PUBLICATIONS DE L'INSTITUT MATHÉMATIQUE
Nouvelle série, tome 17 (31), 1974, pp. 77—81

ON A GENERALIZATION OF FERMAT'S THEOREM IN THE THEORY OF GROUPS

A. Krapež

(Comunicated January 5, 1973)

The object of this paper is the algebraic stucture, induced by the finite group on its partitive set. A theorem will be proved, concerning the elements of this structure analogous to the Fermat's about the elements of the group. According to Fermat's theorem, if a is an element of the finite group G with n elements, then $a^n = e$, where e is the neutral element of the group G. According to theorem 2 of this paper, if A is a complex (subset) of the finite group G with n elements then $A^n = H_A$, where H_A is the subgroup of G, related to A in a certain sense (theorem 1). If A has only one element ($A = \{a\}$), then $A^n = \{a^n\} = \{e\}$, and Fermat's theorem is a special case of theorem 2.

*

Let G be a finite group with n elements. Any subset A of G will be called a complex of the group G. The product of complexes is defined as follows:

$$AB = \{ab \mid a \in A \wedge b \in B\}.$$

The product of a complex and an element of the group is reduced to the product of the complexes:

$$Ab = A\{b\} \qquad aB = \{a\}B.$$

$A^0 = \{e\}$ by definition. Other powers of A are defined in the usual way.

Lemma 1. *If A and B are nonempty complexes of the finite group G, then:*

1° $\max\{\operatorname{card} A, \operatorname{card} B\} \leqslant \operatorname{card} AB \leqslant \operatorname{card} A \operatorname{card} B$

2° *If $n \leqslant m$ then* $\operatorname{card} A^n \leqslant \operatorname{card} A^m$.

The proof of lemma 1 is obvious and will be omitted.

In the sequel, our attention will be directed to the sequence $(A^m)_{m \in N}$ and related notions.

It follows from lemma 1 that the sequence $(\operatorname{card} A^m)_{m \in N}$ is nondecreasing. In the next theorem we shall see that this sequence increases to a certain value, which it keeps further on.

Theorem 1. *Let A be a complex of the finite group G. Then:*

1° *There is a natural number k such that A^k is a (unique) subgroup of G in the sequence $(A^m)_{m\in N}$.*

2° *There is a natural number i $(i\leqslant k)$ such that for all natural numbers m_1, m_2 and m_3 $(m_1<m_2<i<m_3)$ the following relations hold:*

$$\operatorname{card} A^{m_1}<\operatorname{card} A^{m_2}<\operatorname{card} A^i=\operatorname{card} A^{m_3} \tag{1}$$

3° *A^m is a coset (conjugate class) of the subgroup A^k iff $i\leqslant m$.*

Proof: 1° (a) Let A have the following property: $\operatorname{card} A^m=\operatorname{card} A$ holds for all $m\in N$. Let $a\in A$ and let k be the order of a. Then:

$$A^k=a^kA^k\subset(A^k)^2=A^{2k}. \tag{2}$$

$$\operatorname{card} A^k=\operatorname{card} A=\operatorname{card} A^{2k}, \quad \text{by hypothesis.} \tag{3}$$

(2) and (3) imply $A^{2k}=A^k$ i.e. A^k is a subgroup of G.

(b) The general case.

According to lemma 1 the sequence $(\operatorname{card} A^m)_{m\in N}$ is nondecreasing. Also $\operatorname{card} A^m\leqslant\operatorname{card} G$. Consequently $(\operatorname{card} A^m)_{m\in N}$ converges. It follows from the fact that all values of $(\operatorname{card} A^m)_{m\in N}$ are natural numbers, that from some m_0 further on the sequence takes only one value. Then the sequence $((A^{m_0})^m)_{m\in N}$ satisfies the condition from (a). Consequently there exists a subgroup of G in $((A^{m_0})^m)_{m\in N}$. Therefore there also exists a subgroup of G in $(A^m)_{m\in N}$. The proof of the uniqueness of this subgroup in $(A^m)_{m\in N}$ will be presented after the proof of 2°.

2° (a) Let j be a natural number such that $\operatorname{card} A^{j+1}=\operatorname{card} A^j$ (there exists such a number; for example if A^k is a subgroup then $\operatorname{card} A^k\leqslant\operatorname{card} A^{k+1}\leqslant\operatorname{card} A^{2k}=\operatorname{card} A^k$). Then A^{j+1} can be represented as aA^j for some $a\in A$. From $a\in A$ it follows that $aA^j\subset A^{j+1}$ and, with $\operatorname{card} A^{j+1}=\operatorname{card} A^j=\operatorname{card} aA^j$, it implies that $aA^j=A^{j+1}$. Let us prove by induction that $A^{j+r}=a^rA^j$, for all natural numbers r. For $r=1$ the proposition is already proved. Suppose that the proposition is valid for some $r-1$, i.e. that $A^{j+r-1}=a^{r-1}A^j$. Then $A^{j+r}=A^{j+r-1}A=a^{r-1}A^jA=a^{r-1}A^{j+1}=a^{r-1}aA^j=a^rA^j$ and the proposition is also valid for r. Consequently the proposition holds for all $r\in N$.

(b) Let i be the smallest natural number such that $\operatorname{card} A^{i+1}=\operatorname{card} A^i$. According to (a), for all natural numbers m_1, m_2 and m_3 $(m_1<m_2<i<m_3)$ it follows that.

$$\operatorname{card} A^{m_1}<\operatorname{card} A^{m_2}<\operatorname{card} A^i=\operatorname{card} A^{m_3} \tag{4}$$

because of $\operatorname{card} A^{m_1}<\operatorname{card} A^{m_1+1}\leqslant\operatorname{card} A^{m_2}<\operatorname{card} A^{m_2+1}\leqslant\operatorname{card} A^i=\operatorname{card} A^{m_3}$. i will be called the index of A.

(c) Let A^k be a subgroup. Then:

$$\operatorname{card} A^k\leqslant\operatorname{card} A^{k+1}\leqslant\operatorname{card} A^{2k}=\operatorname{card} A^k \quad \text{i.e.} \quad \operatorname{card} A^{k+1}=\operatorname{card} A^k.$$

Consequently $i\leqslant k$.

1° (c) Let A^p and A^q $(p\leqslant q)$ be subgroups of G. According to 2° (c) $i\leqslant p\leqslant q$ and:

$$\operatorname{card} A^p=\operatorname{card} A^i=\operatorname{card} A^q. \tag{5}$$

Also $q = sp + t$ $(0 \leqslant t < p)$, whence:

$$A^q = A^{sp+t} = A^{sp} A^t = (A^p)^s A^t = A^p A^t. \tag{6}$$

According to 2° (c) and 2° (a) (for $j = p$, $r = t$) A^q can be represented as

$$A^q = A^p a^t \quad \text{for some} \quad a \in A. \tag{7}$$

It means that any $b \in A^q$ can be represented as $b = ca^t$, for some $c \in A^p$. $e \in A^q$ because A^q is a subgroup. Consequently $e = ca^t$, for some $c \in A^p$. It follows that $a^t = c^{-1}$. A^p, being a group, contains c^{-1} with c; it follows that $a^t \in A^p$ whence (from (6) and (7)):

$$A^q = A^p A^t = A^p a^t = A^p.$$

The unique subgroup in the sequence $(A^m)_{m \in N}$ will be called the characteristic subgroup of A and will be denoted by H_A. The smallest natural number k such that A^k is a subgroup will be called the characteristic of A.

3° (a) Let $i \leqslant m$ and let A^k be a subgroup of G. According to 2° (c) and 2° (a) (for $j = k$ and $r = m$)

$$A^{k+m} = a^m A^k. \tag{8}$$

Also:

$$A^m = A^m e \subset A^m A^k = A^{k+m}. \tag{9}$$

From (9) and

$$\operatorname{card} A^m = \operatorname{card} A^i = \operatorname{card} A^{k+m} \quad (i \leqslant m) \tag{10}$$

we can deduce $A^m = A^{k+m}$. From (8) and (10) it follows that

$$A^m = a^m A^k, \tag{11}$$

i. e. A^m is a coset of A^k.

(b) If A^m is a coset of A^k then $\operatorname{card} A^m = \operatorname{card} A^k$ i. e. $i \leqslant \min\{m, k\} \leqslant m$.

According to 3° A^m (for $i \leqslant m$) can be represented as $A^m = a^m A^k$ for some $a \in A$. This result enables us to prove theorem 2. For this proof we need also the following lemma:

Lemma 2. *Let i be the index of a complex A of the finite group G with n elements. Then $i \leqslant n$.*

Proof: 1° Assume that $\operatorname{card} A = 1$. Then $\operatorname{card} A^2 = \operatorname{card} A = 1$ and $i = 1$. From $n \geqslant 1$ we deduce $i \leqslant n$.

2° Let $\operatorname{card} A > 1$. Suppose that $i > n$. Then:

$\operatorname{card} A > 1$

$\operatorname{card} A^2 > \operatorname{card} A \geqslant 2$ i. e. $\operatorname{card} A^2 > 2$

...

$\operatorname{card} A^{n-1} > \operatorname{card} A^{n-2} > n - 2$ i. e. $\operatorname{card} A^{n-1} > n - 1$ i. e. $\operatorname{card} A^{n-1} = n$.

It follows that $A^{n-1} = G$ and $A^n = AA^{n-1} = AG = G$ i. e. $\operatorname{card} A^n = \operatorname{card} A^{n-1}$. Consequently $i = n - 1$ which contradicts the hypothesis. It follows that $i \leqslant n$.

Let us prove the main theorem of this paper:

Theorem 2. *Let A be a complex of the finite group G with n elements. Then $A^n = H_A$.*

Proof: According to lemma 2, $i \leqslant n$, so A^n is a coset of the subgroup H_A and it can be represented (according to theorem 1) as $A^n = a^n H_A$, for some $a \in A$. Making use of Fermat's theorem ([2] p. 593, [3] p. 188), we can deduce $A^n = H_A$, completing the proof.

Finally, let us consider the relations between the characteristic subgroup of A and the subgroup $[A]$ generated by A ($[A]$ is the minimal subgroup of G containing all the elements of A).

Theorem 3. *Let A be a complex of the finite group G with n elements and let H_A and $[A]$ be respectively the characteristic subgroup of A and the subgroup generated by A. Then:*

1° $[A] = H_{A\cup\{e\}}$ *($H_{A\cup\{e\}}$ being the characteristic subgroup of $A\cup\{e\}$).*

2° *H_A is the normal subgroup of $[A]$.*

3° *If $m = \operatorname{card}[A]$ then $A^m = H_A$.*

4° $[A] = \bigcup_{r=1}^{n} a^r H_A$, *for some $a \in A$.*

5° $[A] = H_A$ *iff* $A \subset H_A$.

Proof. 1° $(A\cup\{e\})^2 = A^2 \cup A\{e\} \cup \{e\}A \cup \{e\} = A^2 \cup A \cup \{e\}$.

Analogously $(A\cup\{e\})^m = \bigcup_{r=0}^{m} A^r$ for all $m \in N$. Consequently $m_1 < m_2$ implies $(A\cup\{e\})^{m_1} \subset (A\cup\{e\})^{m_2}$. Applying lemma 2 ($i \leqslant n$, i is the index of A) we can deduce:

$$(A\cup\{e\})^i = \cdots = (A\cup\{e\})^n = \cdots \tag{12}$$

From (12) $[A] = \bigcup_{r=0}^{\infty} A^r = \bigcup_{r=0}^{n} A^r = (A\cup\{e\})^n = H_{A\cup\{e\}}$ ($[A] = \bigcup_{r=0}^{\infty} A^r$ since G is a finite group).

2° The proof is obvious if we keep in mind that the elements of $[A]$ are the finite products of the elements of A and that $aH_A = H_A a$ holds for all $a \in A$. The last assertion follows from $aH_A = AH_A$ and from theorem 2.

3° If G is a finite group then $[A]$ is also finite, and $A \subset [A]$.

4° For all $m \in N$, complexes $A^m H_A$ are elements of the factorgroup $[A]/H_A$. $i \leqslant k$ implies $A^m H_A = a^m H_A$ for all $m \in N$ and some $a \in A$. Consequently

$$[A] = \bigcup_{m=0}^{\infty} A^m H_A = \bigcup_{m=0}^{\infty} a^m H_A = \bigcup_{m=0}^{n} a^m H_A.$$

5° Suppose that $A \subset H_A$. Then:

$$A^2 \subset H_A^2 = H_A$$

$$\cdots$$

$$A^n \subset H_A^n = H_A$$

$$[A] = \bigcup_{r=0}^{n} A^r \subset \{e\} \cup \left(\bigcup_{r=1}^{n} H_A \right) = \{e\} \cup H_A = H_A \tag{13}$$

$$A^n = H_A \quad \text{i. e.} \quad H_A \subset \bigcup_{r=0}^{n} A^r = [A]. \tag{14}$$

From (13) and (14) we deduce $[A] = H_A$.

Conversely, suppose that $[A] = H_A$. Then $[A]/H_A$ has only one element i. e.

$$AH_A = H_A. \tag{15}$$

$$e \in H_A \quad \text{implies} \quad A \subset AH_A. \tag{16}$$

(15) and (16) implies $A \subset H_A$.

Part 1° of the theorem 3 is a generalisation of a theorem by Frobenius [1], about the subgroup generated by a complex A containing the neutral e. Parts 2° and 5° define completely the relation between H_A and $[A]$. Part 3° is the equivalent of the theorem 2.

REFERENCES

[1] G. Frobenius; *Über endliche Gruppen*, Sitzungsber. preuss. Akad. Wiss., Berlin, 1895, 163—194.

[2] Dj. Kurepa; *Viša algebra I*, Školska knjiga, Zagreb, 1965, 559—667.

[3] N. H. McCoy; *Introduction to modern algebra*, Boston: Allyn and Bacon, Inc., 1964, 187—188.

[4] T. Tamura, J. Shafer; *Power semigroups*, Math. Japonicae, vol. 12, No. 1, pp. 25—32, 1967.