Mathematica Pannonica
20/1 (2009), 1–13

A CHARACTER FREE PROOF FOR RÉDEI'S THEOREM

Keresztély **Corrádi**

Department of General Computer Technics, Eötvös L. University, Pázmány P. sétány 1/c, H–1117 Budapest, Hungary

Sándor **Szabó**

Department of Mathematics, Institute of Mathematics and Informatics, University of Pécs, Ifjúság u. 6, H–7624 Pécs, Hungary

Péter **Hermann**

Department of Algebra and Number Theory, Eötvös L. University, Kecskeméti u. 10–12, H–1053 Budapest, Hungary

Received: March 2008

MSC 2000: ??

Keywords: ??

Abstract: The paper gives a proof for Rédei's theorem on factoring finite abelian groups by its subsets and the proof does not depend on group characters.

1. Introduction

Let G be a finite abelian group written multiplicatively with identity element e. Let $A_1, \dots, A_n$ be subsets of G. If the product $A_1 \cdots A_n$ is direct and is equal to G, then we say that G is factored into subsets

E-mail addresses: ?

$A_1, \dots, A_n$. We also express this fact saying that the equation $G =$ $= A_1 \cdots A_n$ is a factorization of G. Clearly, $G = A_1 \cdots A_n$ is a factorization of G if and only if each element g of G is uniquely expressible in the form

$$g = a_1 \cdots a_n, \qquad a_1 \in A_1, \dots, a_n \in A_n.$$

The set of elements $e, a, a^2, \dots, a^{m-1}$ of G is called a cyclic subset of G. In order to solve a long standing geometric conjecture of H. Minkowski in 1941 G. Hajós proved that if $G = A_1 \cdots A_n$ is a factorization of G, where each A_i is a cyclic subset and each $|A_i|$ is a prime number, then at least one of the factors $A_1, \dots, A_n$ is a subgroup of G. His proof based on a zero divisor investigation in the group ring of G. L. Rédei was looking for a purely group theoretical proof which does not rely on group rings. Subsequently he developed a technique of substituting factors in a factorization and in 1965 using this technique he proved the following generalization of Hajós' theorem. If $G = A_1 \cdots A_n$ is a factorization of a finite abelian group G such that $|A_i|$ is a prime and $e \in A_i$ for all i, $1 \leq i \leq n$, then at least one of the factors $A_1, \dots, A_n$ is a subgroup of G. Rédei's technique of substitutions uses characters of G. We will give a character free proof for Rédei's theorem. The basic strategy, as in Rédei's original argument, is based on substitutions. The main achievement is the realization that the necessary substitution results can be established without resorting on characters. We drew on many ideas scattered widely in the literature. We will attribute the sources at appropriate places.

2. Replacement results

Let $G = AB$ be a factorization of G. Then each $g \in G$ is uniquely expressible in the form $g = ab$, $a \in A$, $b \in B$. We call a the A-component of g and we denote it by $g_{|A}$. Similarly, we call b the B-component of g and we denote it by $a_{|B}$. The components of g are meaningful only relative to the factorization $G = AB$.

Lemma 1. *Let $G = AB$ be a factorization of G and let $A = \{a_1, \dots, a_n\}$. For each $g \in G$ the elements $(ga_1)_{|A}, \dots, (ga_n)_{|A}$ form a permutation of $a_1, \dots, a_n$.*

Proof. Clearly, $(ga_i)_{|A} \in A$. So we will show that $(ga_i)_{|A} = (ga_j)_{|A}$ implies $a_i = a_j$. From

$$ga_i = (ga_i)_{|A}(ga_i)_{|B}, \quad ga_j = (ga_j)_{|A}(ga_j)_{|B}$$

we get

$$g = (ga_i)_{|A}(ga_i)_{|B}a_i^{-1}, \quad g = (ga_j)_{|A}(ga_j)_{|B}a_j^{-1}.$$

Then $(ga_i)_{|B}a_i^{-1} = (ga_j)_{|B}a_j^{-1}$ and $a_j(ga_i)_{|B} = a_i(ga_j)_{|B}$. Now as $a_i, a_j \in$ $\in A$ and $(ga_i)_{|B}, (ga_j)_{|B} \in B$ it follows that $a_i = a_j$. $\diamondsuit$

Lemma 2. *If $G = AB$ is a factorization of G, then $G = A^{-1}B$ is a factorization of G.*

Proof. We will show that the product $A^{-1}B$ is direct. Choose $a_1, a_2 \in A$, $b_1, b_2 \in B$ and assume that $a_1^{-1}b_1 = a_2^{-1}b_2$. From this we get $a_2b_1 = a_1b_2$ which in turn implies $a_1 = a_2$ and $b_1 = b_2$. $\diamondsuit$

Lemma 3. *Let $G = AB$ be a factorization of G and let q be a prime such that $q \not| |A|$. Then $G = A^qB$ is a factorization of G.*

Proof. Choose $a \in A$, $g \in G$ and define T to be the set of all q tuples

$$(x_1, x_2, \ldots, x_q), \quad x_1, x_2, \ldots, x_q \in A$$

for which $(gx_1x_2\cdots x_q)_{|A} = a$. First note that $|T| = |A|^{q-1}$. For choose $x_1, x_2, ..., x_{q-1}$ in A arbitrarily, then by Lemma 1, $[(gx_1x_2\cdots x_{q-1})x_q]_{|A} = a$ has a unique solution for x_q. Next note that if $(x_1, x_2, \ldots, x_q) \in T$, then $(x_2, \ldots, x_q, x_1) \in T$. We define a graph Γ. The vertices of Γ are the elements of T and we draw an arrow from the node $(x_1, x_2, \ldots, x_q)$ to the node $(x_2, \ldots, x_q, x_1)$. The graph Γ is a union of disjoint cycles. The cycles are of length 1 or of length q. When $x_1 = x_2 = \cdots = x_q$, then the node $(x_1, x_2, \ldots, x_q)$ is on a cycle of length 1. When $x_1, x_2, \ldots, x_q$ are not all equal, then the node $(x_1, x_2, \ldots, x_q)$ is on a cycle of length q. As $q \not| |A|$ there must be a cycle of length 1 in Γ. In other words there is an $x_1 \in A$ such that $(gx_1^q)_{|A} = a$. In addition x_1 is uniquely determined by a and g. As the last step of the proof we claim that the product A^qB is direct. Suppose that $a_1^qb_1 = a_2^qb_2$, $a_1, a_2 \in A$, $b_1, b_2 \in B$. Then $a_1^qb_2^{-1} =$ $= a_2b_1^{-1}$. There are $a \in A$, $b \in B$ such that $a_1^qb_2^{-1} = a^qb_1^{-1} = ab$. From the equation $b^{-1}a_1^q = ab_2$ we get that $(b^{-1}a_1^q)_{|A} = a$. From the equation $b^{-1}a_2^q = ab_1$ we get $(b^{-1}a_2^q)_{|A} = a$. From $(b^{-1}a_1^q)_{|A} = (b^{-1}a_2^q)_{|A} = a$ we get $a_1 = a_2$ which in turn implies $b_1 = b_2$. $\diamondsuit$

Lemma 4. *Let $G = AB$ be a factorization of G and let k be an integer relatively prime to $|A|$. Then $G = A^kB$ is a factorization of G.*

Proof. The $k = -1, 0, 1$ cases do not require any proof so we assume that $k \leq -2$ or $k \geq 2$. If k is positive, then k is a product of positive primes and we can apply Lemma 3 several times starting with the factorization $G = AB$. If k is negative, then $-k$ is positive and we can use a similar procedure starting with the factorization $G = A^{-1}B$. $\diamondsuit$

Lemma 5. *Let $G = AB$ be a factorization such that $e \in A$, $|A| = p$ is a prime. Then $G = A'B$ is a factorization of G, where $A' = \{e, a, a^2, \ldots, a^{p-1}\}$, $a \in A \setminus \{e\}$.*

Proof. By Lemma 4, $G = A^tB$ is a factorization of G whenever $p \not| t$. Let $A = \{e, a_1, a_2, \ldots, a_{p-1}\}$. The fact that $G = A^tB$ is a factorization is equivalent to that the sets

$$eB, a_1^tB, a_2^tB, \ldots, a_{p-1}^tB$$

form a partition of G. Similarly, the fact that $G = A'B$ is a factorization is equivalent to that the sets

$$eB, a_kB, a_k^2B, \ldots, a_k^{p-1}B$$

form a partition of G. Here $A' = \{e, a_k, a_k^2, \ldots, a_k^{p-1}\}$. Since G is finite it is enough to show that $a_k^iB \cap a_k^jB = \emptyset$ for each i, j, $0 \leq i < j \leq p-1$. Assume the contrary that $a_k^iB \cap a_k^jB \neq \emptyset$. Multiplying by a_k^{-i} we get $eB \cap a_k^{j-i}B \neq \emptyset$. Set $t = j - i$. Clearly, $1 \leq t \leq p-1$ and so t is prime to p. Now $eB \cap a_k^tB \neq \emptyset$ contradicts the fact that $G = A^tB$ is a factorization of G. ♢

Lemma 6. *Let $G = AB$ be a factorization of G such that $|A| = p$ is a prime, $e \in A$. Further assume that A contains only (p,q)-elements. $A = \{e, a_1b_1, a_2b_2, \ldots, a_{p-1}b_{p-1}\}$, $|a_i| = p$, $|b_i| = 1$ or $|b_i| = q$ for each i, $1 \leq i \leq p-1$, $|b_1| = q$. Then $G = A'B$ is a factorization of G, where $A' = \{e, a_1, a_1^2, \ldots, a_1^{p-2}, a_1^{p-1}b_1\}$. ($A'$ differs from the subgroup $\langle a_1 \rangle$ in one element.)*

Proof. By Lemma 4, $G = A^qB$ is a factorization of G. Clearly, $a_1^q \in A^q$. There is an integer s such that $(a_1^q)^s = a_1$ as the congruence $qs \equiv 1 \pmod{p}$ is solvable for s. As s is prime to p by Lemma 4, $G = A^{qs}B$ is a factorization of G. From the factorization $G = A^{qs}B$ we get by Lemma 5 that $G = A_1B$ is a factorization of G, where $A_1 = \{e, a_1, a_1^2, \ldots, a_1^{p-1}\}$. The factorization $G = A_1B$ means that the sets

$$eB, a_1B, a_1^2B, \ldots, a_1^{p-1}B$$

form a partition of G. The factorization $G = A'B$ means that the sets

$$eB, a_1B, a_1^2B, \ldots, a_1^{p-2}B, a_1^{p-1}b_1B$$

form a partition of G. Since G is finite it is enough to show that the sets above are pair-wise disjoint. Namely, $a_1^iB \cap a_1^jB = \emptyset$ for each i, j, $0 \leq i < j \leq p-2$, $a_1^iB \cap a_1^{p-1}b_1B = \emptyset$ for each i, $0 \leq i \leq p-2$. The first set of equation holds. Suppose on the contrary that $a_1^iB \cap a_1^{p-1}b_1B \neq \emptyset$ for some i. Multiplying by a_1^{-i} we get $eB \cap a_1^{p-i-1}b_1B \neq \emptyset$. There is a t such that $(a_1^{p-i-1})b_1 = a_1^tb_1^t$ as the system of congruences

$$\begin{aligned} p-i-1 &\equiv t \pmod{p} \\ 1 &\equiv t \pmod{q} \end{aligned}$$

is solvable for t. We get now a contradiction considering the factorization $G = A^t B$. $\Diamond$

The result in Lemma 4 first was proved by L. Rédei in [5] using characters. The proof we presented is from A. D. Sands [6]. Lemma 5 is from L. Fuchs [1] and Lemma 6 is from S. Szabó [8].

3. Hajós' theorem for finite abelian p-groups

Lemma 7. *Let A be a subset of a finite abelian p-group G such that $\big|\langle A\rangle\big| = p^{|A|}$ and $\big|\langle B\rangle\big| \geq p^{|B|}$ holds for each $B \subset A$. Then for each $a \in A$ there is an $s(a)$ such that $s(a)$ is a power of p and*

$$\langle A\rangle = \prod_{a\in A}\big\{e, a^{s(a)}, a^{2s(a)}, \ldots, a^{(p-1)s(a)}\big\}$$

is a factorization of $\langle A\rangle$ and at least one of the factors is a subgroup of $\langle A\rangle$.

Proof. First consider the case when $|A| = 1$. Now $A = \{a\}$ and the order of a is p. So $\langle A\rangle = \{e, a, a^2, \ldots, a^{p-1}\}$. This shows that we can choose $s(1)$ to be 1. Let $h(A) = \prod_{a\in A} |a|$ be the height of the subset A. Clearly $h(A) \geq p^{|A|}$ and equation holds only when $|a| = p$ for each $a \in A$. In this case $\langle A\rangle$ is a direct product of $|A|$ copies of cyclic groups of order p and the consequence of the lemma holds. We start an induction on $n = |A|$ and for a given value of n we start an induction on the height $h(A)$. If for each subset B of A with $B \neq \emptyset$, $B \neq A$, $\big|\langle B\rangle\big| > p^{|B|}$ holds, then replace one element of A by its p-th power to get the set A'. The conditions of the lemma hold for A' and $h(A') < h(A)$. Note that $\langle A'\rangle =$ $= \langle A\rangle$. By induction on $h(A)$ we get that the lemma holds for $\langle A\rangle$. If there is a subset B of A with $B \neq \emptyset$, $B \neq A$ such that $\big|\langle B\rangle\big| = p^{|B|}$, then B satisfies the conditions of the lemma and $|B| < |A|$. Now by the inductive assumption on $|A|$, $\langle B\rangle$ has a factorization

$$\langle B\rangle = \prod_{b\in B}\big\{e, b^{s(b)}, b^{2s(b)}, \ldots, b^{(p-1)s(b)}\big\},$$

where $s(b)$ is a power of p and at least one of the factors is a subgroup of $\langle B\rangle$. Consider the factor group $G' = \langle A\rangle/\langle B\rangle$ and the subset $A' =$ $= \{a\langle B\rangle : a \in A \setminus B\}$ of G'. We can verify that $\big|\langle A'\rangle\big| = p^{|A'|}$ and $\big|\langle B'\rangle\big| \geq p^{|B'|}$ hold for all $B' \subset A'$. By induction on $|A|$ there is a factorization of $\langle A' \rangle$ described in the lemma. Using the factorization of $\langle B \rangle$ and the factorization of $G' = \langle A \rangle / \langle B \rangle$ we can construct the desired factorization of $\langle A \rangle$. $\Diamond$

Lemma 8. *Let $G = A_1 \cdots A_n$ be a factorization of a finite abelian p-group G, where $A_i = \{e, a_i, a_i^2, \dots, a_i^{p-1}\}$. Then at least one of the factors $A_1, \dots, A_n$ is a subgroup of G.*

Proof. Suppose that

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

is a factorization of the finite abelian p-group G and $A_i = \{e, a_i, a_i^2, \dots, a_i^{p-1}\}$ are cyclic subsets of G. Set $A = \{a_1, \dots, a_n\}$. Note that Lemma 7 is applicable to A. So for each i, $1 \leq i \leq n$ there is a power of p, say $s(i)$ and a subset

$$A_i' = \{e, a_i^{s(i)}, a_i^{2s(i)}, \dots, a_i^{(p-1)s(i)}\}$$

such that $G = A_1' \cdots A_n'$ is a factorization of G and at least one of the factors $A_1', \dots, A_n'$ is a subgroup of G. If $s(1) = \cdots = s(n)$, then $A_1 = = A_1', \dots, A_n = A_n'$ and so one of the factors $A_1, \dots, A_n$ is a subgroup of G. So for the rest of the proof we may assume that $s(i) \neq 1$ for some i, $1 \leq i \leq n$. In addition we may assume that $s(1) \neq 1, \dots, s(m) \neq 1$, $s(m+1) = \cdots = s(n) = 1$ and $m \geq 1$ since this is only a matter of rearranging the factors. Since $s(m+1) = \cdots = s(n) = 1$ we have that

$$G = A_1' \cdots A_m' A_{m+1} \cdots A_n$$

is a factorization of G. Consequently, the element $a_1 \cdots a_m$ of G can be represented in the form

$$a_1 \cdots a_m = a_1^{s(1)t(1)} \cdots a_m^{s(m)t(m)} a_{m+1}^{t(m+1)} \cdots a_n^{t(n)},$$

where $0 \leq t(i) \leq p-1$. So

$$e = a_1^{s(1)t(1)-1} \cdots a_m^{s(m)t(m)-1} a_{m+1}^{t(m+1)} \cdots a_n^{t(n)}. \tag{2}$$

As $s(i)$ is a power of p, it follows that $s(i)t(i)-1$ is relatively prime to p. By Lemma 4 the factor A_i can be replaced by the factor

$$A_i^* = \left\{e, a_i^{s(i)t(i)-1}, a_i^{2[s(i)t(i)-1]}, \dots, a_i^{(p-1)[s(i)t(i)-1]}\right\}$$

in the factorization (1) to get the factorization

$$G = A_1^* \cdots A_m^* A_{m+1} \cdots A_n.$$

Equation (2) violates this factorization unless $m = 0$. This completes the proof. $\Diamond$

Lemma 7 is from L. Rédei [5]. He used it to simplify the proof of Hajós' theorem.

4. Rédei's theorem for groups of type (p, p)

Let X be a subset of the affine plane $[\mathrm{GF}(p)]^2$. We say that X determines a direction if there are two points in X that span a line in this direction.

Lemma 9. *Let X be a subset of the affine plane $[\mathrm{GF}(p)]^2$ such that $|X| = p$ is a prime and X is not a straight line. Then X determines at least $(p+3)/2$ directions on the plane.*

Proof. If X determines all $p+1$ directions on the plane, then $p+1 \geq \geq (p+3)/2$ holds. So we may assume that X does not determine all directions. Consequently we may introduce a coordinate system in such a way that the direction of the second coordinate axis is not determined by X. Hence X can be represented in the form

$$X = \{(k, b_k) : k \in \mathrm{GF}(p)\},$$

where $b_0, \ldots, b_{p-1} \in \mathrm{GF}(p)$. ($\mathrm{GF}(p)$ is isomorphic to the field of integers modulo p. We identify $\mathrm{GF}(p)$ with this field using $0, 1, \ldots, p-1$ as elements of the field.) Let U be the collection of directions determined by X. It is convenient to record any direction with the slope of a representative straight line.

$$U = \left\{ \frac{b_k - b_m}{k - m} : k, m \in \mathrm{GF}(p), k \neq m \right\}.$$

In order to prove that $|U| \geq (p+3)/2$ we assume the contrary that $|U| < (p+3)/2$ and derive a contradiction. Consider the polynomials

$$F_j = \sum_{k \in \mathrm{GF}(p)} (b_k - kx)^j$$

in $\mathrm{GF}(p)[x]$ for $0 \leq j \leq p-2$. From

$$(3) \qquad \sum_{k \in \mathrm{GF}(p)} k^j = 0 \quad \text{if and only if} \quad j = 0 \quad \text{or} \quad (p-1) \not| j$$

it follows that $\deg F_j \leq j-1$ for $j \neq 0$. If $x \notin U$, then the elements $b_k - - kx$ are all distinct as k varies over $\mathrm{GF}(p)$. So $x \notin U$ implies $F_j(x) = 0$. Since $\deg F_j \leq j-1$ it follows that if $j-1 < p-|U|$, then F_j is the zero polynomial. In particular F_j is the zero polynomial when $j \leq (p-1)/2$. Using the fact that every function from $\mathrm{GF}(p)$ to $\mathrm{GF}(p)$ is a polynomial of degree less than or equal to $p-1$ we can represent b_k in the form

$$b_k = c_m k^m + \cdots + c_2 k^2 + c_1 k + c_0,$$

where $c_m \neq 0$. If $m \leq 1$, then X is a straight line. So we may assume that $2 \leq m \leq p-1$. (As a consequence we have assumed that $p \geq 3$.) Divide $p-1$ by m with remainder.

$$p-1=ma+b, \quad a\geq 1, \quad 0\leq b\leq m-1.$$

Note that $a+b\leq (p-1)/2$ as $m\geq 2$. So F_{a+b} is the zero polynomial. On the other hand we will show that F_{a+b} is not the zero polynomial. Let us compute the coefficient of $(-x)^b$ in F_{a+b}.

$$0=\sum_k \binom{a+b}{b} b_k^a k^b = \binom{a+b}{b}\sum_k (c_m^a k^{am+b}+\sum_{j=b}^{p-2} d_j k^j)$$

with some $d_j\in \mathrm{GF}(p)$. Using (3) we get that this coefficient is

$$\binom{a+b}{b} c_m^a \sum_k k^{p-1} = -\binom{a+b}{b} c_m^a \neq 0.$$

This completes the proof. ◊

Lemma 10. *If $G=AB$ is a factorization of the group G of type (p,p) such that $e\in A\cap B$, $|A|=|B|=p$, then A or B is a subgroup of G.*

Proof. Let u,v be basis elements of G. The correspondence $u^iv^j\to$ $\to (i,j)$ assigns points of the affine plane $[\mathrm{GF}(p)]^2$ to the elements of G. Subgroups of order p correspond to straight lines of the plane passing through the point $(0,0)$. The $p+1$ subgroups of order p of G correspond to the $p+1$ directions available on the plane. Suppose that the elements $a_1,a_2\in G$ correspond to the points $p_1,p_2\in[\mathrm{GF}(p)]^2$. Then the direction determined by the points p_1,p_2 corresponds to the subgroup $\langle a_1a_2^{-1}\rangle$ of G. Briefly, we will talk about the direction determined by a_1,a_2. Next we will show that if $G=AB$ is a factorization, then the directions determined by the elements of A are distinct from the directions determined by the elements of B. Assume that there are $a_1,a_2\in A$, $b_1,b_2\in B$ $a_1\neq a_2$, $b_1\neq b_2$ and $\langle a_1a_2^{-1}\rangle=\langle b_1b_2^{-1}\rangle$. Multiplying the factorization $G=AB$ by $a_2^{-1}b_2^{-1}$ we get the factorization $G=(Aa_2^{-1})(Bb_2^{-1})$. From this by Lemma 5 we get the factorization $G=\langle a_1a_2^{-1}\rangle\langle b_1b_2^{-1}\rangle$. But this is a contradiction as $\langle a_1a_2^{-1}\rangle=\langle b_1b_2^{-1}\rangle$. Since A and B determine distinct directions it follows that either A or B determines at most $(p+1)/2$ directions. By the previous result A or B is a subgroup of G. ◊

The result in Lemma 9 first was proved by L. Rédei in [4] as an application of his results on lacunary polynomials. The presented proof of Lemma 9 is from L. Lovász and A. Schrijver [3].

5. Rédei's theorem for finite abelian p-groups

Lemma 11. *Rédei's theorem holds for any finite abelian p-group.*

Proof. Let G be an abelian group of order p^n and let $G = A_1 \cdots A_n$ be a factorization of G, where $|A_1| = \cdots = |A_n| = p$ and $e \in A_1, \ldots, e \in A_n$. We want to show that at least one of the factors $A_1, \ldots, A_n$ is a subgroup of G. The $n = 1$ case is trivial. We may assume that $n \geq 2$. By Lemma 5 every factor A_i can be replaced by a cyclic subset. If A_i contains an element of order at least p^2, then A_i can be replaced by a non-subgroup cyclic subset. If each factor has an element of order at least p^2, then we can construct a factorization of G consisting of non-subgroup cyclic subsets. By Lemma 8 it is not possible. So there is a factor, say A_1, whose nonidentity elements all have order p. Using this observation we can settle the $n = 2$ case. Indeed, Lemma 10 takes care of the case when G is of type (p, p). When G is of type (p^2), then the $p - 1$ elements of G of order p together with e form a subgroup of G and A_1 is equal to this subgroup. We assume that $n \geq 3$ and start an induction on n. By Lemma 5 the factor A_1 can be replaced by a subgroup H in the factorization $G = A_1 A_2 \cdots A_n$ to get the factorization $G = HA_2 \cdots A_n$. Considering the factor group G/H we have the factorization $G/H = (A_2H)/H \cdots (A_nH)/H$. By the inductive assumption there is a permutation $B_1, \ldots, B_n$ of the factors $H, A_2, \ldots, A_n$ such that $B_1, B_1B_2, \ldots, B_1B_2 \cdots B_n$ is a ascending chain of subgroups of G and $B_1 = H$. For notational convenience we assume that $B_2 = A_2, \ldots, B_n = A_n$ since this is only a matter of reindexing the factors $A_2, \ldots, A_n$ in the factorization $G = A_1A_2 \cdots A_n$. Consider the subgroup $K = HA_2 \cdots A_{n-1}$. Clearly, each of the factors $H, A_2, \ldots, A_{n-1}$ is a subset of K. If $A_1 \subset K$, then $K = A_1A_2 \cdots A_{n-1}$ is a factorization of K. By the inductive assumption at least one of the factors $A_1, \ldots, A_{n-1}$ is a subgroup of K and so is a subgroup of G. For the remaining part of the proof we may assume that $A_1 \not\subset K$. Then replace the factor A_1 in the factorization $G = A_1A_2 \cdots A_n$ by a subgroup L generated by an element of $A_1 \setminus K$. Since $L \not\subset K$, we have $K \cap L = \{e\}$. Considering the factor group G/L from the factorization $G = LA_2 \cdots A_n$ by the inductive assumption it follows that there is a permutation $C_1, \ldots, C_n$ of the factors $L, A_2, \ldots, A_n$ such that $C_1, C_1C_2, \ldots, C_1C_2 \cdots C_n$ is an ascending chain of subgroups of G and $C_1 = L$. There is an index j such that $C_2 = A_j$ and so LA_j is a subgroup of G. If $j \neq n$, then $K \cap LA_j = A_j$ is a subgroup of G. Therefore for the remaining part of the proof we may assume that LA_n is a subgroup of G. Consider $K \cap LA_n$. If $K \cap LA_n = \{e\}$, then G contains the direct product of the subgroups K and LA_n. This would imply $|G| \geq p^{n+1}$ but we know that $|G| = p^n$. Thus $|K \cap LA_n|$ is p^2 or p. If $|K \cap LA_n| = p^2$, then $LA_n \subset K$. This gives $L \subset K$ which is not the case. Hence $|K \cap LA_n| = p$. We distinguish two cases depending on the type of LA_n. Suppose that LA_n is of type (p^2), that is, LA_n is cyclic. Then $K \cap LA_n$ is the unique subgroup of order p of LA_n, namely L. Since $L \not\subset K$ this case is ruled out. Since LA_n is not cyclic, the nonidentity elements of A_n have order p. Consequently A_n can be replaced by a subgroup M in the factorization $G = A_1 \cdots A_n$ to get the factorization $G = A_1 \cdots A_{n-1}M$. Similarly A_n can be replaced by M in the factorization $G = HA_2 \cdots A_n$ to get the factorization $G = HA_2 \cdots A_{n-1}M$. Note that $G = KM$ is also a factorization of G which implies that $K \cap$ $\cap M = \{e\}$. Considering the factor group G/M from the factorization $G = A_1 \cdots A_{n-1}M$ it follows that there is a permutation $D_1, \dots, D_n$ of the factors $A_1, \dots, A_{n-1}, M$ such that $D_1, D_1D_2, \dots, D_1D_2 \cdots D_n$ is an ascending chain of subgroups of G and $M = D_1$. There is an index j, $1 \leq j \leq n-1$ such that $D_2 = A_j$. Hence MA_j is a subgroup of G. If $j \neq 1$, then $A_j \subset K$. As $K \cap M = \{e\}$, we have that $K \cap MA_j = A_j$ is a subgroup of G. If $j = 1$, the we have that $N = MA_1$ is a subgroup of G. We distinguish two cases depending on $A_n \subset N$ or $A_n \not\subset N$. If $A_n \subset N$, then $A_1A_n \subset N$. Therefore A_1A_n forms a factorization of N. By Lemma 10, A_1 or A_n is a subgroup of N and hence A_1 or A_n is a subgroup of G. If $A_n \not\subset N$, then the factor A_n can be replaced by a subgroup T in $G = A_1 \cdots A_n$ to get the factorization $G = A_1 \cdots A_{n-1}T$, where $T \cap N = \{e\}$. Considering the factorization of the factor group G/T we get that there is a subgroup of G of the form TA_j, with some j, $1 \leq j \leq n-1$. Let us watch $K \cap TA_j = HA_2 \cdots A_{n-1} \cap TA_j$. We can argue as before. If $K \cap TA_j = \{e\}$, then G contains a subgroup of order p^{n+1}. If $K \cap TA_j = TA_j$, then we get the contradiction that $T \subset K$. Thus $|K \cap TA_j| = p$. If $j \neq 1$, then $K \cap TA_j = A_j$ which proves the lemma. If $j = 1$, then both TA_1 and $N = MA_1$ are subgroups of G. Recalling that $T \cap N = \{e\}$ we conclude that $TA_1 \cap N = A_1$ is a subgroup of G. This completes the proof. $\Diamond$

6. Periodic subsets

A subset A of a finite abelian group G is defined to be periodic if there exists an element g of $G \setminus \{e\}$ with $gA = A$. We refer to such elements g as periods of A. All the periods of A together with the identity element e form a subgroup of G. Consequently each periodic subset has a period of prime order.

Lemma 12. *A periodic subset of prime cardinality that contains the identity element is a subgroup.*

Proof. Let A be a periodic subset where $e \in A$ and $|A| = p$ is a prime. Let g be a period of A of prime order r. Consider the permutation of the elements of A defined by $x \to xg$, $x \in A$. This permutation can be decomposed into disjoint cycles of lengths r. Thus $r|p$ and hence $p = r$. So the permutation consists of only one cycle. Let $a \in A$ be the image of the identity element e, that is, let $ge = a$. Now the order of a is p and $A = \{e, a, a^2, \ldots, a^{p-1}\}$. $\Diamond$

Lemma 13. *If A is a nonempty subset of a finite abelian group, $e \in A$ and*

$$H = \bigcap_{a \in A} a^{-1}A \neq \{e\},$$

then A is periodic.

Proof. Let $A = \{a_1, \ldots, a_s\}$ and suppose that $g \in H \setminus \{e\}$. We will show that g is a period of A. There are elements $b_1, \ldots, b_s \in A$ such that $g = b_1a_1^{-1}, \ldots, g = b_sa_s^{-1}$. Since $b_1, \ldots, b_s$ are distinct elements they are all the elements of A. Consequently,

$$\begin{aligned} gA &= \{ga_1, \ldots, ga_s\} = \\ &= \{b_1a_1^{-1}a_1, \ldots, b_sa_s^{-1}a_s\} = \\ &= \{b_1, \ldots, b_s\} = \\ &= A. \qquad \Diamond \end{aligned}$$

7. Proof of Rédei's theorem

Theorem 1. *Let $G = A_1 \cdots A_n$ be a factorization of the finite abelian group G such that $e \in A_i$ and $|A_i|$ is a prime for each i, $1 \leq i \leq n$. Then at least one of the factors $A_1, \ldots, A_n$ is a subgroup of G.*

Proof. The theorem holds for $n = 1$. We start an induction on n and assume that $n \geq 2$. If $|G|$ is a power of 2, then by Lemma 8 at least one of the factors is a subgroup of G. So we may assume that $|G|$ has a prime factor p with $p \geq 3$ and suppose that $A_1, \ldots, A_t$ are all the factors among $A_1, \ldots, A_n$ with cardinality p. By Lemma 4 there is a factorization $G = = A'_1 \cdots A'_t A_{t+1} \cdots A_n$ of G such that A'_i contains only p-elements for each i, $1 \leq i \leq t$. Now $A'_1 \cdots A'_t$ is a factorization of the p-component of G. By Lemma 11 at least one of the factors $A'_1, \ldots, A'_t$ is a subgroup of the p-component of G and hence of G. Let A'_1 be this factor. If A_1 is a subgroup of G, then there is nothing to prove. So we may assume that A_1 contains not only p-elements. Again using Lemma 4, if necessary, we may assume that A_1 satisfies the conditions of Lemma 6. So there is a factorization $G = A_1 \cdots A_n$ such that A_1 is of the form

$$A_1 = \{e, x, x^2, \ldots, x^{p-2}, x^{p-1}y\}.$$

Let $H_1 = \langle x \rangle$. By Lemma 4 there is a factorization $G = H_1 A_2 \cdots A_n$ of G. From this we have the factorization

$$G/H_1 = (A_2 H_1)/H_1 \cdots (A_n H_1)/H_1$$

of the factor group G/H_1. By the inductive assumption on n we get that some factor $(A_i H_1)/H_1$ is a subgroup of G/H_1. We may assume that $i = 2$ since this is only a matter of indexing the factors. We consider a factor group again to get a new factorization. Continuing in this way we conclude that there is a subgroup M of G such that

$$M = H_1 A_2 \cdots A_{n-1}, \qquad G = M A_n$$

are factorizations of M and G respectively. Let $a \in A_n$. From the factorizations

$$\begin{aligned} G &= A_1 A_2 \cdots A_n, \\ G &= H_1 A_2 \cdots A_n, \\ G &= M A_n \end{aligned}$$

multiplying by a^{-1} we have the factorizations

$$\begin{aligned} G &= A_1 A_2 \cdots A_{n-1}(a^{-1} A_n), \\ G &= H_1 A_2 \cdots A_{n-1}(a^{-1} A_n), \\ G &= M(a_1^{-1} A_n). \end{aligned}$$

If $A_1 \subset M$, then $M = A_1 A_2 \cdots A_{n-1}$ is a factorization of M. By the inductive assumption at least one of the factors $A_1, \ldots, A_{n-1}$ is a subgroup of M and so of G. If $A_1 \not\subset M$, then by the factorization $G = M(a^{-1} A_n)$, $a^{-1} A_n$ is a complete set of representatives modulo M. Hence there exists an element c_a of $a^{-1} A_n$ such that the coset $c_a M$ contains the element $(x^{p-1}y)^{-1}$, that is, for which $x^{p-1} y c_a \in M$. Let

$$\begin{aligned} B_a &= \{x^{p-1}yc_a\} \cup \big(H_1 \setminus \{x^{p-1}y\}\big) = \\ &= \{x^{p-1}yc_a\} \cup \big(A_1 \setminus \{x^{p-1}y\}\big). \end{aligned}$$

Note that $M = B_a A_2 \cdots A_{n-1}$ is a factorization of M and each factor contains the identity element e. Indeed, products coming from $B_a A_2 \cdots A_{n-1}$ occur among the product coming from $A_1 A_2 \cdots A_{n-1}(a^{-1}A_n)$ and these are distinct since $G = A_1 A_2 \cdots A_{n-1}(a^{-1}A_n)$ is a factorization of G. From the factorization $M = B_a A_2 \cdots A_{n-1}$ by the inductive assumption it follows that one of the factors $B_a, A_2, \ldots, A_{n-1}$ is a subgroup of M and so of G. If it is not B_a we are done. Thus we may assume that B_a is a subgroup of G. As $p \geq 3$ it follows that $B_a = H_1$. Therefore $x^{p-1}yc_a = x^{p-1}$, that is, $c_a = y^{-1}$ and so $y^{-1} \in a^{-1}A_n$. Thus the fixed element y^{-1} which is not equal to e belongs to

$$\bigcap_{a \in A_n} a^{-1}A_n.$$

By Lemma 13, A_n is periodic. Then by Lemma 12, A_n is a subgroup of G. This completes the proof. ◊

References

[1] FUCHS, L.: Abelian Groups, Hung. Acad. of Sci., Budapest, 1958.

[2] HAJÓS, G.: Über einfache und mehrfache Bedeckung des n-dimensionalen Raumes mit einem Würfelgitter, *Math. Zeit.* **47** (1942), 427–467.

[3] LOVÁSZ, L. and SCHRIJVER, A.: Remarks on a theorem of Rédei, *Studia Sci. Math. Hung.* **16** (1991), 449–454.

[4] RÉDEI, L.: Lacunary polynomials over finite fields, Elsevier Publ. Co. Inc., New York, 1973.

[5] RÉDEI, L.: Die neue Theorie der Endlichen abelschen Gruppen und Verallgemeinerung des Hauptsatzes von Hajós, *Acta Acad. Sci. Hung.* **16** (1965), 329–373.

[6] SANDS, A. D.: Replacement of factors by subgroups in the factorization of abelian groups, *Bull. London Math. Soc.* **32** (2000), 297–304.

[7] STEIN, S. K. and SZABÓ, S.: Algebra and Tiling: Homomorphisms in the Service of Geometry, Math. Assoc. Amer., 1994.

[8] SZABÓ, S.: An elementary proof for Hajós' theorem through a generalization, *Math. Japonica* **40** (1994), 99–107.