したがって，A のすべての元の積をとれば，

$$\begin{aligned} 1 \cdot 2 \cdot \cdots \cdot s &= b_1 \cdots b_m (p - c_1) \cdots (p - c_n) \\ &= b_1 \cdots b_m (-c_1) \cdots (-c_n) \\ &= (-1)^n b_1 \cdots b_m c_1 \cdots c_n \\ &= (-1)^n (a \cdot 1)(a \cdot 2) \cdots (a \cdot s) \\ &= (-1)^n a^s 1(\cdot 2 \cdot \cdots \cdot s). \end{aligned}$$

ゆえに，$(-1)^n a^s = 1$, $a^{\frac{p-1}{2}} = a^s = (-1)^n$. オイラーの規準より，$\mathbb{F}_p$ において，

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} = (-1)^n.$$

□

定理 4.6 (平方剰余の第 2 補充法則)**.**

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1, & p \equiv 1, 7 \pmod 8, \\ -1, & p \equiv 3, 5 \pmod 8. \end{cases}$$

[証明]　補題 4.5 を $a = 2$ について適用する．$s = \dfrac{p-1}{2}$,

$$\mathbb{F}_p^\times = A \cup A', \quad A = \{1, 2, \ldots, s\},\ A' = \{s+1, s+2, \ldots, p-1\}.$$

$2x$ $(x = 1, 2, \ldots, s)$ のうち A' に属するものを $C = \{c_1, \ldots, c_n\}$ とする．$p = 8k+1$ のとき．$s = \dfrac{p-1}{2} = 4k$ である．

$$\{2x \,|\, x = 1, 2, \ldots, s\} = \{2, 4, \ldots, 2(2k)\} \cup \{2(2k+1), 2(2k+2), \ldots, 2(4k)\}$$

より，$n = 4k - 2k = 2k$ である．したがって，$\left(\dfrac{2}{p}\right) = (-1)^{2k} = 1$.

$p = 8k+7$ のとき．$s = \dfrac{p-1}{2} = 4k+3$ である．

$$\{2x \,|\, x = 1, 2, \ldots, s\} = \{2, 4, \ldots, 2(2k+1)\} \cup \{2(2k+2), 2(2k+3), \ldots, 2(4k+3)\}$$

より，$n = 4k+3-(2k+1) = 2k+2$ である．したがって，$\left(\dfrac{2}{p}\right) = (-1)^{2k+2} = 1$.

$p = 8k+3$ のとき．$s = \dfrac{p-1}{2} = 4k+1$ である．

$$\{2x \,|\, x = 1, 2, \ldots, s\} = \{2, 4, \ldots, 2(2k)\} \cup \{2(2k+1), 2(2k+2), \ldots, 2(4k+1)\}$$

より，$n = 4k+1-(2k) = 2k+1$ である．したがって，$\left(\dfrac{2}{p}\right) = (-1)^{2k+1} = -1$.

$p = 8k+5$ のとき．$s = \dfrac{p-1}{2} = 4k+2$ であるから，

$$\{2x \,|\, x = 1, 2, \ldots, s\} = \{2, 4, \ldots, 2(2k+1)\} \cup \{2(2k+2), 2(2k+3), \ldots, 2(4k+2)\}$$

より，$n = 4k+2-(2k+1) = 2k+1$ である．したがって，$\left(\dfrac{2}{p}\right) = (-1)^{2k+1} = -1$. □

4.2 平方剰余の相互法則

定理 4.7 (平方剰余の相互法則). p, q を相異なる奇素数とする．このとき，

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

[証明] $s = \dfrac{p-1}{2}$, $t = \dfrac{q-1}{2}$ とおき，

$$\mathbb{F}_p^\times = A \cup A', \quad A = \{1, 2, \ldots, s\}, \quad A' = \{s+1, s+2, \ldots, 2s\},$$
$$\mathbb{F}_q^\times = B \cup B', \quad B = \{1, 2, \ldots, t\}, \quad B' = \{t+1, t+2, \ldots, 2t\},$$

とおく．また，

$$R = \{(x, y) \in \mathbb{Z}^2 \mid 1 \leq x \leq s,\ 1 \leq y \leq t\}$$

とおく．$q, 2q, \ldots, sq$ のうち，A' に属するものを $\alpha_1, \ldots, \alpha_m$ とすれば，補題 4.5 より，

$$\left(\frac{q}{p}\right) = (-1)^m.$$

同様に，$p, 2p, \ldots, tp$ のうち，B' に属するものを $\beta_1, \ldots, \beta_n$ とすれば，補題 4.5 より，

$$\left(\frac{p}{q}\right) = (-1)^n.$$

いま，各 $i = 1, \ldots, m$ に対して，$a_i, x_i \in \mathbb{Z}$, $1 \leq a_i, x_i \leq s$ で，

$$\alpha_i = qx_i + p\mathbb{Z} = p - a_i + p\mathbb{Z} = -a_i + p\mathbb{Z}$$

となるものが一意的に存在する．そのとき，$a_i + qx_i = py_i$ となる $y_i \in \mathbb{Z}$ が一意的に定まる．$a_i, x_i > 0$ より，$y_i > 0$ である．また，$a_i, x_i \leq s < \dfrac{p}{2}$ より，

$$py_i = a_i + qx_i < \frac{p}{2} + \frac{p}{2}q, \quad y_i < \frac{1}{2} + \frac{q}{2}$$

したがって，$y_i \leq \dfrac{q-1}{2} = t$ である．ゆえに，$1 \leq y_i \leq t$ である．さらに，$a_i = py_i - qx_i$ より，$0 < py_i - qx_i < \dfrac{p}{2}$ である．このようにして，各 $i = 1, \ldots, m$ に対して，格子点 $(x_i, y_i) \in R$ で，$0 < py_i - qx_i < \dfrac{p}{2}$ となるものが対応する．逆に，このような格子点 $(x, y) \in R$ に対して，$a = py - qx$ とおけば，$1 \leq a, x \leq s$ であり，$qx + p\mathbb{Z} = -a + p\mathbb{Z} \in qA \cap A'$ である．したがって，

$$m = \#(qA \cap A') = \#\left\{(x, y) \in R \,\middle|\, 0 < py - qx < \frac{p}{2}\right\}$$

を得る．同様にして，

$$n = \#(pB \cap B') = \#\left\{(x,y) \in R \,\middle|\, 0 < qx - py < \frac{q}{2}\right\}$$

を得る．したがって，

$$\begin{aligned} m + n &= \#\left\{(x,y) \in R \,\middle|\, 0 < py - qx < \frac{p}{2}\right\} \\ &\quad + \#\left\{(x,y) \in R \,\middle|\, 0 < qx - py < \frac{q}{2}\right\} \\ &= \#\left\{(x,y) \in R \,\middle|\, -\frac{q}{2} < py - qx < \frac{p}{2}\right\}. \end{aligned}$$

ここで，

$$\begin{aligned} R_1 &= \left\{(x,y) \in R \,\middle|\, py - qx \geq \frac{p}{2}\right\}, \\ R_2 &= \left\{(x,y) \in R \,\middle|\, py - qx \leq -\frac{q}{2}\right\} \end{aligned}$$

とおけば，

$$m + n + \#R_1 + \#R_2 = \#R = st.$$

さらに，$\#R_1 = \#R_2$ である．実際，

$$F(x,y) = (s + 1 - x, t + 1 - y)$$

とおけば，F は R から R への全単射であり，$F \circ F = id_R$ である．

$$p(t + 1 - y) - q(s + 1 - x) = \frac{p - q}{2} - (py - qx)$$

に注意する．$(x,y) \in R_1$ ならば，$py - qx \geq \frac{p}{2}$,

$$\frac{p - q}{2} - (py - qx) \leq -\frac{q}{2},$$

したがって，$F(x,y) \in R_2$ である．$(x,y) \in R_2$ ならば，$py - qx \leq -\frac{q}{2}$,

$$\frac{p - q}{2} - (py - qx) \geq \frac{p}{2},$$

したがって，$F(x,y) \in R_1$ である．ゆえに，F は R_1 から R_2 への全単射を引き起こし，$\#R_1 = \#R_2$ を得る．よって，

$$m + n + 2\#R_1 = st$$

であり，

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{m+n} = (-1)^{st} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

□

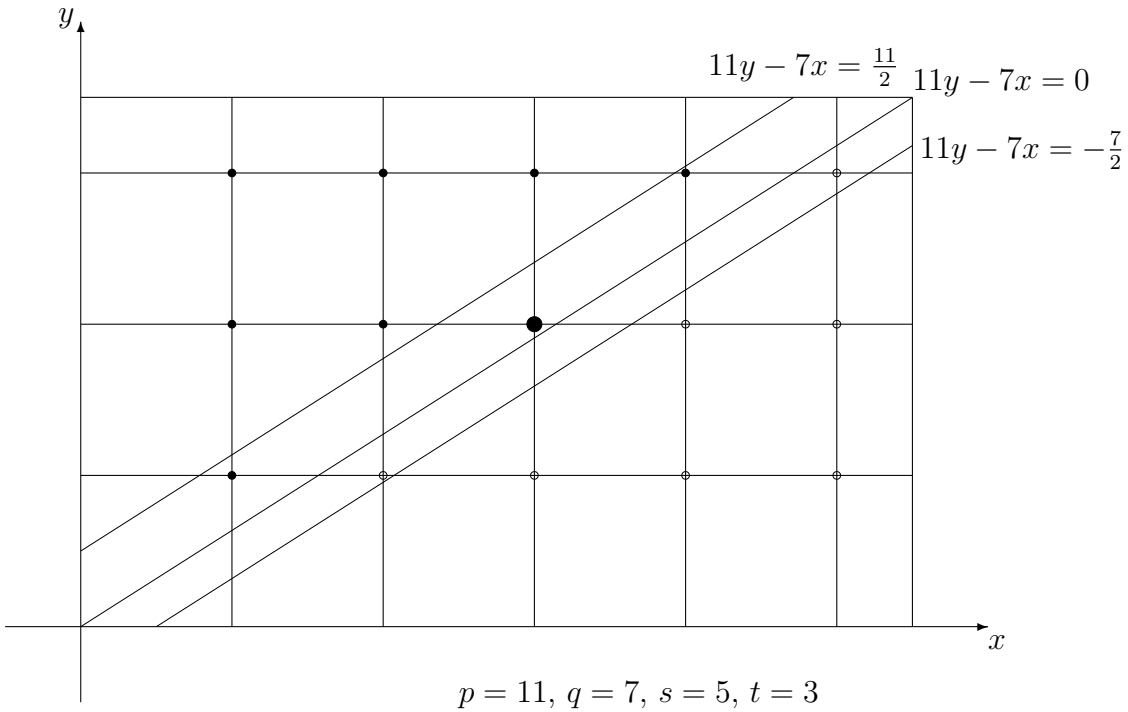

図 1: 平方剰余の相互法則の証明

例 4.8.

$$\left(\frac{5}{43}\right) = (-1)^{\frac{5-1}{2}\frac{43-1}{2}}\left(\frac{43}{5}\right) = \left(\frac{3}{5}\right) = (-1)^{\frac{3-1}{2}\frac{5-1}{2}}\left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

練習問題 6. 次のルジャンドル記号の値を求めよ.

$$\left(\frac{23}{29}\right), \quad \left(\frac{15}{17}\right), \quad \left(\frac{14}{19}\right), \quad \left(\frac{19}{37}\right).$$

$$\begin{aligned}\left(\frac{23}{29}\right) &= (-1)^{\frac{23-1}{2}\cdot\frac{29-1}{2}}\left(\frac{29}{23}\right) = \left(\frac{6}{23}\right)\\ &= \left(\frac{2}{23}\right)\left(\frac{3}{23}\right) = \left(\frac{3}{23}\right)\\ &= (-1)^{\frac{3-1}{2}\cdot\frac{23-1}{2}}\left(\frac{23}{3}\right) = (-1)\left(\frac{2}{3}\right) = 1.\end{aligned}$$

$$\begin{aligned}\left(\frac{15}{17}\right) = \left(\frac{3}{17}\right)\left(\frac{5}{17}\right) &= (-1)^{\frac{3-1}{2}\cdot\frac{17-1}{2}}\left(\frac{17}{3}\right)(-1)^{\frac{5-1}{2}\cdot\frac{17-1}{2}}\left(\frac{17}{5}\right)\\ &= \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1.\end{aligned}$$

$$\left(\frac{15}{17}\right) = \left(\frac{-2}{17}\right) = \left(\frac{-1}{17}\right)\left(\frac{2}{17}\right)$$
$$= (-1)^{\frac{17-1}{2}} = 1$$

$$\left(\frac{14}{19}\right) = \left(\frac{2}{19}\right)\left(\frac{7}{19}\right) = (-1)(-1)^{\frac{7-1}{2}\cdot\frac{19-1}{2}}\left(\frac{19}{7}\right)$$
$$= \left(\frac{5}{7}\right) = (-1)^{\frac{5-1}{2}\cdot\frac{7-1}{2}}\left(\frac{7}{5}\right)$$
$$= \left(\frac{2}{5}\right) = -1.$$

$$\left(\frac{14}{19}\right) = \left(\frac{-5}{19}\right) = \left(\frac{-1}{19}\right)\left(\frac{5}{19}\right)$$
$$= (-1)^{\frac{19-1}{2}}(-1)^{\frac{19-1}{2}\cdot\frac{5-1}{2}}\left(\frac{19}{5}\right)$$
$$= (-1)\left(\frac{4}{5}\right) = (-1)\left(\frac{2}{5}\right)^2 = -1.$$

$$\left(\frac{19}{37}\right) = (-1)^{\frac{19-1}{2}\cdot\frac{37-1}{2}}\left(\frac{37}{19}\right)$$
$$= \left(\frac{18}{19}\right) = \left(\frac{-1}{19}\right) = (-1)^{\frac{19-1}{2}} = -1.$$

$$\left(\frac{19}{37}\right) = (-1)^{\frac{19-1}{2}\cdot\frac{37-1}{2}}\left(\frac{37}{19}\right)$$
$$= \left(\frac{18}{19}\right) = \left(\frac{2}{19}\right)\left(\frac{9}{19}\right)$$
$$= (-1)\left(\frac{3}{19}\right)^2 = -1.$$