代数学の基本定理

Masato Nakata

Faculty of Science, Kyoto University

Contents

§ 1.1 代数学の基本定理

次の定理は代数学の基本定理と呼ばれ，とても重要なものである．この証明には，主に複素関数論によるものが知られているが，ここでは Galois 理論による代数的なものを紹介する．

Theorem 1.1.1

複素数体は代数閉体である．

以下，実数体を $\mathbb{R}$，複素数体を $\mathbb{C}$ で表す．$\mathbb{C}$ が代数閉体であることを言うには，定義より，次を示せば良い：

- $\mathbb{C}$ 上代数的な任意の元 α に対して，$\alpha \in \mathbb{C}$ である．

ただし，α は $\mathbb{C}$ の十分大きな拡大体（たとえば $\mathbb{C}$ の代数閉包）の中で考えている．$\mathbb{C}(\alpha)$ で $\mathbb{C}$ に α を添加した体を表すとき，$\alpha \in \mathbb{C}$ は $\mathbb{C}(\alpha) = \mathbb{C}$ と同値である．さらに，$\mathbb{C}(\alpha)$ を含むような，$\mathbb{R}$ の有限次 Galois 拡大体 K を一つ取る[*1]．$K = \mathbb{C}$ を示せば，自動的に $\mathbb{C}(\alpha) = \mathbb{C}$ も従う．よって，次を示せば良い：

Theorem 1.1.2

$\mathbb{C}$ を中間体として持つような，$\mathbb{R}$ の任意の有限次 Galois 拡大 $K/\mathbb{C}/\mathbb{R}$ について，その拡大次数 $[K : \mathbb{R}]$ は 2 である．

実際，$\mathbb{C}$ の $\mathbb{R}$ 上拡大次数は $[\mathbb{C} : \mathbb{R}] = 2$ であり，さらに $[K : \mathbb{R}] = [K : \mathbb{C}] \cdot [\mathbb{C} : \mathbb{R}]$ が成り立つから，もし上を示すことができれば $[K : \mathbb{C}] = 1$，すなわち $K = \mathbb{C}$ となる．

さて，**Theorem 1.1.2** の証明に一つだけ解析的な道具を使う．

Lemma 1.1.1

奇数次の $\mathbb{R}$ 上多項式は 1 次式または可約である．

Proof. $f(X) \in \mathbb{R}[X]$ を奇数次の多項式とすると，十分大きな実数 $x \in \mathbb{R}$ について $f(-x) < 0 < f(x)$ が成り立つ．よって，中間値の定理により f の零点 $x_0 \in \mathbb{R}$ が存在する．このとき $f(X)$ は $X - x_0$ を因子に持つから，$f(X)$ の次数が $\geqslant 3$ ならば可約である． □

Corollary 1.1.3

R の奇数次拡大体は $\mathbb{R}$ 自身のみである．

[*1] このような K は，$f(X) \in \mathbb{C}[X]$ を α の（$\mathbb{C}$ 上）最小多項式としたときに $f(X)$ の（$\mathbb{R}$ 上）最小分解体として取れば良い．

Proof. $L \neq \mathbb{R}$ を $\mathbb{R}$ の奇数次拡大体として, 元 $a \in L \backslash \mathbb{R}$ を任意に取る. a の $\mathbb{R}$ 上最小多項式を $f(X) \in \mathbb{R}[X]$ とすれば, その次数は $\mathbb{R}$ に a を添加した体 $\mathbb{R}(a)$ の拡大次数 $[\mathbb{R}(a) : \mathbb{R}]$ と一致する. 一方 $[\mathbb{R}(a) : \mathbb{R}] = [L : \mathbb{R}]/[L : \mathbb{R}(a)]$ が成り立ち，また $[L : \mathbb{R}]$ は奇数であると仮定したから，$[\mathbb{R}(a) : \mathbb{R}]$ も奇数となる．よって **Lemma 1.1.1** より $f(X)$ は 1 次式または可約となるが，いずれの場合も仮定に矛盾する．従って $L = \mathbb{R}$. □

以下，特に断らない限り，群はすべて有限群を指すものとする.

Theorem 1.1.2 の証明のために，次の二つの事実は一旦認めることにする（これらは次節で証明する）:

i)（Sylow の定理）群 G の位数の素因子 p を任意に取り，$|G| = p^e r$（$\gcd(p, r) = 1$）とする．このとき，位数が p^e であるような G の部分群（**p-Sylow 部分群**と呼ぶ）が存在する.

ii) p 群（位数が素数 p の冪であるような群）は指数 p の部分群を持つ.

*Proof of **Theorem 1.1.2**.* 有限次 Galois 拡大 $K/\mathbb{R}$ の Galois 群を $G = \mathrm{Gal}(K/\mathbb{R})$ と置く．G の位数は拡大次数 $[K : \mathbb{R}]$ と等しく，また $[K : \mathbb{R}] = [K : \mathbb{C}] \cdot [\mathbb{C} : \mathbb{R}]$ は $[\mathbb{C} : \mathbb{R}] = 2$ の倍数であるから，$|G|$ は 2 を素因子に持つ．よって i) より 2-Sylow 部分群 $S \leqslant G$ が存在して，$|G|/|S|$ は $|S|$ と互いに素，すなわち奇数となる.

S に対応する中間体 $K/L/\mathbb{R}$ を取る（Galois の基本定理）と，拡大次数について

$$[L : \mathbb{R}] = \frac{[K : \mathbb{R}]}{[K : L]} = \frac{|G|}{|S|}$$

が成り立つ．特に L は $\mathbb{R}$ の奇数次の拡大体であるが，**Corollary 1.1.3** より，これは $[L : \mathbb{R}] = 1$，すなわち $L = \mathbb{R}$ でしかあり得ない．従って $S = G$ となり，G は 2 群（位数が 2 の冪 $|G| = 2^n$）である.

$n \leqslant 1$ ならば良い．$n \geqslant 2$ として矛盾を導こう．中間体 $K/\mathbb{C}/\mathbb{R}$ に対応する G の部分群を $H_0 \leqslant G$ とする．G が 2 群だから H_0 もまた 2 群であり，ii) より指数 2 の部分群 $H \leqslant H_0$ を持つ．これに対応する中間体を $K/C/\mathbb{R}$ とすると，$H \leqslant H_0$ であるから C は $\mathbb{C}$ の拡大体であり，その拡大次数は $[C : \mathbb{C}] = [L : \mathbb{C}]/[L : C] = |H_0|/|H| = 2$ となる．しかし $\mathbb{C}$ の 2 次拡大体は存在しない（**Lemma 1.1.2**）から矛盾する．よって $n \leqslant 1$. □

Lemma 1.1.2

$\mathbb{C}$ の 2 次拡大体は存在しない.

Proof. $K/\mathbb{C}$ を 2 次拡大体とすると，ある 2 次既約多項式 $f(X) \in \mathbb{C}[X]$ が存在して $K \cong \mathbb{C}[X]/(f(X))$ となる．一方，$\mathbb{C}$ 上の 2 次方程式については解の公式が知られていて，2 次式は常に可約である．よって $\mathbb{C}$ の 2 次拡大体は存在しない. □

§ 1.2 有限群論

この節では，前節で認めた二つの事実を証明する．p を素数とする.

1.2.1 冪零群と可解群

有限群論の基本的な概念に，**冪零**と**可解**がある．これらの定義には多くのバリエーションがあり，ここではそのうちの一つを採り上げる．

Definition 1.2.1

群 G が**冪零**（*nilpotent*）であるとは，$G_0 = G$，$G_i = [G_{i-1}, G]$（$i = 1, 2, \ldots$）によって定まる G の正規部分群の列

$$G = G_0 \geqslant G_1 \geqslant G_2 \geqslant \cdots \geqslant G_n \geqslant \cdots$$

が有限回で終わる，すなわち十分大きな n について $G_n = 1$ となることを言う．
また，G が**可解**（*solvable*）[*2]であるとは，$G^{(0)} = G$，$G^{(i)} = [G^{(i-1)}, G^{(i-1)}]$（$i = 1, 2, \ldots$）によって定まる G の部分群の列

$$G = G^{(0)} \trianglerighteq G^{(1)} \trianglerighteq G^{(2)} \trianglerighteq \cdots \trianglerighteq G^{(n)} \trianglerighteq \cdots$$

が有限回で終わることを言う．簡単のため，$G' = G^{(1)}$，$G'' = G^{(2)}$ といった表記をよく用いる．

定義からすぐ分かるように，

Lemma 1.2.1

冪零群は可解である．

Proof. G が冪零群であれば，上の定義のように正規部分群 $G_i \trianglelefteq G$ を定義したとき，十分大きな n に対して $G_n = 1$ となる．任意の $i \geqslant 1$ に対して，もし $G^{(i-1)} \subset G_{i-1}$ ならば $G^{(i)} = [G^{(i-1)}, G^{(i-1)}] \subset [G_{i-1}, G] = G_i$ となるから，結局 $G^{(n)} \subset G_n = 1$ が分かる．よって G は可解． □

あとで示すように p 群は冪零であるから，可解でもある．よって，次の命題から事実 ii) が従う：

Proposition 1.2.1

G が可解群であれば，各 G_{i-1}/G_i が素数位数であるような G の部分群の列

$$G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_n = 1$$

が存在する．

[*2] **可解**という名前の由来は，方程式の可解性にある．そもそも Galois 理論は「5 次以上の方程式が代数的に解ける（方程式が可解である）ための必要十分条件」の研究に端を発することは聞いたことがあると思う．この方程式の解を $\alpha_1, \ldots, \alpha_n$ としたときに，有理数体 $\mathbb{Q}$ にこれらを添加した体拡大 $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)/\mathbb{Q}$ の Galois 群の可解性と，元の方程式の代数的な可解性とが密接に関係する．詳しい議論は本稿の範囲を大きく逸脱するため，省略する．

Corollary 1.2.2

p 群は指数 p の（正規）部分群を持つ．

Proof. G を p 群とすると，上で述べたことにより，これは可解である．よって **Proposition 1.2.1** を使えば，G/G_1 が素数位数であるような正規部分群 $G_1 \trianglelefteq G$ を取れる．G が p 群であるから，G/G_1 もまた p 群でなければならない．よって G/G_1 の位数は p であり，すなわち G_1 の指数は p となる． □

まず **Proposition 1.2.1** を示そう．

Definition 1.2.2

群 G が $1 \leqslant G$ と G 自身以外に正規部分群を持たないとき，G を**単純群**（*simple group*）と呼ぶ．

Lemma 1.2.2

単純可換群は素数位数である．

Proof. G を単純可換群として，その元 $1 \neq g \in G$ を任意に取る．G が可換だから，g によって生成された部分群 $\langle g \rangle \leqslant G$ は G の正規部分群であり，G が単純だから $\langle g \rangle = G$ となる．よって G は g を生成元とする巡回群である．

G の位数を n として，これが合成数 $n = pq$ であるとき，G の非自明な正規部分群 $\langle g^p \rangle$ が存在するが，これは G が単純であることに矛盾する．よって n は素数． □

Proof of ***Proposition 1.2.1***. 任意の部分群 $G' \leqslant H \leqslant G$ に対して，G/H は可換であることに注意する．

G/G' が単純であれば，**Lemma 1.2.2** より素数位数となる．単純でなければ，G/G' の非自明な（正規）部分群が存在する．すなわち，G の部分群 $G' < H < G$ が存在する．このとき G/H は可換群となるが，もし単純でなければ，やはり G の部分群 $H < H_1 < G$ を取れる．以下同様の操作を繰り返せば，G の部分群の列

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_n = G'$$

であって，各 G_{i-1}/G_i が単純可換群であるものを取れる．**Lemma 1.2.2** より，各 G_{i-1}/G_i はすべて素数位数である． □

さて，p 群が冪零であることを証明しよう．冪零群の定義として，次のものが使いやすい：

Proposition 1.2.3

群 $G = G_0$ から出発して，$G_i = G_{i-1}/Z(G_{i-1})$ という群の列 $G_0, G_1, \dots$ を作るとき，もし十分大きな n に対して $G_n = 1$ となるならば G は冪零である．

Proof. n に関する帰納法で証明する．$n=1$ のときは $G=Z(G)$，つまり G が可換群であることを意味するから，冪零である．

$n\geqslant 2$ のとき $n-1$ までを仮定すると，G_1 が冪零群となる．すると，次の **Lemma 1.2.3** によって G も冪零となる． □

Lemma 1.2.3

群 G について，$G/Z(G)$ が冪零群のとき G もまた冪零群となる．

Proof. $G/Z(G)$ を冪零群として，G の正規部分群の列

$$G=G_0\geqslant G_1\geqslant\cdots\geqslant G_n\geqslant\cdots,\quad G_i=[G_{i-1},G]$$

を考える．これを自然な全射 $G\twoheadrightarrow G/Z(G)$ で送ることで，$G/Z(G)$ の正規部分群の列

$$G/Z(G)=Z_0\geqslant Z_1\geqslant\cdots\geqslant Z_n\geqslant\cdots,\quad Z_i=G_iZ(G)/Z(G)$$

を得る．準同型は交換子を保つから，$Z_i=[Z_{i-1},Z_0]$ が成り立ち，十分大きな n に対して $Z_n=1$ となる．これは G_n が準同型 $G\twoheadrightarrow G/Z(G)$ の核に含まれること，すなわち $G_n\leqslant Z(G)$ を意味する．すると $[G_n,G]\leqslant[Z(G),G]=1$ となるから，G は冪零． □

1.2.2 群作用と p 群

群 G が有限集合 X に右から作用している状況を考える：$X\curvearrowleft G$．元 $g\in G$ の X への作用を $x\mapsto x^g$ と表す．$x\in X$ の G 軌道を x^G，固定化群を $G_x=\{g\in G\mid x^g=x\}$，$S\subset G$ の固定点の集合を $C_X(S)=\{x\in X\mid S\subset G_x\}$ と書く．

Lemma 1.2.4

任意の元 $x\in X$ に対して，$|x^G|=[G:G_x]$.

Proof.

$$x^g=x^h\iff gh^{-1}\in G_x\iff G_xg=G_xh\quad(x\in X,\ g,h\in G).$$

□

Lemma 1.2.5

$|G:G_x|$（$x\in X$）の公約数は $|X|$ の約数でもある．

Proof. X は軌道の非交叉和となっているから，**Lemma 1.2.4** から従う． □

Lemma 1.2.6

G が p 群ならば，$|X| \equiv |C_X(G)| \pmod p$．

Proof. $Y := X \setminus C_X(G)$ とおくと，G は自然に Y へ作用する．任意の元 $y \in Y$ に対して $G_y < G$ だから，$[G : G_y] \neq 1$ となる．さらに G が p 群だから $[G : G_y]$ は p の倍数．よって **Lemma 1.2.5** より $|Y|$ も p の倍数で，$|X| = |Y| + |C_X(G)| \equiv |C_X(G)|$． □

Lemma 1.2.7

$G \neq 1$ を p 群，$1 \neq N \trianglelefteq G$ をその正規部分群とする．このとき $Z(G) \cap N \neq 1$ となる．特に $N = G$ と取れば $Z(G) \neq 1$．

Proof. $X := N \curvearrowleft G$ を共役作用とする．**Lemma 1.2.6** より $|C_X(G)| \equiv |X| \pmod p$ となるが，N も p 群であるから $|X| \equiv 0$ である．よって $|C_X(G)|$ は p の倍数となる．

一方で $1 \in C_X(G)$ だから $|C_X(G)| \neq 0$ となり，p の倍数でもあるから $|C_X(G)| \geqslant 2$．さらに定義より $C_X(G) = Z(G) \cap N$ だから $Z(G) \cap N \neq 1$． □

Theorem 1.2.4

p 群は冪零である．

Proof. G を p 群として，群 $G_0, G_1, \ldots$ を $G_0 = G$，$G_i = G_{i-1}/Z(G_{i-1})$ によって帰納的に定義する．G が p 群だから，各 G_i もまた p 群である．よって **Lemma 1.2.7** より，十分大きな n に対して $G_n = 1$ となる．すると **Proposition 1.2.3** から G の冪零性が従う． □

1.2.3 Sylow の定理

以上で事実 ii) を証明できた．次は i) について見ていこう．

Definition 1.2.3

群 G の部分群のうち，p 群でもあるものを G の p **部分群**（*p-subgroup*）と呼ぶ．G の p 部分群のうちで極大なものを p-**Sylow 部分群**（*p-Sylow subgroup*）と呼び，その全体を $\mathrm{Syl}_p(G)$ と書く．

Proposition 1.2.5

任意の群において，p-Sylow 部分群は存在する．

Proof. 群 G の p 部分群全体のなす族を $\mathcal{P}$ と置くと，これは単位群 $1 \leqslant G$ を含むから空でない．さらに $\mathcal{P}$ は有限集合であるから，極大元 $P \in \mathcal{P}$ を持つ．（$P_0 = 1 \in \mathcal{P}$ から出発して，$P_{i-1} < P_i \in \mathcal{P}$ なる P_i を繰り返し取っていけば良い．$\mathcal{P}$ が有限集合だからこの繰り返しは有限回で終わる．） □

Sylow 部分群を考えるにあたって，重要な役割を果たすのが p **核**と呼ばれるものである．

Definition 1.2.4

群 G の p-Sylow 部分群すべての共通部分 $\mathcal{O}_p(G) \coloneqq \bigcap_{P \in \mathrm{Syl}_p(G)} P$ を G の p **核**（*p-core*）と呼ぶ．

Proposition 1.2.6

群の p 核は最大の正規 p 部分群である．

Proof. 群 G の p 核を $O \coloneqq \mathcal{O}_p(G)$ と置く．

これが G の p 部分群であることは明らか．また，G 上の自己同型によって p-Sylow 部分群は p-Sylow 群へ移るから，特に内部自己同型を考えれば，O の正規性が従う[*3]．

次に G の正規 p 部分群 $N \trianglelefteq G$ と p-Sylow 部分群 $P \in \mathrm{Syl}_p(G)$ を任意に取る．$P = NP$ を言えば良い．実際，このとき $N \leqslant P$ となり，P は任意であったから $N \leqslant O$ が従う．

$P \leqslant NP$ は明らか．逆の包含関係を示す．次の **Lemma 1.2.8** より $|NP|$ は $|N \times P| = |N| \times |P|$ の約数であり，N と P はともに p 部分群だから NP もまた p 部分群となる．すると，p-Sylow 部分群の極大性により，$P = NP$ となる． □

Lemma 1.2.8

$H_1, H_2 \leqslant G$ を群 G の部分群とすれば，

$$|H_1 H_2| = \frac{|H_1 \times H_2|}{|H_1 \cap H_2|}.$$

特に，$|H_1 H_2|$ は $|H_1 \times H_2|$ の約数となる．

[*3] G の自己同型群 $\mathrm{Aut}(G)$ は集合 $\mathrm{Syl}_p(G)$ へ作用している．このことから，O は $\mathrm{Aut}(G)$ の各元の下で不変に保たれることが分かる．すなわち，任意の元 $g \in G$ と自己同型 $\sigma \in \mathrm{Aut}(G)$ に対して，$g \in O$ ならば $g^\sigma \in O$ が成り立つ．

Proof. 直積集合 $H_1 \times H_2$ 上の同値関係 $\sim$ を

$$(a,b) \sim (c,d) \overset{\text{def}}{\Longleftrightarrow} ab = cd$$

で定義すれば，$|H_1 H_2|$ は同値類の個数に等しい．また，各 $(a,b) \in H_1 \times H_2$ の同値類はちょうど $|H_1 \cap H_2|$ 個の元を含むから，主張が従う． $\square$

COROLLARY 1.2.7

群 G が正規 p-Sylow 部分群 $P \in \mathrm{Syl}_p(G)$ を持てば，$\mathrm{Syl}_p(G) = \{P\}$ となる．逆に，$\mathrm{Syl}_p(G) = \{P\}$ であれば P は G の正規部分群となる．

Proof. もしある p-Sylow 部分群 $P \in \mathrm{Syl}_p(G)$ が正規であれば，**PROPOSITION 1.2.6** より $P \leqslant \mathcal{O}_p(G)$ が成り立つ．一方 p 核の定義から $P \geqslant \mathcal{O}_p(G)$ であるから，$P = \mathcal{O}_p(G)$，すなわち $\mathrm{Syl}_p(G) = \{P\}$ が従う．

逆は **PROPOSITION 1.2.6** から分かる． $\square$

続いて，古典的に知られた次の定理を考える：

THEOREM 1.2.8 （Cauchy の定理）

群 G の位数が p の倍数であれば，G は位数 p の元を持つ．

Proof. 集合 X を

$$X = \{(x_1, \ldots, x_p) \mid x_1 \cdots x_p = 1,\ x_i \in G\ (1 \leqslant i \leqslant p)\}$$

で定義すると，p 次巡回群 $\mathbb{Z}_p$ は X へ作用する：

$$(x_1, \ldots, x_p) \mapsto (x_2, \ldots, x_p, x_1).$$

実際，

$$x_1 \cdots x_p = 1 \Longleftrightarrow x_2 \cdots x_p = x_1^{-1} \Longleftrightarrow x_2 \cdots x_p x_1 = 1.$$

この作用に **LEMMA 1.2.6** を適用すれば，$|X| \equiv |C_X(\mathbb{Z}_p)|$（$\bmod p$）を得る．一方仮定により $|X| = |G|^{p-1}$ は p の倍数であるから，$|C_X(\mathbb{Z}_p)| \equiv 0$ となる．ここで $(1, \ldots, 1) \in C_X(\mathbb{Z}_p)$ だから $|C_X(\mathbb{Z}_p)| \neq 0$，特に $\geqslant 2$ となる．従ってある $(1, \ldots, 1) \neq (x_1, \ldots, x_p) \in C_X(\mathbb{Z}_p)$ が存在するが，これは $x_1 = \cdots = x_p \neq 1$ かつ $x_1^p = 1$ を意味する． $\square$

COROLLARY 1.2.9

群 G について，$\mathrm{Syl}_p(G) = \{P\}$ ならば p は $[G:P]$ の約数でない．

Proof. $\mathrm{Syl}_p(G) = \{P\}$ とすれば，**COROLLARY 1.2.7** の後半によって，P は G の正規部分群となる．そこでもし p が $[G : P]$ の約数であれば，**THEOREM 1.2.8** より位数 p の元 $gP \in G/P$ が存在する．一方このとき $\langle g \rangle P$ は G の p 部分群であるから，p-Sylow 部分群の極大性から $\langle g \rangle P = P$，すなわち $g \in P$ となり矛盾する．（$\langle g \rangle$ は g によって生成される部分群を表す．）よって p は $[G : P]$ の約数ではない． □

最後に，有限群論において最も重要な定理の一つである Sylow の定理を証明する．ただし，本来の Sylow の定理はもっと強い主張を含むが，ここでは事実 i) に相当する部分だけを述べる．定理の他の部分に関しても，証明中の $\mathrm{Syl}_p(N) = \{P\}$，$[N : P] \not\equiv 0$ および $[G : N] \equiv 1$ という関係からすぐに従う．

THEOREM 1.2.10 （Sylow の定理）

> 群 G の位数が $|G| = p^e r$（$\gcd(p, r) = 1$）という形に書けたとする．このとき，G の p-Sylow 部分群の位数は p^e である．

Proof. G の p-Sylow 部分群 $P \in \mathrm{Syl}_p(G)$ を任意に取り，その正規化部分群 $N = N_G(P) = \{g \in G \mid g^{-1}Pg = P\}$ を考える．$P \trianglelefteq N$ であるから，**COROLLARY 1.2.7** と **COROLLARY 1.2.9** より，$\mathrm{Syl}_p(N) = \{P\}$ かつ $[N : P] \not\equiv 0$（$\bmod p$）が分かる．（P は N の p-Sylow 部分群であることに注意する．）

残りは $[G : N] \equiv 1$（$\bmod p$）を示せば良い．実際，$|G| = [G : N] \cdot [N : P] \cdot |P|$ であるから，$[G : N], [N : P] \not\equiv 0$ ならば $|P| = p^e$ となる．

P を次の集合 X へ右から作用させる：

$$X = \{Ng \mid g \in G\} \curvearrowleft P.$$

このとき $|X| = [G : N]$ であり，**LEMMA 1.2.6** を使うと $[G : N] = |X| \equiv |C_X(P)|$ を得る．$C_X(P) = \{N\}$ を示そう．P は N の部分群だから $N \in C_X(P)$ は明らかである．逆の包含関係を見るために，$Ng \in C_X(P)$ とする．これは $NgP = Ng$，すなわち $gPg^{-1} \leqslant N$ を意味する．脚注 [*3] で述べたように gPg^{-1} もまた p-Sylow 部分群であるから，$\mathrm{Syl}_p(N) = \{P\}$ より $gPg^{-1} = P$ を得る．これは $g \in N$ に他ならない．よって $C_X(P) = \{N\}$ となり，$[G : N] \equiv 1$（$\bmod p$）が言えた． □

§ 1.3 Galois 理論の基本定理