#A52 INTEGERS 9 (2009), 699-702

FACTORIZATION RESULTS WITH COMBINATORIAL PROOFS

Keresztély Corrádi
Department of General Computer Technics, Eötvös L. University, Pázmány P. sétány 1/c, Budapest, HUNGARY

Sándor Szabó
Institute of Mathematics and Informatics, University of Pécs, Pécs, HUNGARY
sszabo7@hotmail.com

Received: 6/27/09, Accepted: 9/18/09, Published:

Abstract

Two results on factorization of finite abelian groups are proved using combinatorial character free arguments. The first one is a weaker form of Rédei's theorem and presented only to motivate the method. The second one is an extension of Rédei's theorem for elementary 2-groups, which was originally proved by means of characters.

1. Introduction

We will use multiplicative notation in connection with abelian groups. The neutral element of a group will be called identity element and it will be denoted by e. Let G be a finite abelian group and let $A_1, \ldots, A_n$ be subsets of G. The product $A_1 \cdots A_n$ is defined to be the set

$$\{a_1 \cdots a_n : \ a_1 \in A_1, \ldots, a_n \in A_n\}.$$

The product $A_1 \cdots A_n$ is called direct if

$$a_{1,1} \cdots a_{1,n} = a_{2,1} \cdots a_{2,n}, \quad a_{1,1}, a_{2,1} \in A_1, \ldots, a_{1,n}, a_{2,n} \in A_n$$

imply that $a_{1,1} = a_{2,1}, \ldots, a_{1,n} = a_{2,n}$. If the product $A_1 \cdots A_n$ is direct and if it is equal to G, then we say that $G = A_1 \cdots A_n$ is a factorization of G.

A subset A of G is called normalized if $e \in A$. A factorization $G = A_1 \cdots A_n$ is called normalized if each A_i is a normalized subset of G. Rédei [2] has proved the following result. Let G be a finite abelian group and let $G = A_1 \cdots A_n$ be a normalized factorization of G. If each $|A_i|$ is a prime, then at least one of the factors $A_1, \ldots, A_n$ must be a subgroup of G.

Examples show that the condition that each factor has a prime number of elements cannot be dropped from Rédei's theorem. However for elementary 2-groups Sands and Szabó [3] proved the following generalization. Let G be a finite elementary 2-group and let $G = A_1 \cdots A_n$ be a normalized factorization of G. If each $|A_i| = 4$, then at least one of the factors $A_1, \ldots, A_n$ is a subgroup of G.

In this paper we will present an elementary combinatorial argument to verify a weaker version of Rédei's theorem for elementary p-groups, where p is an odd prime.

Then applying the method to elementary 2-groups we obtain a combinatorial character free proof for the Sands-Szabó result.

2. Elementary p-groups

Let G be a finite abelian group of odd order. Let $G = A_1 \cdots A_n$ be a normalized factorization of G, where each $|A_i|$ is a prime. By Rédei's theorem at least one of the factors $A_1, \ldots, A_n$ is a subgroup of G. Say A_i is a subgroup of G. Now as $|A_i|$ is odd, it follows that the product of the elements of A_i is equal to e. This indicates that the following theorem is a weaker version of Rédei's theorem. The essential point is that we are able to give a combinatorial proof of this result.

Theorem 1 *Let p be an odd prime. Let G be a finite elementary p-group and let $G = A_1 \cdots A_n$ be a normalized factorization of G, where $|A_i| = p$, for each i, $1 \leq i \leq n$. Let*

$$d_i = \prod_{a \in A_i} a.$$

Then $d_i = e$ for some i, $1 \leq i \leq n$.

Proof. Assume on the contrary that there is a counterexample

$$G = A_1 \cdots A_n, \tag{1}$$

where none of the elements d_i is equal to e. For $n = 1$, the factor A_1 is equal to G and so $d_1 = e$. Thus we may assume that $n \geq 2$. Among the counterexamples we choose one with minimal n.

We introduce the following notations. For each i, $1 \leq i \leq n$ let

$$\begin{aligned} A_i &= \{e, a_{i,1}, \ldots, a_{i,p-1}\}, \\ U_i &= \langle a_{i,1} \rangle, \\ V_i &= \langle a_{i,2} \rangle, \\ X_i &= U_i \cup V_i, \\ d_i &= a_{i,1} \cdots a_{i,p-1}. \end{aligned}$$

If A_i is a subgroup of G, then $d_i = e$. In the counterexample (1) $d_i \neq e$ and so A_i is not a subgroup of G. In particular $A_i \neq U_i$. We may choose the notation such that $a_{i,2} \notin U_i$. As a consequence, $U_i \neq V_i$.

By Lemma 5 of [1], in the factorization (1) the factor A_1 can be replaced by U_1, V_1 to get the factorizations

$$G = U_1 A_2 \cdots A_n, \tag{2}$$
$$G = V_1 A_2 \cdots A_n, \tag{3}$$

respectively. From (2), by considering the factor group G/U_1 we get the factorization

$$G/U_1 = (A_2U_1)/U_1 \cdots (A_nU_1)/U_1$$

of G/U_1. Here

$$(A_iU_1)/U_1 = \{aU_1 : \ a \in A_i\}.$$

The minimality of the counterexample (1) forces that

$$d_iU_1 = \prod_{a \in A_i} aU_1$$

must be equal to eU_1 for some i, $2 \le i \le n$. Or equivalently $d_i \in U_1$ must hold for some i, $2 \le i \le n$.

Starting with factorization (3) we get that there is an index j, $2 \le j \le n$, such that $d_j \in V_1$.

If $d_i = d_j$, then by $d_i \in U_1 \cap V_1 = \{e\}$ we end up with the $d_i = e$ contradiction. Thus $d_i \ne d_j$.

The argument above provides that for the index 1 there are indices $\alpha(1)$, $\beta(1)$ such that $d_{\alpha(1)}, d_{\beta(1)} \in X_1$ and $\alpha(1) \ne \beta(1)$. In general, for the index i, $1 \le i \le n$ there are indices $\alpha(i)$, $\beta(i)$ such that $d_{\alpha(i)}, d_{\beta(i)} \in X_i$ and $\alpha(i) \ne \beta(i)$.

By Lemma 5 of [1], in the factorization (1) the factor A_1 can be replaced by U_1 to get the factorization $G = U_1A_2 \cdots A_n$. In this factorization the factor A_2 can be replaced by U_2 to get the factorization $G = U_1U_2A_3 \cdots A_n$. It follows that $U_1 \cap U_2 = \{e\}$. Similar arguments give that

$$\begin{array}{rcccl} U_1 \cap U_2 & = & U_1 \cap V_2 & = & \{e\}, \\ V_1 \cap U_2 & = & V_1 \cap V_2 & = & \{e\}. \end{array}$$

Therefore

$$X_1 \cap X_2 = (U_1 \cup V_1) \cap (U_2 \cup V_2) = \{e\}.$$

In general, $X_i \cap X_j = \{e\}$ for each i, j, $1 \le i, j \le n$, $i \ne j$.

Choose i, j such that $1 \le i, j \le n$, $i \ne j$. If $\alpha(i) = \alpha(j)$, then $d_{\alpha(i)} = d_{\alpha(j)}$ and so $d_{\alpha(i)} \in X_i \cap X_j = \{e\}$ gives the $d_{\alpha(i)} = e$ contradiction. Thus $i \ne j$ implies $\alpha(i) \ne \alpha(j)$. Similar arguments give that $i \ne j$ implies

$$\begin{array}{ll} \alpha(i) \ne \alpha(j), & \alpha(i) \ne \beta(j), \\ \beta(i) \ne \alpha(j), & \beta(i) \ne \beta(j). \end{array}$$

In particular the indices $\alpha(1), \ldots, \alpha(n)$ form a permutation of the elements $1, \ldots, n$. We know that $\alpha(1) \ne \beta(1)$. Since $\alpha(1), \ldots, \alpha(n)$ is a permutation of $1, \ldots, n$, there is an i, $2 \le i \le n$, such that $\alpha(i) = \beta(1)$. This violates $\alpha(i) \ne \beta(j)$.

The proof is complete. □

3. Elementary 2-groups

Theorem 1 is a weaker version of Rédei's theorem for elementary p-groups where p is an odd prime. The method of the proof of this theorem can be used to prove an extension of Rédei's theorem. First we present two lemmas.

Let G be a finite abelian group and let $A = \{e, u, v, w\}$ be a subset of G such that $u^2 = v^2 = w^2 = e$. Set

$$\begin{aligned} U &= \langle v, w \rangle, \\ V &= \langle u, w \rangle, \\ W &= \langle u, v \rangle, \\ X &= U \cup V \cup W, \\ d &= uvw. \end{aligned}$$

Lemma 2 *Let G be a finite abelian group and let $G = AB$ be a factorization of G. If A is a subset defined above, then*

$$G = UB, \quad G = VB, \quad G = WB$$

are factorizations of G.

Proof. As $G = AB$ is a factorization of G, the sets

$$eB,\ uB,\ vB,\ wB \tag{4}$$

form a partition of G. Multiplying the factorization $G = AB$ by u we get the factorization $G = Gu = (Au)B$. So the sets

$$uB,\ u^2B,\ uvB,\ uwB$$

form a partition of G. As $u^2 = e$ we get that the sets

$$uB,\ eB,\ uvB,\ uwB \tag{5}$$

form a partition of G. Comparing the partitions (4) and (5) we get

$$vB \cup wB = uvB \cup uwB.$$

From (4) we can see that $eB \cap uB = \emptyset$. Multiplying by v provides that $vB \cap uvB = \emptyset$. It follows that $vB \subset uwB$. A consideration on the cardinalities implies $vB = uwB$. In other words in (4) wB can be replaced by uvB which shows that the sets

$$eB,\ uB,\ vB,\ uvB$$

form a partition of G. Therefore $G = WB$ is a factorization of G. Similar arguments give that $G = VB$, $G = UB$ are factorizations.

This completes the proof. □

Lemma 3 *Using the notations introduced before Lemma 2 the subset A is a subgroup of G if and only if $d = e$.*

Proof. Suppose that A is a subgroup of G. Let us consider the product of u and v. As $uv \in A$ we face the following possibilities

$$uv = e,\ uv = u,\ uv = v,\ uv = w.$$

The first three lead to the

$$u = v,\ v = e,\ u = e$$

contradictions respectively. Thus $uv = w$. Consequently $uvw = e$, that is, $d = e$ as required.

Suppose that $d = e$. Now $e = uvw$ and so $w = uv$. Therefore $A = \langle u, v\rangle$ is a subgroup of G. □

Theorem 4 *Let G be a finite elementary 2-group and let $G = A_1 \cdots A_n$ be a normalized factorization of G, where $|A_i| = 4$, for each i, $1 \le i \le n$. Then A_i is a subgroup of G for some i, $1 \le i \le n$.*

Proof. Assume on the contrary that there is a counterexample

$$G = A_1 \cdots A_n, \tag{6}$$

where none of the factors A_i is a subgroup of G. For $n = 1$, the factor A_1 is equal to G and so we may assume that $n \ge 2$. Among the counterexamples we choose one for which n is as small as possible.

We introduce the following notation. For each i, $1 \le i \le n$ let

$$\begin{aligned} A_i &= \{e, u_i, v_i, w_i\}, \\ U_i &= \langle v_i, w_i\rangle, \\ V_i &= \langle u_i, w_i\rangle, \\ W_i &= \langle u_i, v_i\rangle, \\ X_i &= U_i \cup V_i \cup W_i, \\ d_i &= u_i v_i w_i. \end{aligned}$$

Note that $u_i^2 = v_i^2 = w_i^2 = e$. Since A_i is not a subgroup, by Lemma 3, $d_i \ne e$ must hold.

By Lemma 2, in the factorization (6) the factor A_1 can be replaced by U_1, V_1, W_1 to get the factorizations

$$G = U_1 A_2 \cdots A_n, \tag{7}$$
$$G = V_1 A_2 \cdots A_n, \tag{8}$$
$$G = W_1 A_2 \cdots A_n, \tag{9}$$

respectively. From (7), by considering the factor group G/U_1 we get the factorization

$$G/U_1 = (A_2U_1)/U_1 \cdots (A_nU_1)/U_1$$

of G/U_1. Here

$$(A_iU_1)/U_1 = \{aU_1 : \ a \in A_i\}.$$

The minimality of the counterexample (6) implies that $(A_iU_1)/U_1$ is a subgroup of G/U_1 for some i, $2 \leq i \leq n$. By Lemma 3 $(u_iU_1)(v_iU_1)(w_iU_1)$ must be equal to eU_1, that is, $u_iv_iw_i \in U_1$. This means $d_i \in U_1$ must hold.

Starting with factorization (8) we get that there is an index j, $2 \leq j \leq n$ such that $d_j \in V_1$. Starting with factorization (9) we get that there is an index k, $2 \leq k \leq n$ for which $d_k \in W_1$.

Note that

$$\begin{aligned} U_1 \cap V_1 \cap W_1 &= (U_1 \cap V_1) \cap W_1 \\ &= (\langle v_1, w_1\rangle \cap \langle u_1, w_1\rangle) \cap W_1 \\ &= \langle w_1\rangle \cap W_1 \\ &= \langle w_1\rangle \cap \langle u_1, v_1\rangle \\ &= \{e\}. \end{aligned}$$

If $d_i = d_j = d_k$, then $d_i \in U_1 \cap V_1 \cap W_1 = \{e\}$ lands on the $d_i = e$ contradiction. Thus d_i, d_j, d_k cannot all be equal.

We may summarize the previous argument in the following way. For the index 1 there are indices $\alpha(1)$, $\beta(1)$, $\gamma(1)$ such that $d_{\alpha(1)}, d_{\beta(1)}, d_{\gamma(1)} \in X_1$ and $\alpha(1)$, $\beta(1)$, $\gamma(1)$ are not all equal. In general, for the index i, $1 \leq i \leq n$ there are indices $\alpha(i)$, $\beta(i)$, $\gamma(i)$ such that $d_{\alpha(i)}, d_{\beta(i)}, d_{\gamma(i)} \in X_i$ and $\alpha(i)$, $\beta(i)$, $\gamma(i)$ are not all equal.

By Lemma 2, in the factorization (6) the factor A_1 can be replaced by U_1 to get the factorization $G = U_1A_2 \cdots A_n$. In this factorization the factor A_2 can be replaced by U_2 to get the factorization $G = U_1U_2A_3 \cdots A_n$. It follows that $U_1 \cap U_2 = \{e\}$. Similar arguments give that

$$\begin{aligned} U_1 \cap U_2 &= U_1 \cap V_2 = U_1 \cap W_2 = \{e\}, \\ V_1 \cap U_2 &= V_1 \cap V_2 = V_1 \cap W_2 = \{e\}, \\ W_1 \cap U_2 &= W_1 \cap V_2 = W_1 \cap W_2 = \{e\}. \end{aligned}$$

Therefore,

$$X_1 \cap X_2 = (U_1 \cup V_1 \cup W_1) \cap (U_2 \cup V_2 \cup W_2) = \{e\}.$$

In general, $X_i \cap X_j = \{e\}$ for each i, j, $1 \leq i, j \leq n$, $i \neq j$.

Choose i, j such that $1 \leq i, j \leq n$, $i \neq j$. If $\alpha(i) = \alpha(j)$, then $d_{\alpha(i)} = d_{\alpha(j)}$ and so $d_{\alpha(i)} \in X_i \cap X_j = \{e\}$ gives the $d_{\alpha(i)} = e$ contradiction. Thus $\alpha(i) \neq \alpha(j)$. Similar arguments give that

$$\begin{array}{lll} \alpha(i) \neq \alpha(j), & \alpha(i) \neq \beta(j), & \alpha(i) \neq \gamma(j), \\ \beta(i) \neq \alpha(j), & \beta(i) \neq \beta(j), & \beta(i) \neq \gamma(j), \\ \gamma(i) \neq \alpha(j), & \gamma(i) \neq \beta(j), & \gamma(i) \neq \gamma(j). \end{array}$$

In particular the list $\alpha(1), \ldots, \alpha(n)$ is a permutation of the elements $1, \ldots, n$. We know that $\alpha(1)$, $\beta(1)$, $\gamma(1)$ are not all equal, say $\alpha(1) \neq \beta(1)$. Since $\alpha(1), \ldots, \alpha(n)$ is a permutation of $1, \ldots, n$, there is an i, $2 \leq i \leq n$ such that $\alpha(i) = \beta(1)$. This contradicts to $\alpha(i) \neq \beta(j)$.

The proof is complete. □

References

[1] K. Corrádi, S. Szabó, and P. Z. Hermann, A character free proof for Rédei's theorem, *Mathematica Pannonica* **20** (2009), 3–15.

[2] L. Rédei, Die neue Theorie der endlichen Abelschen Gruppen und Verallgemeinerung des Hauptsatzes von Hajós, *Acta Math. Acad. Sci. Hung.*, **16** (1965), 329–373.

[3] A. D. Sands and S. Szabó, Factorization of periodic subsets, *Acta Math. Acad. Sci. Hungar.* **57** (1991), 159–167.