

Nielsen-Schreier の定理と選択公理

alg-d

<http://alg-d.com/math/ac/>

2016 年 1 月 17 日

命題 (Nielsen-Schreier の定理). 自由群の部分群は自由群である.

Nielsen-Schreier の定理は ZF で証明できない. (Nielsen-Schreier の定理から「有限集合の族についての選択公理」が導かれることが知られている. また, Nielsen-Schreier の定理が選択公理を導くかどうかは未解決問題のようだ.) 一方, Nielsen-Schreier の定理に条件を付け加えると選択公理と同値になることが知られている. ここではそれを証明する.

G を集合 X で生成される自由群とする. 部分集合 $A \subset G$ に対して $A^{-1} := \{a^{-1} \mid a \in A\}$ として $A^{\pm 1} := A \cup A^{-1}$ とする. 任意の $g \in G$ は $z_1, \dots, z_n \in X^{\pm 1}$ を使って

$$g = z_1 \cdots z_n \quad (z_1 z_2 \neq e, \dots, z_{n-1} z_n \neq e)$$

と一意に書ける. そこで, この表示に現れる非負整数 n を z の長さといい $L(z)$ で表す.

定義. G を集合 X で生成される自由群とし, $A \subset G$ を部分集合とする.

1. A で生成される G の部分群を $\langle A \rangle$ と書く.
2. 以下の条件を満たす A をレベル (level) という.
 - $\langle A \rangle$ は A で生成される自由群である.
 - 任意の $b \in \langle A \rangle$ に対し $b \in \langle \{a \in A \mid L(a) \leq L(b)\} \rangle$ である.
3. 以下の条件を満たす A を Nielsen 集合という.
 - $A \cap A^{-1} = \emptyset$.
 - $a, b \in A^{\pm 1}$ が $L(ab) < L(a)$ を満たせば $ab = e$ である.
 - $a, b, c \in A^{\pm 1}$ が $L(abc) \leq L(a) - L(b) + L(c)$ を満たせば $ab = e$ または $bc = e$ である.

補題. Nielsen 集合はレベルである.

証明. 略 ([3] を参照). □

定理. 次の命題は (ZF 上) 同値.

1. 選択公理
2. G を集合 X で生成される自由群とする. 任意の部分群 $H \subset G$ は, ある Nielsen 集合 $A \subset G$ で生成される自由群になる.
3. G を集合 X で生成される自由群とする. 任意の部分群 $H \subset G$ は, あるレベル $A \subset G$ で生成される自由群になる.

証明. (1 \implies 2) 選択公理により X に整列順序を入れて, G に辞書式順序 \triangleleft を入れる ($^{-1}$ は濁点のように扱って順序を決める). G に整列順序 \leq を以下のように定める.

$g \in G$ とする. $L(g) = 2n$ とすると $g = st^{-1}$, $s, t \in G$, $L(s) = L(t) = n$ と書ける. s, t のうち (\triangleleft で) 小さい方を g の前半, 大きい方を g の後半と呼ぶ. $L(g) = 2n + 1$ の場合は $g = sct^{-1}$, $s, t \in G$, $c \in X^{\pm 1}$, $L(s) = L(t) = n$ と書ける. s, t のうち (\triangleleft で) 小さい方を g の前半, 大きい方を g の後半と呼び, c を g の中央と呼ぶ. $g, h \in G$, $g \neq h$ に対しての順序 \leq を

- まず長さを比較し, $L(g) < L(h)$ ならば $g < h$ とする.
- 長さが一致した場合は前半を比較し, (g の前半) \triangleleft (h の前半) ならば $g < h$ とする.
- 前半も一致した場合は後半を比較し, (g の後半) \triangleleft (h の後半) ならば $g < h$ とする.
- 後半も一致した場合, 長さが奇数の場合は中央を比較し, (g の中央) \triangleleft (h の中央) ならば $g < h$ とする.
- 以上に当てはまらない場合は $g = h^{-1}$ である. $g = st^{-1}$ もしくは $g = sct^{-1}$ と書いたときに, s が前半ならば $g < h$, t が前半ならば $h < g$ とする.

により定める. \leq により G は整列順序集合となる.

$g, h \in G$ が $s, t, u \in G$ により $g = st^{-1}$, $h = su^{-1}$, $L(s) = L(t) = L(u) = \frac{1}{2}L(g) = \frac{1}{2}L(h)$ と書けているとする. このとき $st^{-1} < su^{-1}$ ならば $t \triangleleft u$ である.

∴) まず $s \triangleleft t$ とする. $u \triangleleft s$ とすると $st^{-1} < su^{-1}$ の定義より $s \triangleleft u$ となり矛盾するから $s \triangleleft u$ である. このとき $st^{-1} < su^{-1}$ の定義より $t \triangleleft u$ である.

次に $t \triangleleft s$ とする. $u \triangleleft s$ とすると $st^{-1} < su^{-1}$ の定義より $t \triangleleft u$ である. $s \triangleleft u$ の場合は $st^{-1} < su^{-1}$ の定義より $t \triangleleft s$ となり, $t \triangleleft s \triangleleft u$ である.

定義から明らかに, $st^{-1} < us^{-1}$ などの場合も同様のことが成り立つ.

$\Gamma(H)$ を Hartogs 数として, H に含まれない元 ∞ を一つ取る. 写像 $f: \Gamma(H) \rightarrow H \cup \{\infty\}$ を

$$f(\alpha) := \begin{cases} \min(H \setminus K_\alpha) & (H \setminus K_\alpha \neq \emptyset \text{ のとき}) \\ \infty & (\text{それ以外の場合}) \end{cases}$$

(ただし $K_\alpha := \langle \{f(\xi) \mid \xi < \alpha\} \rangle$ とする.)

により定めて $\lambda := \min\{\alpha \in \Gamma(H) \mid f(\alpha) = \infty\}$ として $A := \{f(\alpha) \mid \alpha < \lambda\} \subset H$ と置く. 定義から明らかに $H = \langle A \rangle$ だから, A が Nielsen 集合であることを示せばよい.

まず明らかに $A \cap A^{-1} = \emptyset$ である.

次に $a, b \in A^{\pm 1}$ が $L(ab) < L(a)$ を満たすとする. $\alpha, \beta < \lambda$, $\varepsilon, \delta \in \{\pm 1\}$ を使って $a = f(\alpha)^\varepsilon$, $b = f(\beta)^\delta$ と書ける. $\alpha < \beta$ と仮定する. $L(ab) < L(a)$ だから $ab < a$ であり, $a = \min(H \setminus K_\alpha)$ だから $ab \in K_\alpha$ となる. よって $b = a^{-1}(ab) \in K_{\alpha+1}$ となって $b = \min(H \setminus K_\beta)$ に矛盾する. 故に $\alpha \geq \beta$ である. 同様に $\alpha \leq \beta$ も分かり, $\alpha = \beta$ となる. よって $L(ab) < L(a)$ となるには $ab = e$ でなければならない.

最後に $a, b, c \in A^{\pm 1}$ が $L(abc) \leq L(a) - L(b) + L(c)$ を満たすとする. $ab \neq e$, $bc \neq e$ と仮定する. $\alpha, \beta, \gamma < \lambda$, $\varepsilon, \delta, \eta \in \{\pm 1\}$ を使って $a = f(\alpha)^\varepsilon$, $b = f(\beta)^\delta$, $c = f(\gamma)^\eta$ と書ける.

$L(abc) \leq L(a) - L(b) + L(c)$ となるには積 abc において b が全てキャンセルしなければならない. また $ab \neq e$ だから $L(ab) \geq L(a)$ であり, よって積 ab で b がキャンセルされるのは半分以下である. 同様に積 bc で b がキャンセルされるのも半分以下である. 従って $a = st^{-1}$, $b = tu^{-1}$, $c = uv^{-1}$, $L(t) = L(u) = \frac{1}{2}L(b)$ と書けることが分かる.

$\alpha < \beta$ とすると $t \triangleleft u$ である.

$\therefore \alpha < \beta$ とする. $ab \in K_\beta$ とすると $b = a^{-1}(ab) \in K_\beta$ となり $b = \min(H \setminus K_\beta)$ に矛盾する. 故に $ab \notin K_\beta$ である. よって $b = \min(H \setminus K_\beta)$ により $b < ab$ でなければならない.

$L(s) = L(t)(= L(u))$ である.

$\therefore \alpha < \beta$ だから $a < b$ であり, よって $L(st^{-1}) = L(a) \leq L(b) = L(tu^{-1})$ となる. よって $L(s) \leq L(u) = L(t)$ である. 一方 $b < ab$ だから $L(tu^{-1}) = L(b) \leq L(ab) = L(su^{-1})$ より $L(t) \leq L(s)$ となる.

よって $tu^{-1} = b < ab = su^{-1}$ より $t \triangleleft s$ となる.

$u \triangleleft t$ と仮定すると $st^{-1} = a < b = tu^{-1}$ の定義から $t \triangleleft u$ となり矛盾するから,

$t \triangleleft u$ である。

$\beta < \alpha$ としても $t \triangleleft u$ である。

$\therefore \beta < \alpha$ とする。 $b < a$ だから $L(tu^{-1}) = L(b) \leq L(a) = L(st^{-1})$ である。従って $L(u) \leq L(s)$ となる。

$ab \in K_\alpha$ と仮定すると $a = (ab)b^{-1} \in K_\alpha$ となり $a = f(\alpha) = \min(H \setminus K_\alpha)$ に矛盾する。故に $ab \notin K_\alpha$ である。よって $a = \min(H \setminus K_\alpha)$ により $a < ab$ でなければならない。 $L(a) = L(st^{-1}) = L(su^{-1}) = L(ab)$ で $L(t) = L(u) \leq L(s)$ だから、 $a < ab$ の定義より $t \triangleleft u$ が分かる。

以上により $t \triangleleft u$ であることが分かる。同様の議論を β, γ に対しても行う。まず $\gamma < \beta$ とすると $u \triangleleft t$ である。

$\therefore \gamma < \beta$ とすると $bc \notin K_\beta$ で、 $b < bc$ となる。また $L(u) = L(v)$ である。

$\therefore \gamma < \beta$ だから $c < b$ であり、よって $L(uv^{-1}) = L(c) \leq L(b) = L(tu^{-1})$ だから $L(v) \leq L(t) = L(u)$ である。一方 $b < bc$ だから $L(tu^{-1}) = L(b) \leq L(bc) = L(tv^{-1})$ より $L(u) \leq L(v)$ となる。

よって $tu^{-1} = b < bc = tv^{-1}$ より $u \triangleleft v$ が分かる。一方 $uv^{-1} = c < b = tu^{-1}$ より $v \triangleleft t$ が分かるから $u \triangleleft t$ である。

$\beta < \gamma$ としても $u \triangleleft t$ である。

$\therefore \beta < \gamma$ とすると $bc \notin K_\gamma$ で $c < bc$ が分かる。 $L(c) = L(uv^{-1}) = L(tv^{-1}) = L(bc)$ だから、 $c < bc$ の定義より $u \triangleleft t$ である。

故に $u \triangleleft t$ かつ $t \triangleleft u$ となり矛盾し、 $ab = e$ または $bc = e$ が分かった。

以上により A は Nielsen 集合である。

(2 \implies 3) 補題により明らか。

(3 \implies 1) $\{X_\lambda\}_{\lambda \in \Lambda}$ を互いに素な非空集合の族とする。 $\Lambda \cap \bigcup_{\lambda \in \Lambda} X_\lambda = \emptyset$ としてよい。 $X := \Lambda \cup \bigcup_{\lambda \in \Lambda} X_\lambda$ で生成される自由群を G とする。 $H \subset G$ を $\{x\lambda^3 \mid \lambda \in \Lambda, x \in X_\lambda\}$ で生成される部分群とすると、仮定 3 により H はあるレベル $A \subset G$ で生成される自由群である。

$\lambda \in \Lambda$ とする。ある $x \in X_\lambda$ が一意に存在して $x\lambda^3 \in A^{\pm 1}$ となる。

\therefore まず存在を示す。 $X_\lambda \neq \emptyset$ だから、元 $y \in X_\lambda$ が取れる。 $y\lambda^3 \in H = \langle A \rangle$ で、

A はレベルだから $y\lambda^3 \in \{a \in A \mid L(a) \leq 4\}$ となる。故に $L(a_0) \leq 4$ なる $a_0 \in A \cup A^{-1}$ で λ が現れるようなものが存在する。 H は長さが偶数の元で生成されているから、 a_0 の長さも偶数である。 よって $L(a_0) = 2$ または $L(a_0) = 4$ 。 H の生成の仕方から、 λ が現れるときには 3 つ同時に現れなければならないから、 $L(a_0) = 4$ が分かる。 H の生成の仕方から、 ある $x \in X_\lambda$ も a_0 に現れなければならない。 従って $a_0 = x\lambda^3$, $a_0 = \lambda x\lambda^2$, $a_0 = \lambda^2 x\lambda$, $a_0 = \lambda^3 x$ の 4 通りのうちのどれかである。 しかし H の生成の仕方から $a_0 = x\lambda^3$ 以外はありえない。 故に $x\lambda^3 = a_0 \in A^{\pm 1}$ となる。

次に一意性を示す。 その為に $x, y \in X_\lambda$, $x \neq y$, $x\lambda^3, y\lambda^3 \in A^{\pm 1}$ と仮定する。 $xy^{-1} = (x\lambda^3)(y\lambda^3)^{-1} \in H = \langle A \rangle$ であり、 A はレベルだから $xy^{-1} \in \{a \in A \mid L(a) \leq L(xy^{-1})\}$ となる。 しかし $L(xy^{-1}) = 2$ だから $x\lambda^3, y\lambda^3 \notin \{a \in A \mid L(a) \leq L(xy^{-1})\}$ となり矛盾。

そこで $f(\lambda) := (x\lambda^3 \in A \cup A^{-1}$ となる唯一つの $x \in X_\lambda$) と定めれば f が選択関数である。 □

参考文献

- [1] Paul E. Howard, Subgroups of a Free Group and the Axiom of Choice, The Journal of Symbolic Logic, Vol. 50, No. 2 (1985), 458–467, <http://www.jstor.org/pss/2274234>
- [2] Paul E. Howard, the Existence of Level Sets in a Free Group implies the Axiom of Choice, Mathematical Logic Quarterly 33(1987), pp315–316, <http://onlinelibrary.wiley.com/doi/10.1002/malq.19870330406/abstract>
- [3] H. Federer and B. Jónsson, Some Properties of Free Groups, Trans. Amer. Math. Soc. 68 (1950), 1–27, <http://www.ams.org/journals/tran/1950-068-01/S0002-9947-1950-0032643-4/>