FUNDAMENTAL THEOREM OF FINITE ABELIAN GROUPS

M. G. MAHMOUDI

Abstract. The proof presented here is a variation of the one given in Gallian's book [1].

Lemma 1. *Let p be a prime number and let G be a finite p-group. Let $a \in G$ be an element whose order is maximum among all elements of G.*
(i) If $G \neq \langle a \rangle$ then there exists an element $b \in G \backslash \langle a \rangle$ such that $\langle a \rangle \cap \langle b \rangle = \{e\}$.
(ii) There exists a subgroup K of G such that $G = \langle a \rangle K$ with $\langle a \rangle \cap K = \{e\}$.

Proof. (i) Let $b \in G \backslash \langle a \rangle$ be an element with minimum order. Since G is a p-group, $o(b) < o(b^p)$, hence by the choice of b we have $b^p \in \langle a \rangle$. Thus there exists an integer i such that $b^p = a^i$. If $(i, p) = 1$ then $o(b^p) = o(a^i) = o(a) \geq o(b)$ which is a contradiction. Hence $p|i$ and so there exists an integer j such that $i = pj$. Now $b^p = a^i$ implies that $(ba^{-j})^p = e$. Since $ba^{-j} \notin \langle a \rangle$, we have $ba^{-j} \neq e$ and hence $o(ba^{-j}) = p$. The minimality of the order of b implies that $o(b) = p$. This implies that the order of $\langle a \rangle \cap \langle b \rangle$ divides p. If this order is 1, the claim is proved, if this order is p, then $\langle b \rangle \subseteq \langle a \rangle$ which contradicts the fact that $b \notin \langle a \rangle$.

(ii) We prove the assertion by induction on $|G|$. For $|G| = 1$ the assertion is clear. If $\langle a \rangle = G$ we can take $K = \{e\}$ and the result is proved. Hence we may assume that $G \neq \langle a \rangle$. By (i) there exists an element $b \in G \backslash \langle a \rangle$ such that $\langle a \rangle \cap \langle b \rangle = \{e\}$. We have $|G/\langle b \rangle| < |G|$. Since $\langle a \rangle \cap \langle b \rangle = e$, the order of the coset $a\langle b \rangle \in G/\langle b \rangle$ is equal to $o(a)$. Hence $a\langle b \rangle$ is also an element of maximum order in $G/\langle b \rangle$. Also note that $\langle a\langle b \rangle \rangle = \langle a \rangle \langle b \rangle / \langle b \rangle$. By induction there exists a subgroup $K/\langle b \rangle$ of $G/\langle b \rangle$ such that $\frac{\langle a \rangle \langle b \rangle}{\langle b \rangle} \frac{K}{\langle b \rangle} = \frac{G}{\langle b \rangle}$ and $\frac{\langle a \rangle \langle b \rangle}{\langle b \rangle} \cap \frac{K}{\langle b \rangle} = \frac{\langle b \rangle}{\langle b \rangle}$. It follows that $\langle a \rangle \langle b \rangle K = G$ and $\langle a \rangle \langle b \rangle \cap K = \langle b \rangle$. We claim that $G = \langle a \rangle K$ and $\langle a \rangle \cap K = \{e\}$. In fact $\langle a \rangle K = \langle a \rangle (\langle b \rangle K) = \langle a \rangle \langle b \rangle K = G$. Also on the one hand $\langle a \rangle \cap K \subseteq \langle a \rangle$, on the other hand, $\langle a \rangle \cap K \subseteq \langle a \rangle \langle b \rangle \cap K = \langle b \rangle$, thus $\langle a \rangle \cap K \subseteq \langle a \rangle \cap \langle b \rangle = \{e\}$. □

Theorem 2 (Converse of Lagrange theorem)**.** *Let G be a finite abelian group of order n and let d be a divisor of n. Then G has a subgroup H of order d.*

Theorem 3. *Let G be a finite abelian group. Then there exists cyclic groups $C_1, \ldots, C_k$ such that $G \simeq C_1 \times \cdots \times C_k$.*

Proof. We prove the claim by induction on the order of G. If $|G| = 1$, the assertion is clear. Let $|G| = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ be the decomposition of $|G|$ into primes where $p_i \neq p_j$ for $i \neq j$. By the converse of Lagrange's theorem, G has a subgroup H of order $p_1^{\alpha_1}$ and a subgroup L of order $p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, and $G = HL \simeq H \times L$. If $|G|$ has at least two distinct prime divisors, by induction both groups H and L are isomorphic to a product of cyclic groups, hence so is G. Hence it suffices to prove the result for the case where G is a p-group for some prime number p. Let $a \in G$ be an element whose order is maximum. If $\langle a \rangle = G$, then G is cyclic and the result is proved. If $\langle a \rangle \neq G$, by Lemma 1, there exists a subgroup K of G such that $\langle a \rangle \cap K = \{e\}$ and $G = \langle a \rangle K$, hence $G \simeq \langle a \rangle \times K$. By induction K is isomorphic to a product of cyclic groups hence so is G. □

References

[1] J. A. Gallian, *Contemporary abstract algebra. 9th edition.*, 9th edition ed., Boston, MA: Brooks/Cole, Cengage Learning, 2016.

M. G. Mahmoudi, mmahmoudi@sharif.ir, Department of Mathematical Sciences, Sharif University of Technology, P. O. Box 11155-9415, Tehran, Iran. Fax: (+98) (21) 6616-5117

Date: November 24, 2019.