Canad. Math. Bull. Vol. 14 (3), 1971

ON CANONICAL GENERATORS OF SUBGROUPS

BY
PETER FANTHAM

Introduction. Let H be a cyclic group, $K\subset H$ a subgroup and x, y generators of H, K. We shall say that x, y are *related* if $y=x^a$ where a is the index of K in H, in other words, y is the smallest positive power of x in K. The main purpose of this note is to show that for any group G one may, by means of the axiom of choice, choose for each cyclic group $H\subset G$ a generator x_H such that when $K\subset H$ then x_K, x_H are related.

Let H be a cyclic group with generator x and let $K\subset H$ be a subgroup.

LEMMA 1. *If z is a generator of K there is a generator y of H such that y, z are related.*

Proof. If $o(H)=\infty$, the result is clear. If $o(K)=k$, $o(H)=ak$, then $z=x^{an}$, say, where $(n, k)=1$. The problem of finding a generator x^m of H related to z reduces, then, to solving for m the equations $(m, ak)=1$, $am\equiv an \pmod{ak}$ and a solution is given by any prime of the form $n+\lambda k$.

If G is a group, a subset $B\subset G$ is called a *k-set* if (i) no cyclic subgroup has more than one generator in B, (ii) if $x, y\in B$ generate comparable subgroups they are related. We denote by $F(B)$ the family of cyclic subgroups of G with a generator in B. B is called *semi-complete* if $F(B)$ is hereditary and *complete* if $F(B)$ is the set of all cyclic subgroups of G.

LEMMA 2. *If G is finite cyclic and B is a k-set for which $F(B)$ comprises all proper subgroups of G then B is a subset of a complete k-set.*

Proof. Let $n=p_1^{a_1}p_2^{a_2}\dots p_r^{a_r}$ be a primary decomposition of $o(G)$. Let H_i be the subgroup of G of order n/p_i. By Lemma 1 there is a generator x of G such that x^{p_1} is the generator of H_1 in B. Let the generator of H_i in B be $x^{r_ip_i}$. The generators of $H_i\cap H_j$ related to $x^{r_ip_i}$ and $x^{r_jp_j}$ are $x^{r_ip_ip_j}$, $x^{r_jp_ip_j}$ respectively, and since B is a semi-complete k-set they are equal. Thus $r_1=1$ and $r_i\equiv r_j \pmod{n/p_ip_j}$ for $i, j=1, 2, \dots, r$. It follows that $r_i=1+s_in/p_1p_i$, say, for $i=2,\dots, r$, and since $r_i-r_j=n(s_ip_j-s_jp_i)/p_1p_ip_j$ we deduce that $s_ip_j-s_jp_i$ is divisible by p_1. We wish to find a generator x^r of G such that $x^{r_ip_i}$ is related to x^r for all i. This requires finding $r \pmod n$ such that $(r, n)=1$ and such that $r\equiv r_i \pmod{n/p_i}$, $i=1, 2, \dots, r$. The equation with $i=1$ is satisfied for any value of r of the form $r=1+kn/p_1$.

Received by the editors July 3, 1970 and, in revised form, October 15, 1970.

The remaining equations expressed in k then become $kn/p_1 \equiv s_i n/p_1 p_i \pmod{n/p_i}$, $i=2, \ldots, r$, i.e. $kp_i \equiv s_i \pmod{p_1}$, $i=2, \ldots, r$. Since p_1, p_2 are relatively prime, the equation for $i=2$ has a solution, and with this value

$$(kp_i - s_i)p_2 \equiv kp_i p_2 - s_2 p_i \pmod{p_1} \equiv 0 \pmod{p_1},$$

i.e. $kp_i \equiv s_i \pmod{p_1}$, $i=2, \ldots, r$. Finally, since r_i is prime to n/p_i, so also is r, and hence r is prime to n. This completes the proof.

LEMMA 3. *Any semi-complete k-set B is contained in a k-set C such that F(C) contains all finite cyclic subgroups.*

Proof. Let F_n denote the family of cyclic subgroups of G whose orders have at most n prime factors. For each $H \in F_1$, $H \notin F(B)$, choose a generator x of H and add all the generators arising in this way to B to form the set B_1. Clearly, B_1 is semi-complete and $F_1 \subset F(B_1)$. Suppose, inductively, that we have constructed $B_n \supset B$ with the property that $F_n \subset F(B_n)$. Let $H \in F_{n+1}$, $H \notin F(B_n)$. Then $H \cap B_n$ is a semi-complete k-set in H such that every proper subgroup of H has a generator in B_n and so, by Lemma 2, we can extend $H \cap B_n$ by adding a generator of H to form a complete k-set of H. If we add all such generators to B_n we obtain a set B_{n+1}, which by construction is semi-complete and includes a generator of every subgroup in F_{n+1}. This completes the induction. If we now put $C = \bigcup_{n=1}^{\infty} B_n$, it is immediate that C satisfies the conditions of the theorem.

THEOREM 1. *Every group G possesses a complete k-set.*

Proof. In view of Lemma 3, it suffices to show that there is a semi-complete k-set B for which $F(B)$ includes all infinite cyclic subgroups.

If H, K are infinite cyclic subgroups of G, write $H \simeq K$ if $H \cap K \neq \{e\}$. Since the intersection of two infinite cyclic subgroups of a cyclic group is always nontrivial, this relation is an equivalence. If H is an infinite cyclic subgroup of G, let $\bar{H}$ denote the set of all cyclic subgroups K of G with $H \simeq K$. Choose a generator x_H of H. If $H \simeq K$, let x_K be the generator of K such that $H \cap K$ is generated by $x_H^p = x_K^q$, say, where p, q are both positive. If $A(\bar{H})$ is the set of all such elements x_K then $A(\bar{H}) \cup \{e\}$ is a semi-complete k-set, for if $H \simeq K$, $H \simeq L$ and $K \supset L$ then $x_H^p = x_K^q$, $x_H^r = x_L^s$, $x_L = x_K^t$ say, where p, q, r, s are positive. Then t is positive and hence x_L is related to x_K. Thus $A(\bar{H})$ is a k-set and is semi-complete by construction. Any two sets of the form $A(\bar{H})$ have only the element e in common and hence the union of the sets $A(\bar{H})$ constitutes a semi-complete k-set with the required property.

THEOREM 2. *Any semi-complete k-set B in G can be extended to a complete k-set.*

Proof. By virtue of Lemma 3 it suffices to show that if all elements of B have infinite order then B is contained in a semi-complete k-set A such that $F(A)$ coincides with the set of all infinite cyclic subgroups.

Referring to the proof of the previous theorem, it suffices to show that if H is

https://doi.org/10.4153/CMB-1971-059-4 Published online by Cambridge University Press

an infinite cyclic subgroup of G and B' is a semi-complete k-set all of whose elements generate members of $\bar{H}$, then there is an extension C' of B' with $F(C')=\bar{H}$. If $B'=\varnothing$ we proceed as in Theorem 1. Otherwise, we may suppose without loss of generality, that H has a generator x_H in B'. We construct $A(\bar{H})$ as before, whence we must show that, if $H\simeq K$, where K has a generator x'_K in B', then $x_K=x'_K$. However, if $L=H\cap K$ and L is generated by the element $x_H^p=x_K^q=(x'_K)^r$, say, then since $A(\bar{H})$ and B' are both semi-complete, p, q, r are all positive and hence $x_K=x'_K$.

UNIVERSITY OF TORONTO,
TORONTO, ONTARIO