Open Journal of Discrete Mathematics, **2011, 1, 1-5**
doi: 10.4236/ojdm.2011.11001 Published Online April 2011 (http://www.SciRP.org/journal/ojdm)

Factoring Elementary *p*-Groups for $p \le 7$

Sándor Szabó
Institute of Mathematics and Informatics, University of Pécs, Ifjúság, Pécs, Hungary
E-mail: *sszabo7@hotmail.com*
Received March 10, 2011; *revised March* 20, 2011; *accepted April* 5, 2011

Abstract

It is an open problem if an elementary *p*-group of rank $k \ge 3$ does admit full-rank normalized factorization into two of its subsets such that one of the factors has *p* elements. The paper provides an answer in the $p \le 7$ special case.

Keywords: Factorization of Finite Abelian Groups, Full-Rank Subset, Full-Rank Factorization, Periodic Subset, Periodic Factorization, Rédei's Conjecture, Corrádi's Conjecture

1. Introduction

Let *G* be a finite abelian group. We use multiplicative notation in connection with abelian groups and *e* will denote the identity element of *G*. For two subset *A* and *B* of *G* the product *AB* is defined to be consisting of all the elements *ab*, where $a \in A$, $b \in B$. If

$$a_1 b_1 = a_2 b_2,\ \ a_1, a_2 \in A,\ b_1, b_2 \in B$$

imply $a_1 = a_2$, $b_1 = b_2$, then we say that the product *AB* is direct. If the product *AB* is direct and is equal to *G*, then the equation $G = AB$ is called a factorization of *G*.

We say that a subset *A* of *G* is normalized if $e \in A$. The factorization $G = AB$ is called a normalized factorization if the factors *A* and *B* are normalized. A normalized subset *A* of *G* is termed a full-rank subset of *G* if $\langle A \rangle = G$. Here $\langle A \rangle$ denotes the span of *A* in *G*. In other words $\langle A \rangle$ is the smallest subgroup of *G* containing *A*. A normalized factorization $G = AB$ is called a full-rank factorization if the factors *A* and *B* are full-rank subsets of *G*.

Let *p* be a prime and let *k* be a positive integer. A group that is a direct product of *k* cyclic groups of order *p* is called an elementary *p*-group of rank *k*. In 1970 in the open problems section in his book [4] L. Rédei advanced the following conjecture.

Conjecture 1 *Let p be a prime. An elementary p-group of rank* 3 *does not admit any full-rank factorization.*

Let $G = AB$ be a normalized factorization, where *G* is an elementary *p*-group of rank 3. One of the factors *A* and *B* must have *p* elements while the other factor must have p^2 elements. A normalized subset of order *p* in the $p = 3$ case cannot contain three generator elements of the group. Thus Rédei's conjecture holds for $p = 3$ and for the remaining part we may restrict our attention to the $p \ge 5$ case.

In 1998 S. Szabó and C. Ward [7] carried out a computer assisted exhaustive search to verify Rédei's conjecture for $p \le 11$. In a private conversation K. Corrádi proposed the following generalization to Rédei's conjecture.

Conjecture 2 *Let p be a prime and let G be an elementary p-group of rank* $k \ge 3$. *If* $G = AB$ *is a normalized factorization of G such that* $|A| = p$ *and* $|B| = p^{k-1}$, *then at least one of the factors does not span G.*

The normalized factor *A* can contain only $p-1$ generator elements of *G* and so the generalized conjecture certainly holds for $k > p-1$ and so it is enough to deal with the $3 \le k \le p-1$ case.

In this note we verify Corrádi's conjecture for $p \le 7$.

2. The $k = 3$ Case

At certain points in this paper we rely on some elementary concepts of graph theory. We presents these here. Let Γ be a simple graph, that is, Γ does not have double edges or loops. The set of vertices of Γ is denoted by *V*. Suppose *U* is a subset of *V*. If each two distinct elements of *U* are always connected in Γ by an edge of Γ, then the subgraph Δ of Γ spanned by *U* is called a clique of Γ. The set of vertices of Δ is *U*. If *U* has *k* elements, then we say that Δ is a clique of size *k* of Γ. Sometimes we express this fact simply by saying the Δ is a *k*-clique of Γ. The following problem is called the listing version of the *k*-clique problem.

Problem 1 *Given a finite simple graph* Γ *and a positive integer k. List all k-cliques of* Γ.

By the complexity theory of computation, Problem 1 belongs to the NP complete complexity class. Loosely speaking Problem 1 is computationally hard. We will solve two instances of the k-clique problem. In these cases the sizes of Γ are not overly large and the existing algorithms presented in [1,3] can handle them.

Let p be a prime and let G be an elementary p-group of rank 3 with basis elements x_1, x_2, x_3, where $|x_1| = |x_2| = |x_3| = p$. Let $G = AB$ be a normalized factorization of G such that $|A| = p$, $|B| = p^2$.

Proposition 1 *For* $p \le 7$, $\langle A \rangle = G$ *implies that B is a subgroup of G.*

Proof. As $\langle A \rangle = G$, we may choose the basis elements x_1, x_2, x_3 such that $x_1, x_2, x_3 \in A$. We will work with the subset $A_1 = \{a_1, a_2, a_3, a_4\}$ of A, where

$$a_1 = e, a_2 = x_1, a_3 = x_2, a_4 = x_3.$$

For each i, j, $1 \le i < j \le 4$ we set $H_{i,j} = \langle a_i a_j^{-1} \rangle$. Choose an $a_j \in A_1$. Multiplying the factorization $G = AB$ by a_j^{-1} gives the normalized factorization $G = Ga_j^{-1} = (Aa_j^{-1})B$. By Lemma 5 of [2], in the factorization $G = (Aa_j^{-1})B$ the factor Aa_j^{-1} can be replaced by $H_{i,j}$ to get the normalized factorization $G = H_{i,j}B$. Since the product $H_{i,j}B$ is direct, by Lemma 2.1 of [6],

$$H_{i,j}H_{i,j}^{-1} \cap BB^{-1} = \{e\}.$$

Plainly, $H_{i,j}H_{i,j}^{-1} = H_{i,j}$ and so

$$H_{i,j} \cap BB^{-1} = \{e\}$$

holds for each i, j, $1 \le i < j \le 4$. Set

$$T = \bigcup_{1 \le i < j \le 4} H_{i,j}.$$

Clearly, $T \cap BB^{-1} = \{e\}$. We define a graph Γ. The nodes of Γ are the elements of G. Two nodes $g, h \in G$ are connected if $gh^{-1} \notin T$. We may call T a test set since we use it for testing if a pair $\{g, h\}$ is an edge of Γ.

The graph Γ has $|G| = p^3$ nodes. We focus our attention on cliques of size p^2 in Γ. The reason is the following. If the products $H_{i,j}B$ are direct for each i, j, $1 \le i < j \le 4$, then $T \cap BB^{-1} = \{e\}$ and so the elements of B form the nodes of a clique of size p^2 in Γ. Conversely, if the elements of B are the nodes of a clique of size p^2 in Γ, then $T \cap BB^{-1} = \{e\}$ and hence the products $H_{i,j}B$ are direct for each i, j, $1 \le i < j \le 4$.

We call a clique normalized if e is one of its nodes. A computer assisted inspection reveals that each normalized cliques of size p^2 in Γ is a subgroup of G.

One can draw the following conclusion. If $G = AB$ is a normalized factorization of G, where $x_1, x_2, x_3 \in A$, then B must be a subgroup of G.

This completes the proof. □

For $p = 5$ the graph Γ has $5^3 = 125$ nodes. The search found 30 cliques of size $5^2 = 25$. Each of them was a coset modulo some subgroup of order 25 of G. (The subgroup that plays the role of the modulus of course may vary from case to case.) In particular the normalized cliques of size 25 in Γ correspond to subgroups of G.

For $p = 7$ the graph Γ has $7^3 = 343$ nodes. The inspection gave 140 cliques of size $7^2 = 49$. Each of them turned out to be a coset modulo some subgroup of order 49.

For $p = 11$ the graph Γ does contain normalized cliques of size 11^2 that are not subgroups of G. So our approach to verify Rédei's conjecture (or Corrádi's conjecture) breaks down for $p \ge 11$.

The above mentioned computer searches are not particularly demanding in terms of the time of computation. However, one cannot be cautious enough in connection with computer aided proofs. Therefore, in order to be on the safe side we used the algorithms described in [1,3] respectively as these algorithms have well tested implementations.

One can view the elements of G as points of the 3-dimensional affine space $[\mathrm{GF}(p)]^3$. Using geometrical terminology one can say that for $p \le 7$ a clique of size p^2 in Γ is a 2-dimensional linear complex in $[\mathrm{GF}(p)]^3$. A 2-dimensional linear complex is a translated copy of some 2-dimensional subspace of $[\mathrm{GF}(p)]^3$.

3. The *k* = 4 Case

Let p be a prime and let G be an elementary p-group of rank 4 with basis elements $x_1, \cdots, x_4$, where $|x_1| = \cdots = |x_4| = p$. Let $G = AB$ be a normalized factorization of G such that $|A| = p$, $|B| = p^3$.

Proposition 2 *For* $p \le 7$, $\langle A \rangle = G$ *implies that B is a subgroup of G.*

Proof. We may assume that $x_1, \cdots, x_4 \in A$ since this is only a matter of choosing the basis elements $x_1, \cdots, x_4$ suitably. We set $A_1 = \{a_1, \cdots, a_5\}$, where

$$a_1 = e, a_2 = x_1, \cdots, a_5 = x_4.$$

We know that $A_1 \subseteq A$. For each $\underline{i}$, j, $1 \le i < j \le 5$ we set $H_{i,j} = \langle a_i a_j^{-1} \rangle$. By Lemma 5 of [2], in the factorization $G = AB$ the factor A can be replaced by $H_{i,j}$ to get the normalized factorization $G = H_{i,j}B$. As the product $H_{i,j}B$ is direct, by Lemma 2.1 of [6], it follows that

$$H_{i,j} \cap BB^{-1} = \{e\} \tag{1}$$

for each $\underline{i}, j$, $1 \le i < j \le 5$.

We partition B into subsets $B_0, B_1, \cdots, B_{p-1}$. Each

$b \in B$ can be represented uniquely in the form

$$b = x_1^{\beta(1)} \cdots x_4^{\beta(4)},\ \ 0 \le \beta(1), \cdots, \beta(4) \le p-1. \quad (2)$$

The set B_i consists of each $b \in B$ for which $\beta(4) = i$. Note that

$$\begin{aligned} BB^{-1} &= (B_0 \cup \cdots \cup B_{p-1})(B_0 \cup \cdots \cup B_{p-1})^{-1} \\ &= (B_0 \cup \cdots \cup B_{p-1})(B_0^{-1} \cup \cdots \cup B_{p-1}^{-1}) \\ &\supseteq B_0 B_0^{-1} \cup \cdots \cup B_{p-1} B_{p-1}^{-1}. \end{aligned}$$

In particular it follows that $B_k B_k^{-1} \subseteq BB^{-1}$. We use now equations (1) only for i, j, $1 \le i < j \le 4$ to conclude that

$$H_{i,j} \cap B_k B_k^{-1} = \{e\} \quad (3)$$

holds for each i, j, k, $1 \le i < j \le 4$, $0 \le k \le p-1$.

Set $L_4 = \langle x_1, x_2, x_3 \rangle$. (The index 4 intends to indicate that x_4 is missing from the basis $x_1, \cdots, x_4$ in the definition of L_4.) Set

$$T_4 = \bigcup_{1 \le i < j \le 4} H_{i,j}.$$

Obviously $T_4 \cap B_k B_k^{-1} = \{e\}$. We define a graph Γ_4. The nodes of Γ_4 are the elements of L_4. Two nodes $g, h \in L_4$ are connected if $gh^{-1} \notin T_4$.

The graph Γ_4 has $|L_4| = p^3$ nodes. In addition $T_4 \subseteq L_4$ and $B_k B_k^{-1} \subseteq L_4$. Note that Γ_4 is isomorphic to the graph Γ used in the proof of Proposition 1. Consequently the nodes of a clique of size p^2 in Γ_4 form a 2-dimensional linear complex in $[\mathrm{GF}(p)]^4$.

From (3) one can see that $T_4 \cap B_k B_k^{-1} = \{e\}$ and consequently the elements of B_k form the nodes of a clique of size p^2 in Γ_4. Using geometrical terminology one may say that B_k is a 2-dimensional linear complex in $[\mathrm{GF}(p)]^4$.

We set out now to prove that the union of the p disjoint 2-dimensional linear complexes $B_0, B_1, \cdots, B_{p-1}$ forms a 3-dimensional linear complex. This will show that B is in fact a subgroup of G of order p^3.

We partition B into $C_0, C_1, \cdots, C_{p-1}$. Each $b \in B$ can be represented uniquely in the form (9). The set C_i contains each $b \in B$ for which $\beta(1) = i$. Note that

$$\begin{aligned} BB^{-1} &= (C_0 \cup \cdots \cup C_{p-1})(C_0 \cup \cdots \cup C_{p-1})^{-1} \\ &= (C_0 \cup \cdots \cup C_{p-1})(C_0^{-1} \cup \cdots \cup C_{p-1}^{-1}) \\ &\supseteq C_0 C_0^{-1} \cup \cdots \cup C_{p-1} C_{p-1}^{-1}. \end{aligned}$$

Therefore in particular $C_k C_k^{-1} \subseteq BB^{-1}$ holds. We use now equations (1) only for i, j, $2 \le i < j \le 5$ to conclude that

$$H_{i,j} \cap C_k C_k^{-1} = \{e\} \quad (4)$$

holds for each i, j, k, $2 \le i < j \le 5$, $0 \le k \le p-1$.

Set $L_1 = \langle x_2, x_3, x_4 \rangle$. (The meaning of the index 1 is that x_1 is missing from the basis $x_1, \cdots, x_4$ in the definition of the subgroup L_1.) Set

$$T_1 = \bigcup_{2 \le i < j \le 5} H_{i,j}.$$

Plainly $T_1 \cap C_1 C_1^{-1} = \{e\}$. We define a graph Γ_1. The nodes of Γ_1 are the elements of L_1. Two nodes $g, h \in L_4$ are connected if $gh^{-1} \notin T_1$.

The graph Γ_1 has $|L_1| = p^3$ nodes. In addition $T_1 \subseteq L_1$ and $C_k C_k^{-1} \subseteq L_1$. Therefore, in fact Γ_1 is isomorphic to the graph Γ we defined in the proof of Proposition 1. From (4) it follows that $T_1 \cap C_k C_k^{-1} = \{e\}$ and so C_k is a 2-dimensional linear complex in $[\mathrm{GF}(p)]^4$.

Let us observe that $B_0 \cap C_0$ is a subgroup of G of order p. Using geometrical terminology $B_0 \cap C_0$ is a 1-dimensional linear complex in $[\mathrm{GF}(p)]^4$. We may view B_0 as a union of p disjoint 1-dimensional linear complexes. Similarly, we may view C_0 as a union of p disjoint 1-dimensional complexes. In addition each of these linear complexes is a translated copy of $B_0 \cap C_0$. Using the 1-dimensional linear complexes

$$B_1 \cap C_0, B_2 \cap C_0, \cdots, B_{p-1} \cap C_0$$

analogously we can conclude that B is a union of p^2 disjoint 1-dimensional complexes each of which is a translated copy of $B_0 \cap C_0$. The translation vectors form a 2-dimensional linear complex. Therefore B is a 3-dimensional linear complex in $[\mathrm{GF}(p)]^4$.

This completes the proof. □

For the $k = 6$ case we need a corollary of Proposition 2. Set

$$T = \bigcup_{1 \le i < j \le 5} H_{i,j}$$

and define a graph Γ. The nodes of Γ are the elements of G. Two nodes $g, h \in G$ are connected if $gh^{-1} \notin T$.

Corollary 1 *Each clique of size p^3 in Γ corresponds to a 3-dimensional linear complex in $[\mathrm{GF}(p)]^4$.*

4. The $k \ge 5$ Case

Let p be a prime and let G be an elementary p-group of rank 5 with basis elements $x_1, \cdots, x_5$, where $|x_1| = \cdots = |x_5| = p$. Let $G = AB$ be a normalized factorization of G such that $|A| = p$, $|B| = p^4$.

Proposition 3 *For $p \le 7$, $\langle A \rangle = G$ implies that B is a subgroup of G.*

Proof. The proof is similar to the proof of Proposition 2 and we just outline the argument. It may be assumed that $x_1, \cdots, x_5 \in A$. We set $A_1 = \{a_1, \cdots, a_6\}$, where

$$a_1 = e, a_2 = x_1, \cdots, a_6 = x_5.$$

Clearly $A_1 \subseteq A$. For each $i, j,\ 1 \le i < j \le 6$ we set $H_{i,j} = \langle a_i a_j^{-1} \rangle$. From the factorization $G = AB$ we get the normalized factorization $G = H_{i,j}B$. From the directness of the product $H_{i,j}B$ it follows that

$$H_{i,j} \cap BB^{-1} = \{e\} \tag{5}$$

for each $i, j,\ 1 \le i < j \le 6$.

We partition B into subsets $B_0, B_1, \cdots, B_{p-1}$, Each $b \in B$ can be represented uniquely in terms of the basis $x_1, \cdots, x_5$ in the form

$$b = x_1^{\beta(1)} \cdots x_5^{\beta(5)},\ \ 0 \le \beta(1), \cdots, \beta(5) \le p-1 \tag{6}$$

The set B_i consists of each $b \in B$ for which $\beta(5) = i$. It follows that $B_k B_k^{-1} \subseteq BB^{-1}$. The equations (5) for $i, j,\ 1 \le i < j \le 5$ give that

$$H_{i,j} \cap B_k B_k^{-1} = \{e\} \tag{7}$$

for each $i, j, k,\ 1 \le i < j \le 5,\ 0 \le k \le p-1$.

Set $L_5 = \langle x_1, \cdots, x_4 \rangle$ and

$$T_5 = \bigcup_{1 \le i < j \le 5} H_{i,j}.$$

We define a graph Γ_5. The nodes of Γ_5 are the elements of L_5. Two nodes $g, h \in L_5$ are connected if $gh^{-1} \notin T_5$. Note that Γ_5 is isomorphic to the graph Γ in Corollary 1. From (7) one can see that the elements of B_k form the nodes of a clique of size p^3 in Γ_5 and so B_k is a 3-dimensional linear complex in $[\mathrm{GF}(p)]^5$.

Next we partition B into $C_0, C_1, \cdots, C_{p-1}$, where C_i contains each $b \in B$ for which $\beta(1) = i$ in the representation (6). A routine computation shows that $C_k C_k^{-1} \subseteq BB^{-1}$ The equations (5) for $i, j,\ 2 \le i < j \le 6$ imply that

$$H_{i,j} \cap C_k C_k^{-1} = \{e\} \tag{8}$$

for each $i, j, k,\ 2 \le i < j \le 6,\ 0 \le k \le p-1$.

Set $L_1 = \langle x_2, \cdots, x_5 \rangle$ and

$$T_1 = \bigcup_{2 \le i < j \le 6} H_{i,j}.$$

We define a graph Γ_1. The nodes of Γ_1 are the elements of L_1. Two nodes $g, h \in L_1$ are connected if $gh^{-1} \notin T_1$. Let us observe that Γ_1 is isomorphic to the graph Γ in Corollary 1. From (8) it follows that C_k is a 3-dimensional linear complex in $[\mathrm{GF}(p)]^5$.

Using the fact that $B_0 \cap C_0$ is a subgroup of G of order p^2 one can show that B is a 4-dimensional linear complex in $[\mathrm{GF}(p)]^5$.

This completes the proof. □

For the $k = 6$ case we need a corollary of Proposition 3. Set

$$T = \bigcup_{1 \le i < j \le 6} H_{i,j}$$

and define a graph Γ. The nodes of Γ are the elements of G. Two nodes $g, h \in G$ are connected if $gh^{-1} \notin T$.

Corollary 2 *Each clique of size p^4 in Γ corresponds to a 4-dimensional linear complex in $[\mathrm{GF}(p)]^5$.*

Let p be a prime and let G be an elementary p-group of rank 6 with basis elements $x_1, \cdots, x_6$, where $|x_1| = \cdots = |x_6| = p$. Let $G = AB$ be a normalized factorization of G such that $|A| = p$, $|B| = p^5$.

Proposition 4 *For $p \le 7$, $\langle A \rangle = G$ implies that B is a subgroup of G.*

Proof. The proof is similar to the proof of Proposition 3 and we do not detail it. □

We spell out the main result of this note formally as a theorem.

Theorem 1 *Let G be a finite elementary p-group, where p is a prime and let $G = AB$ be a normalized factorization such that $|A| = p$. If $p \le 7$, then either $\langle A \rangle \ne G$ or $\langle B \rangle \ne G$.*

5. An Application

Let G be a finite abelian group and let A be a subset of G. We say that the subset A is periodic if there is an element $g \in G$ such that $gA = G$ and $g \ne e$. A factorization $G = AB$ is called periodic if the factors A and B are both periodic. A. D. Sands has proved the following lemma. (See Lemma 3 of [5].)

Lemma 1 *Let $G = AB$ be a factorization of a finite abelian group G such that $|A| \ge 2$, $|B| \ge 2$. If $\min\{|A|, |B|\} \le 3$, then the factorization $G = AB$ is periodic.*

Motivated by this result we prove the next theorem.

Theorem 2 *Let $G = AB$ be a normalized factorization of a finite abelian group G such that $|A| = p$ is a prime and $|B| \ge 2$. If $p \le 7$, then either $\langle A \rangle \ne G$ or B is periodic.*

Proof. Let $p \le 7$ be a prime and consider a normalized factorization $G = AB$ of a finite abelian group G such that $|A| = p$, $|B| \ge 2$ and $\langle A \rangle = G$. We claim that B is periodic.

If $|A| \le 2$ or $|A| \le 3$, then by Sands' lemma it follows that either A or B is periodic. Thus for the remaining part of the proof we may assume that $|A| = 5$ or $|A| = 7$.

Choose an element $a \in A/\{e\}$. By Lemma 5 of [2], in the factorization $G = AB$ the factor A can be replaced by $A' = \{e, a, a^2, \cdots, a^{p-1}\}$ to get the normalized factorization $G = AB$. This factorization is equivalent to the fact that the sets

$$eB, aB, a^2B, \cdots, a^{p-1}B \tag{9}$$

form a partition of G. Multiplying the factorization $G = A'B$ by the element a we get the normalized factorization $G = Ga = (A'a)B$. This factorization is equivalent to the fact that the sets

$$aB, a^2B, a^3B, \cdots, a^pB \tag{10}$$

form a partition of G. Comparing the partitions (9) and (10) provides that $eB = a^pB$. Therefore, if $a^p \neq e$, then B is periodic. Thus for the remaining part of the proof we may assume that $a^p = e$ for each $a \in A/\{e\}$. As $G = \langle A \rangle$, it follows that G is an elementary p-group. From the factorization $G = AB$, by Theorem 1, it follows that either $\langle A \rangle \neq G$ or $\langle B \rangle \neq G$. Using $G = \langle A \rangle$ we get that $\langle B \rangle \neq G$.

The reader can check that in the course of the proof of Theorem 1 we obtained the following side result. Let G be a finite elementary p-group where $p \leq 7$ is a prime. If $G = AB$ is a normalized factorization such that $|A| = p$ and $\langle A \rangle = G$, then B is a subgroup of G. Clearly, a subgroup B of G is a periodic subset unless $|B| = 1$. But in our case, by the hypotheses of the theorem, $|B| \geq 2$ holds.

This completes the proof. □

6. References

[1] R. Carraghan and P. M. Pardalos, "An exact algorithm for the maximum clique problem," *Operation Research Letters* **9** (1990), 375-382. doi:10.1016/0167-6377(90)90057-C

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

[3] P. R. J. Östergå rd, "A fast algorithm for the maximum clique problem," *Discrete Applied Mathematics* **120** (2002), 195-205.

[4] L. Rédei, *Lückenhafte Polynome über endlichen Körpern*, Birkhäuser Verlag, Basel 1970, (English translation: *Lacunary Polynomials over Finite Fields*, North-Holland, Amsterdam, 1973.)

[5] A. D. Sands, "On the factorisation of finite abelian groups," *Acta Math. Acad. Sci. Hung.* **8** (1957), 65-86. doi:10.1007/BF02025232

[6] S. Szabó and A. D. Sands, "Factoring Groups into Subsets," CRC Press, Taylor and Francis Group, Boca Raton, 2009.

[7] S. Szabó and C. Ward, "Factoring elementary groups of prime cube order into subsets," *Mathematics of Computation* **67** (1998), 1199-1206. doi:10.1090/S0025-5718-98-00929-6

