The Subgroup Theorem

By

Robert Kubota

We give a simplified proof of a theorem of Federer and Jónsson [1], which contains Nielsen's theorem, that every subgroup of a free group is free.

Theorem. *Let F be a free group with basis X, and, for $a \in F$, let $|a|$ be the length of a relative to X. Let G be a subgroup of F, well ordered by a relation $\prec$ such that $|a| < |b|$ implies $a \prec b$. For $a \in G$, let $G_a = \text{gp}\,\{b \in G \,|\, b \prec a\}$. Let $A = \{a \in G \,|\, a \notin G_a\}$. Then G is free on the basis A.*

We prove that A generates G. Suppose not. Let c be the least member of $G - \text{gp}\,A$. Then $c \notin A$, whence $c \in G_c$. But G_c is generated by elements $b \prec c$ which, by the minimality of c, lie in $\text{gp}\,A$, whence $G_c \subseteqq \text{gp}\,A$. This implies that $c \in \text{gp}\,A$, a contradiction.

We prove that A is a free basis for G. Suppose not. Then there is a relation $u_1 \cdots u_n = 1$ where $n \geqq 1$, $u_i^{\pm 1} \in A$, and $u_i \neq u_{i+1}^{-1}$. Let a be maximal among the $u_i^{\pm 1} \in A$. We may suppose our relation chosen such that a is minimal, and hence such that $A_a = \{b \in A \,|\, b \prec a\}$ is a basis for a free group. Note that, for $1 \leqq i \leqq n$, either $u_i = a^{\pm 1}$ or $u_i \in G_a$, and in either case $|u_i| \leqq |a|$.

The sequence $u_1, \ldots, u_n$ satisfies the following conditions:

(1) *For* $1 \leqq i \leqq n-1$, $u_i \neq u_{i+1}^{-1}$.

(2) *For* $1 \leqq i \leqq n$, $0 < |u_i| \leqq |a|$.

(3) *For* $1 \leqq i \leqq n$, *either* $u_i \in G_a$ *or* $u_i = a^{\pm 1}$.

(4) *For some* $i, 1 \leqq i \leqq n$, $u_i = a^{\pm 1}$.

(5) $u_1 \cdots u_n = 1$.

If, for some i, $1 \leqq i \leqq n-1$, we have $u_i, u_{i+1} \in G_a$ and $|u_i u_{i+1}| \leqq |a|$, then we replace the two factors u_i and u_{i+1} by a single factor $u_i u_{i+1}$ to obtain a sequence $v_1, \ldots, v_{n-1}$ of $n-1$ factors. Since A_a is a basis for a free group not containing a, the sequence $v_1, \ldots, v_{n-1}$ satisfies (1)—(6), and iteration of this process will yield a new sequence satisfying the further condition:

(7) *For* $1 \leqq i \leqq n-1$, *if* $u_i, u_{i+1} \in G_a$ *then* $|u_i u_{i+1}| > |a|$.

Lemma 1. *If* $1 \leqq i \leqq n-1$, *then* $|u_i u_{i+1}| \geqq |u_i|, |u_{i+1}|$, *and both inequalities are strict unless exactly one of* u_i, u_{i+1} *is* $a^{\pm 1}$.

Proof. Either $u_i \in G_a$ or $u_i = a^{\pm 1}$, and either $u_{i+1} \in G_a$ or $u_{i+1} = a^{\pm 1}$. The case that $u_i, u_{i+1} \in G_a$ is given by (7). The case that $u_i = u_{i+1}^{-1} = a^{\pm 1}$ is excluded by (1). In the case that $u_i = u_{i+1} = a^{\pm 1}$, since $a \neq 1$ we have $|a^{\pm 2}| > |a|$. The case remains that one of u_i, u_{i+1} is in G_a and the other is $a^{\pm 1}$. Suppose $u_i \in G_a$ and $u_{i+1} = a^{\pm 1}$. Then $|u_i u_{i+1}| < |a|$ would imply $u_i u_{i+1} \in G_a$. This, with $u_i \in G_a$ would give $a = u_{i+1}^{\pm 1} \in G_a$, contrary to $a \in A$.

Lemma 2. *If $2 \leqq i \leqq n-1$ and u_i cancels exactly half in each of its neighbors, that is,*

$$|u_{i-1} u_i| = |u_{i-1}| \quad \textit{and} \quad |u_i u_{i+1}| = |u_{i+1}|,$$

then either:

$$\text{(A)} \qquad u_i = a^{\pm 1}; \quad u_{i-1}, u_{i+1} \neq a^{\pm 1}; \quad |u_{i-1}| = |u_{i+1}| = |a|;$$

and exactly half of each of u_i, u_{i+1} remains in $u_{i-1} u_i u_{i+1}$; or:

$$\text{(B)} \qquad u_{i-1} = u_{i+1} = a^{\pm 1}; \quad |u_i| < |a|;$$

and more than half of each of u_{i-1}, u_{i+1} remains in $u_{i-1} u_i u_{i+1}$.

Proof. By Lemma 1, we must have either (A): $u_i = a^{\pm 1}$ and $u_{i-1}, u_{i+1} \in G_a$; or (B): $u_i \in G_a$ and $u_{i-1}, u_{i+1} = a^{\pm 1}$.

In Case A, Lemma 1 gives $|a| = |u_i| \leqq |u_{i-1} u_i| = |u_{i-1}|$, whence, by (2), $|u_{i-1}| = |a|$; similarly, $|u_{i+1}| = |a|$. If there were cancellation between u_{i-1} and u_{i+1} we should have $|u_{i-1} u_i u_{i+1}| < |a|$ and so $u_{i-1} u_i u_{i+1} \in G_a$. This with u_{i-1}, $u_{i+1} \in G_a$ would give $a = u_i^{\pm 1} \in G_a$, contrary to $a \in A$.

In Case B, we can write $u_i = pq$ where $|p| = |q| = \frac{1}{2} \cdot |u_i|$. Now $u_{i-1} = u_{i+1}^{-1} = a^{\pm 1}$ would imply that $p = q^{-1}$ and $u_i = 1$, contrary to (2). Therefore $u_{i-1} = u_{i+1} = a^{\pm 1}$ and we can write $a^{\pm 1} = q^{-1} r p^{-1}$ for some r. Now $|u_i| = |a|$ would imply that $r = 1$ and $u_i = a^{\pm 1}$, contrary to (1). Therefore $|u_i| < |a|$ and $r \neq 1$. If as much as half of one of u_{i-1} or u_{i+1}, and so of both, cancelled in the product $u_{i-1} u_i u_{i+1} = q^{-1} r^2 p^{-1}$, then each factor r in r^2 would have to cancel at least half, giving $|r^2| \leqq |r|$, which is not possible for $r \neq 1$.

Since, by (5), $u_1 \cdots u_n = 1$, the proof of the theorem will be complete when we have established the following lemma.

Lemma 3. $0 < |u_1| \leqq |u_1 u_2| \leqq \cdots \leqq |u_1 \cdots u_n|$.

Proof. We write $p_i = u_1 \cdots u_i$. We shall show, by induction on i, that $0 < |p_1| \leqq \cdots \leqq |p_i|$ and that $|p_{i-2}| = |p_{i-1}| = |p_i|$ only in case that $|p_{i-3}| < |p_{i-2}|$ and that u_{i-2}, u_{i-1}, u_i fall under Case A of Lemma 2. For $i = 1, 2, 3$, this follows directly from (2) and Lemmas 1 and 2. We assume this condition for some i, $3 \leqq i \leqq n-1$, and shall prove it for $i+1$.

Suppose $|p_{i-1}| < |p_i|$; then we must show that $|p_i| \leqq |p_{i+1}|$. Now $|p_{i-1}| < |p_i|$ implies that more than half of u_i remains in p_i; since at most half of u_i cancels in $u_i u_{i+1}$, some part of u_i remains in p_{i+1}. Therefore as much of u_{i+1} remains in p_{i+1} as in $u_i u_{i+1}$, that is, at least half, and $|p_i| \leqq |p_{i+1}|$.

Suppose $|p_{i-2}| < |p_{i-1}| = |p_i|$; we must show that $|p_i| \leqq |p_{i+1}|$, with equality only under Case A. Now part of u_{i-1} remains in p_i, whence as much of u_{i+1} remains in p_{i+1} as in $u_{i-1} u_i u_{i+1}$, and the conclusion follows by Lemma 2.

Finally, suppose that $|p_{i-2}| = |p_{i-1}| = |p_i|$; we must show that $|p_i| < |p_{i+1}|$. By the induction hypothesis, u_{i-2}, u_{i-1}, u_i fall under Case A, and half of u_i remains in p_i. Then $|u_i| = |a|$, and u_{i-1}, u_i, u_{i+1} cannot fall under Lemma 2, whence less than half of u_i cancels in $u_i u_{i+1}$, and part of u_i remains in p_{i+1}. But then u_{i+1} cancels no more in p_{i+1} than in $u_i u_{i+1}$. If $u_{i+1} = a^{\pm 1}$ this is less than u_i cancels in $u_i u_{i+1}$, hence less than half, while if $u_{i+1} \in G_a$, this is less than half by (7). In both cases, $|p_i| <$ $< |p_{i+1}|$.

Reference

[1] H. Federer and B. Jónsson, Some properties of free groups. Trans. Amer. Math. Soc. **68**, 1–27 (1950).

Eingegangen am 12. 5. 1964

Anschrift des Autors:
Robert Kubota
c. o. R. C. Lyndon
Mathematics Angell Hall
University of Michigan
Ann Arbor (Mich.), USA