群論, これはおもしろい; 共立出版社 2013 p43,44,45 訂正

飯高 茂

平成 29 年 1 月 21 日

1 ガウスの定理の証明

$G = \mathbb{Z}_p^*$ とおき, 単位元でない $x = \overline{a}$ をとり a を原始根の候補と考えて $H = \langle x \rangle$ とおく. $r = |H|$ は x の位数であり

$$a^r \equiv 1 \mod p$$

を満たす. p を法とするとき a は方程式

$$X^r \equiv 1 \mod p \tag{1}$$

の解である.

したがって $G = \mathbb{Z}_p^*$ での $\overline{a}, \overline{a}^2, \cdots, \overline{a}^{r-1}, 1$ は方程式 (1) の解であり r 個ある.

p は素数なので $\mathbb{Z}_p$ は体[1] になりこの元を係数にもつ r 次方程式 (1) の解は r 個以下である. すでに解が r 個みつかっているので (1) の解は $\overline{a}, \overline{a}^2, \cdots, \overline{a}^{r-1}, 1$ だけである. この事実が証明のキモである.

1. $G = H$ なら a が原始根になり証明は終わる.
2. $G \neq H$ なら a は原始根にならない. そこで位数が r より大きい元 z の存在を示す. $z = \overline{c}$ となる整数 c を原始根の候補とすればよいからである.

$y \in G \setminus H$ [2] をとり $H' = \langle y \rangle$ を定義する. $s = |H'|$ とおく.

$s > r$ なら 位数が r より大きい元 y がえられたので $z = y$ とすれば良い.

$r \geq s$ の場合を考える. $d = \mathrm{GCD}(r, s)$ とおく.

次の結果を用いる.

補題 1 有限群 G の元 x, y について $xy = yx$ とし x, y の位数をそれぞれ r, s とおき $d = GCD(r, s)$ とする.

$\langle 1 \rangle$ $d = 1$ のとき $z = xy$ の位数は $L = LCM(r, s)$ となる.

[1] 四則計算のできる集合を体, という. 参考 ([?])

[2] 2 つの集合 X, Y について 差集合を $X \setminus Y$ で示す.

$\langle 2 \rangle$ 一般に 自然数 r, s に対し $r = AB, s = CD$ と自然数の積に分解し $LCM(r, s) = AD, GCD(r, s) = BC$, A, D は互いに素にできる.$x_1 = x^B, y_1 = y^C$ とおくとこの位数はそれぞれ A, D なので,*1)* により $x_1 y_1$ の位数は $L = LCM(r, s)$.

これによれば $d = 1$ ならば xy の位数は r と s の最小公倍数 $L = rs$ になる. $rs > r$ なので $z = xy$ とすれば良い.

$x_1 = x^B, y_1 = y^C$ とおくとこの位数はそれぞれ A, D なので,1) により $x_1 y_1$ の位数は L.

3. $L > r$ とすると $x_1 y_1$ の位数は r より大きいから $z = x_1 y_1$ とすれば良い.

4. $L = r$ とすると, $\mathrm{LCM}(r, s) = r$ により $r = sm$ とかけて $d = s$, $y^d = y^s = 1$. ゆえに $r = dr'$ により $y^r = (y^d)^{r'} = 1$. したがって, $y = \overline{b}$ は r 次方程式 (1) の解になるので $b \equiv a^j \bmod p$ となる j があり $y \in H$. これは仮定 ($y \notin H$) に反する. したがってこの場合は起きない.

以上の操作を繰り返せばいつかは, 位数が $p - 1$ の元が見つけられる.

原始根の存在はオイラー (1707–1803) によって予想されていたがガウス (1777–1855) によってはじめて証明された. したがって, 上記の証明がかなり複雑で理解するだけでも困難なのは当然である. 大天才オイラーにしてできなかったのだから.

1.1 補題の証明

i) $d = 1$ のとき z の位数を t とおくと $z^t = 1$. $z^{ts} = 1$,$z^{ts} = (xy)^{ts} = (x)^{ts} = 1$ により $ts \equiv 0 \mod r$. $d = 1$ により,$t \equiv 0 \mod r$. 同様にして $t \equiv 0 \mod s$. よって t は rs の倍数. 一方 $z^{rs} = (xy)^{rs} = y^{rs} = y^{sr} = 1$ により,z の位数は rs.

ii) $d > 1$ のとき A, B, C, D の構成を説明する.r, s を素因子を同じにとった素因数分解を行う. $r = \prod_{j=1}^{w} {p_j}^{e_j}, s = \prod_{j=1}^{w} {p_j}^{f_j}$. 添え字を必要なら付け替えて $e_1 \geq f_1, \cdots, e_{u-1} \geq f_{u-1}, e_u \leq f_u, \cdots, e_w \leq f_w$ とする. $A = \prod_{j=1}^{u} {p_j}^{e_j}, B = \prod_{j=u+1}^{w} {p_j}^{e_j}, C = \prod_{j=1}^{u} {p_j}^{f_j}, D = \prod_{j=u+1}^{w} {p_j}^{f_j}$ とおけばよい.

1.2 $p = 41$ の場合

$p = 41$ の場合に上記のプロセスを実行してみよう. まずは手堅く $a = 2$ から始める. $H_1 = \langle 2 \rangle$ は次の集合になり位数 r は 20.

$$\{2, 4, 8, 16, 32, 23, 5, 10, 20, 40, 39, 37, 33, 25, 9, 18, 36, 31, 21, 1\}.$$

H_1 に属さない 3 をとると

$$H_2 = \langle 3 \rangle = \{3, 9, 27, 40, 38, 32, 14, 1\}.$$

位数 s は 8. $\mathrm{GCD}(r, s) = 4$ なので $z = 2^4 3 \equiv 7$ とおく $H_3 = \langle 7 \rangle$ の位数は 40. したがって 7 は原始根[3]である.

なお, 素数 p を法とするとき 2,3 がともに原始根でなく,3 が $\langle 2 \rangle$ に属さない最小の p は 41 である.

[3] 6 も原始根.