ON A THEOREM OF KRAPEZ

PETR VOJTĚCHOVSKÝ

In a private conversation, Alexandar Krapez told me about the following theorem for groups:

Theorem 0.1 (Krapez)**.** *Let A be a nonempty subset of a group G of order n. Then $A^n = \{x_1x_2\cdots x_n;\ x_i \in A\}$ is a subgroup of G.*

The purpose of this note is to give a short proof. (I never saw Krapez's proof. It is possible that it is very similar. But my impression was that the original proof was longer.)

Proof. Note that $A^{m+1} = \bigcup_{x\in A} A^m x$. Since all translations inject, we have $|A^{m+1}| \geq |A^m|$. If $|A^{m+1}| > |A^m|$ for every $m < n$, we must have $A^n = G$, and there is nothing to prove.

Otherwise, let $m < n$ be such that $|A^m| = |A^{m+1}|$. Then $A^{m+1} = A^m x$ for every $x \in A$. Thus $A^{m+1}x = AA^m x = AA^{m+1} = A^{m+2}$, and $|A^{m+2}| = |A^{m+1}|$ follows. By induction, $|A^{m+k}| = |A^m|$ for every positive k.

In particular $|A^{2n}| = |A^n|$. As $1 = x^n$ for any $x \in A$, we have $A^nA^n \supseteq 1A^n = A^n$, and $A^nA^n = A^n$ follows. This means that A^n is closed under multiplication, i.e, it is a subgroup of G. □

The fact that $|A^m| = |A^{m+1}| = |A^{m+2}| = \cdots$ does not imply that $A^m = A^{m+1} = A^{m+2}\cdots$. Consider, for instance, the cyclic group $G = \{1, g\}$, and let $A = \{g\}$. Then $|A^m| = 1$ for any positive m. However, $A^m = A$ when m is odd, and $A^m = \{1\}$ when m is even.

Department of Mathematics, University of Denver, 2360 S Gaylord St, Denver, CO, 80200, U.S.A.

E-mail address: petr@math.du.edu