1　記号

$\omega = (-1+\sqrt{-3})/2$ とおく．ω は 1 の原始 3 乗根であり，$1+\omega+\omega^2 = 0$ が成り立つ．また $\overline{\omega} = \omega^2$ である．

$R = \mathbb{Z}[\omega]$ とおく．R は素元分解整域である．R の元は $a+b\omega$ $(a,\, b \in \mathbb{Z})$ の形に一意的に書ける．$R^\times$ で R の単数群を表すことにすると

$$R^\times = \{\pm 1,\, \pm\omega,\, \pm\omega^2\}$$

である．

R の元 α, β が同伴であるとは，$\alpha = \beta\varepsilon$ $(\exists\varepsilon \in R^\times)$ と表されるときにいう．同伴は R 上の同値関係である．素元と同伴な元もまた素元になる．

以下，

$$\lambda = 1-\omega$$

とおく．また，R の元 α と素元 π に対して

$$\mathrm{ord}_\pi(\alpha) = \max\{k \in \mathbb{N} \mid \pi^k \text{ は } \alpha \text{ を割る }\}$$

と定義する．

2　$n = 3$ における Fermat の定理

定理 2.1 ($n = 3$ **における Fermat の定理**)**.** 方程式

$$X^3 + Y^3 = Z^3 \tag{1}$$

は，$x \neq 0$, $y \neq 0$, $z \neq 0$ なる有理整数解 $(x,\, y,\, z)$ を持たない．

証明.　$x^3+y^3 = z^3$ となる有理整数 x, y, z で $x \neq 0$, $y \neq 0$, $z \neq 0$ となるものが存在したと仮定する．このとき $\max\{|x|,\, |y|,\, |z|\}$ が最小になるものがとれる．それを改めて x, y, z で表すことにする．このとき

$$x' \neq 0, \qquad y' \neq 0 \qquad z' \neq 0,$$
$$\max\{|x'|,\, |y'|,\, |z'|\} < \max\{|x|,\, |y|,\, |z|\}$$

なる有理整数解 $(x',\, y',\, z')$ が存在することを示して矛盾を導く．

x, y, z はどの 2 つも互いに素である (注意 3.6)．また，y, z が奇数であると仮定することができる (注意 3.7)．

$x^3+y^3 = z^3$ を

$$x^3 = (z-y)(z-\omega y)(z-\overline{\omega}y) \tag{2}$$

と変形する．以下，x が 3 で割り切れる場合とそうでない場合とに分けて証明する．

(I)　x が 3 で割り切れないとき．$c \in \mathbb{Z}$, $\alpha \in R$ が存在して

$$z-y = c^3 \tag{3}$$
$$z-\omega y = \overline{\omega}\alpha^3 \tag{4}$$
$$z-\overline{\omega}y = \omega\overline{\alpha}^3 \tag{5}$$

が成り立つ (注意 3.8).

$\alpha = a + b\omega$ (a, $b \in \mathbb{Z}$) とおく．(4) より

$$y = a^3 - 3ab^2 + b^3, \qquad z = -a^3 + 3a^2b - b^3 \tag{6}$$

したがって

$$z - y = (a + b)(2a - b)(2b - a) \tag{7}$$

となる．よって (3) より

$$c^3 = (a + b)(2a - b)(2b - a)$$

を得る．ここで $a + b$, $2a - b$, $2b - a$ はどの二つも互いに素である (注意 3.9)．ゆえにそれぞれが有理整数の 3 乗になる．そこで

$$a + b = (z')^3, \qquad 2a - b = (x')^3, \qquad 2b - a = (y')^3$$

とおくと

$$(x')^3 + (y')^3 = (z')^3$$

x', y', z' はどの二つも互いに素なので，$x' \neq 0$, $y' \neq 0$, $z' \neq 0$ でなければならない．さらに

$$\max\{|x'|, |y'|, |z'|\} < \max\{|x|, |y|, |z|\}$$

がいえる (注意 3.10)．これは $\max\{|x|, |y|, |z|\}$ が最小であるという仮定に矛盾する．

(II) x が 3 で割り切れるとき．$c \in \mathbb{Z}$, $\alpha \in R$ が存在して

$$z - y = 9c^3 \tag{8}$$

$$z - \omega y = \lambda\alpha^3 \tag{9}$$

$$z - \overline{\omega} y = \overline{\lambda}\overline{\alpha}^3 \tag{10}$$

が成り立つ (注意 3.11).

$\alpha = a + b\omega$ (a, $b \in \mathbb{Z}$) とおく．(9) より

$$y = a^3 - 6a^2b + 3ab^2 + b^3, \qquad z = a^3 + 3a^2b - 6ab^2 + b^3 \tag{11}$$

したがって

$$z - y = 9ab(a - b) \tag{12}$$

となる．よって (8) より

$$c^3 = 9ab(a - b)$$

を得る．ここで a, b, $a - b$ はどの二つも互いに素である (注意 3.12)．ゆえにそれぞれが有理整数の 3 乗になる．そこで

$$a = (z')^3, \qquad b = (x')^3, \qquad a - b = (y')^3$$

とおくと

$$(x')^3 + (y')^3 = (z')^3$$

x', y', z' はどの二つも互いに素なので，$x' \neq 0$, $y' \neq 0$, $z' \neq 0$ でなければならない．さらに

$$\max\{|x'|, |y'|, |z'|\} < \max\{|x|, |y|, |z|\}$$

となる (注意 3.13)．これは矛盾である．

□

3　行間を埋める

この節では，先に述べた $n = 3$ における Fermat の定理の証明において，省略した部分を補うことを目的とする．

補題 3.1.　λ は R の素元である．

証明.　R は素元分解整域であり，λ は単数ではないので，ある素元 π が存在して

$$\lambda = \pi\alpha \ (\exists\alpha \in R)$$

となる．

$$3 = \lambda\overline{\lambda} = \pi\overline{\pi}\alpha\overline{\alpha}, \qquad \pi\overline{\pi},\ \alpha\overline{\alpha} \in \mathbb{Z}, \qquad \pi\overline{\pi} \neq 1$$

であるから

$$\pi\overline{\pi} = 3, \qquad \alpha\overline{\alpha} = 1$$

ゆえに α は単数である．すなわち π と λ とは同伴である．したがって λ は素元である．　□

補題 3.2.　3 と λ^2 とは R において同伴である．

証明.　$3 = -\lambda^2\omega^2$ であり，$-\omega^2$ は R の単数である．　□

補題 3.3.　y, z を互いに素な有理整数とする．R の素元 π が

$$z - y, \qquad z - \omega y, \qquad z - \overline{\omega} y$$

のいずれか二つを割り切れば，π と λ とは同伴である．

証明.　R の素元が，例えば $z - y$ と $z - \omega y$ を割り切れば

$$\lambda y = (z - y) - (z - \omega y)$$

を割る．π が λ と同伴でないとすると，π は y を割り切らなければならない．したがって π は $z = (z - y) + y$ も割り切る．しかしながらこれは y, z が互いに素であることに反する．

$$1 - \overline{\omega} = -(1 - \omega)\omega^2, \qquad \omega - \overline{\omega} = \omega(1 - \omega)$$

に注意すれば，残りの 2 つの場合も同様にして議論することができる．　□

補題 3.4.　剰余環 $R/2R$ は四つの類からなり，

(13)　$$0, \quad 1, \quad \omega, \quad 1 + \omega$$

が完全代表系である．また

$$1^3 \equiv \omega^3 \equiv (1+\omega)^3 \equiv 1 \pmod{2R} \tag{14}$$

$$\pm 1 \equiv 1, \qquad \pm\omega \equiv \omega, \qquad \pm\omega^2 \equiv 1+\omega \pmod{2R} \tag{15}$$

が成り立つ．

証明． R の元はすべて $a+b\omega$ $(a, b \in \mathbb{Z})$ の形で一意的に書ける．よって

$$a+b\omega \equiv c+d\omega \pmod{2R} \Longleftrightarrow a \equiv c,\ b \equiv d \pmod{2R}$$

であることから，(13) が $R/2R$ における完全代表系であることがわかる．
(14) および (15) は $1+\omega+\omega^2=0$ に注意して計算すればわかる． □

補題 3.5. $\alpha_1, \ldots, \alpha_r$ を R の 0 でない元，k を自然数とし，

$$\alpha_1 \cdots \alpha_r = \beta^k \tag{16}$$

とする．さらに $i \neq j$ ならば α_i と α_j とは共通の素元では割れないとする．このとき各 α_i に対して，R の元 β_i と単数 u_i が存在して

$$\alpha_i = u_i \beta_i^k$$

と書ける．

証明． まず R が素元分解整域であることに注意する．π を R の素元とする．π が α_i を割り切るとすると，仮定より $j \neq i$ ならば $\mathrm{ord}_\pi(\alpha_j) = 0$．よって

$$\mathrm{ord}_\pi(\alpha_1 \cdots \alpha_r) = \mathrm{ord}_\pi(\alpha_i)$$

一方，(16) により

$$\mathrm{ord}_\pi(\alpha_i) = k \cdot \mathrm{ord}_\pi(\beta_i)$$

よって R のすべての素元 π に対して $\mathrm{ord}_\pi(\alpha_i)$ は k の倍数になる．ゆえに R の元 β_i と単数 u_i が存在して $\alpha_i = u_i\beta_i^k$ と書ける． □

注意 3.6. x, y, z のどの二つも互いに素であること：例えば，x, y の 2 つを割り切る素数 l が存在したとする．$x^3+y^3=z^3$ により l は z を割る．したがって $(x/l, y/l, z/l)$ も方程式 (1) の有理整数解となる．ところがこれは $\max\{|x|, |y|, |z|\}$ の最小性に反する．

注意 3.7. y, z を奇数と仮定できること：x, y, z はどの二つも互いに素だから，偶数は多くとも一つである．必要に応じて (x, y, z) の代わりに (y, x, z), $(z, -y, x)$ を考えれば，y, z を奇数と仮定することができる．

注意 3.8. 実際,

$$z-y, \qquad z-\omega y, \qquad z-\overline{\omega} y \tag{17}$$

のうち二つを割る素元 π が存在すれば，補題 3.3 により π と λ とは同伴である．補題 3.2 により 3 と λ^2 とは同伴であるから，π^2 と 3 とは同伴である．よって (2) より x^3 が 3 で割れることになり，x が 3 で割り切れてしまう．これは x が 3 で割り切れないという仮定に反する．よって (17) のど

の二つも R の共通の素元で割り切れない．したがって補題 3.5 により (17) の三つの元はそれぞれ R の元を 3 乗したものと同伴である．

$z-y=u\beta^3$ $(u\in R^\times,\ \beta\in R)$ とおくと

$$(z-y)^2=u\beta^3\overline{u}\overline{\beta}^3=(\beta\overline{\beta})^3,\qquad \beta\overline{\beta}\in\mathbb{Z}$$

よって $(z-y)^2$ は有理整数の 3 乗であるが，これは $z-y$ が有理整数の 3 乗であることを意味する．

次に $z-\omega y=v\alpha^3$ $(v\in R^\times,\ \alpha\in R)$ とおく．(4) を示すためには $v=\pm\overline{\omega}$ を示せばよい．$y,\ z$ が奇数であるという仮定を用いれば，

$$v\alpha^3\equiv z-\omega y\equiv 1-\omega\equiv\overline{\omega}\pmod{2R}$$

よって補題 3.4 から $\alpha^3\equiv 1\pmod{2R}$ であって

$$v\equiv\overline{\omega}\pmod{2R}$$

ゆえに $v=\pm\overline{\omega}$ を得る．

(5) は (4) の両辺の共役をとることにより得られる．

注意 3.9. $a+b,\ 2a-b,\ 2b-a$ がどの二つも互いに素であること：仮に素数 l が $a+b,\ 2a-b,\ 2b-a$ のうち二つを割り切るとすると，l は

$$3a=(a+b)+(2a-b)=2(a+b)+(a-2b)=2(2a-b)-(a-2b),$$
$$3b=2(a+b)-(2a-b)=(a+b)-(a-2b)=(2a-b)-2(a-2b)$$

を割る．また l は $z-y$ を割り，その倍数 x^3 を割るから，x を割る．x が 3 で割り切れないという仮定から $l\neq 3$ でなければならない．よって l は $a,\ b$ を割る．(6) より l は $y,\ z$ の両方を割る．これは $y,\ z$ が互いに素であることに反する．

注意 3.10. (2)，(7) より

$$\max\{|x'|^3,\ |y'|^3,\ |z'|^3\}\le|z-y|<|x|^3\le\max\{|x|^3,\ |y|^3,\ |z|^3\}$$

ゆえに

$$\max\{|x'|,\ |y'|,\ |z'|\}<\max\{|x|,\ |y|,\ |z|\}$$

が成り立つ．ここで $|z-y|\neq|x|^3$ は次のようにして示される．もし仮に $|z-y|=|x|^3$ ならば，(2) より

$$|(z-\omega y)(z-\overline{\omega}y)|=1$$

(4)，(5) および $|\omega|=1$ より

$$|\alpha\overline{\alpha}|^3=1\qquad\therefore|\alpha\overline{\alpha}|=1$$

$\alpha=a+b\omega$ とおいたから，計算すると

$$(2a-b)^2+3b^2=4$$

を得る．このとき $(a,\ b)=(1,\ 1)$ または $(1,\ 0)$ でなければならない．前者の場合は $a+b=2$，後者の場合は $2a-b=2$．このことは $a+b,\ 2a-b$ が有理整数の 3 乗であることに反する．

注意 3.11. 実際，x が 3 で割り切れると仮定したから，補題 3.2 より x は λ で割り切れる．また

$$z - y \equiv z - \omega y \equiv z - \overline{\omega} y \pmod{\lambda R}$$

だから，$z-y$, $z-\omega y$, $z-\overline{\omega}y$ のすべてが λ で割り切れる．一方

$$\mathrm{ord}_\lambda(z - \omega y) = \mathrm{ord}_\lambda(z - \overline{\omega} y) = 1 \tag{18}$$

である．なぜなら

$$z - \omega y \in \lambda^2 R \Longleftrightarrow z - \omega y \in 3R \Longleftrightarrow z \equiv y \equiv 0 \,(\mathrm{mod}\, 3\mathbb{Z})$$

z, y が互いに素であることから $z-\omega y \notin \lambda^2 R$ でなければならない．$z-\overline{\omega}y$ についても同様である．

$m = \mathrm{ord}_\lambda(x)$, $n = \mathrm{ord}_\lambda(z-y)$ とおくと，(2)，(18) により

$$3m = n + 1 + 1$$

x は 3 で割れるから補題 3.2 により $m \geq 2$．したがって $n \geq 4$．よって，ある $r \in \mathbb{Z}$, $\xi \in R$ が存在して

$$z - y = 9r, \qquad z - \omega y = \lambda \xi, \qquad z - \overline{\omega} y = \overline{\lambda}\,\overline{\xi}$$

となる．これを (2) に代入すれば，$(x/3)^3 = r\xi\overline{\xi}$ を得る．(18) と補題 3.3 より r, ξ, $\overline{\xi}$ のどの二つも R の共通の素元では割れない．よって補題 3.5 により r, ξ, $\overline{\xi}$ はそれぞれ R の単数と R の元を 3 乗したものとの積である．したがって

$$\begin{aligned} z - y &= 9c^3 \qquad (\exists c \in \mathbb{Z}), \\ z - \omega y &= v\lambda\alpha^3 \qquad (\exists v \in R^\times, \exists \alpha \in R) \end{aligned}$$

となる．あとは $v = \pm 1$ を示せばよい．y, z が奇数であると仮定しているから

$$\lambda \equiv z - \omega y \equiv v\lambda\alpha^3 \pmod{2R}$$

補題 3.4 より $\alpha^3 \equiv \lambda^3 \equiv 1 \,(\mathrm{mod}\, 2R)$，よって $v \equiv 1 \,(\mathrm{mod}\, 2R)$ となり，これより $v = \pm 1$ を得る．

注意 3.12. a, b, $a-b$ がどの二つも互いに素であること：仮に素数 l が a, b, $a-b$ のうち二つを割り切るとすれば，l は a, b を割る．したがって (11) より l は y, z を割る．これは y, z が互いに素であることに反する．

注意 3.13. (2)，(12) より

$$\max\{|x'|^3, |y'|^3, |z'|^3\} < |z-y| \leq |x|^3 \leq \max\{|x|^3, |y|^3, |z|^3\}$$

ゆえに

$$\max\{|x'|, |y'|, |z'|\} < \max\{|x|, |y|, |z|\}$$

が成り立つ．