PACIFIC JOURNAL OF MATHEMATICS
Vol. 140, No. 1, 1989

A NEW PROOF OF RÉDEI'S THEOREM

KERESZTÉLY CORRÁDI AND SÁNDOR SZABÓ

If a finite abelian group is expressed as the product of subsets each of which has a prime number of elements and contains the identity element, then at least one of the factors is a subgroup. This theorem was proved by L. Rédei in 1965. In this paper we will give a shorter proof.

1. Introduction. Let G be a finite abelian group written multiplicatively, and let $A_1, \ldots, A_n$ be subsets of G. If each $g \in G$ is uniquely expressible in the form $g = a_1 \cdots a_n$, $a_1 \in A_1, \ldots, a_n \in A_n$, then we say that $G = A_1 \cdots A_n$ is a factorization of G. If each A_i contains the identity element, we speak of a normed factorization.

The subset $\{1, g, g^2, \ldots, g^{q-1}\}$ will be denoted by $[g, q]$ and called the simplex generated by g with length q, provided that q is a positive integer not greater than the order of g.

Let H be the p-Sylow subgroup of G and K its direct factor complement. We denote the order of K by p'. Each $g \in G$ can be expressed uniquely in the form $g = hk$, $h \in H$, $k \in K$. The element h will be called the p-part of g and denoted by $g|_p$, and the element k will be denoted by $g|_{p'}$.

We will use these two known facts.

(1) The nth cyclotomic polynomial is irreducible over the mth cyclotomic field if m is prime to n.

(2) Let $n > 1$ be an integer and p its smallest prime factor. Then any set of fewer than p nth roots of unity is linearly independent over the field of rationals.

For a short proof see [5].

Proving a conjecture made by H. Minkowski in 1896, G. Hajós in 1941 showed that in a simplex factorization of a finite abelian group at least one of the simplices must be a subgroup.

It may be assumed without loss of generality that in this theorem the lengths of the simplices are primes. So the following result of L. Rédei is a broad generalization of it.

THEOREM 1 (*L. Rédei*). *In any normed factorization of a finite abelian group by subsets of prime cardinality, at least one of the factors is a subgroup.*

This theorem actually implies a stronger form of itself. Indeed, let $G = A_1 \cdots A_n$ be such a factorization. Factoring the group modulo a subgroup factor we obtain a normed factorization of the factor group. Repeating this process, we conclude that after a suitable permutation of the factors, the partial products A_1, A_1A_2, $A_1A_2A_3, \ldots, A_1A_2 \cdots A_n$ form an increasing chain of subgroups.

The purpose of this paper is to give a shorter proof for Rédei's theorem. Our proof follows Rédei's proof which consists of five steps. Although each of them is shortened and simplified, the simplifications of the last two steps are the most significant.

2. Replaceable factors. If χ is a character and A is a subset of G, then $\chi(A)$ denotes $\sum_{a \in A} \chi(a)$. Let χ_i be the ith character of G and g_j the jth element of G. The standard orthogonality relations show that the columns of the matrix $\chi_i(g_j)$ are linearly independent. Using this we see that if A and B are subsets of G and $\chi(A) = \chi(B)$ for each character of G, then $A = B$.

From the factorization $G = AB$ it follows that $\chi(G) = \chi(A)\chi(B)$. For the principal character this reduces to the equation $|G| = |A||B|$. For other characters we have $0 = \chi(A)\chi(B)$.

The set of characters for which $\chi(A) = 0$ will be called the annihilator of A and denoted by $\mathrm{Ann}(A)$.

The previous consideration shows that if $|G| = |A||B|$ and the non-principal characters of G are in $\mathrm{Ann}(A) \cup \mathrm{Ann}(B)$, then $G = AB$ is a factorization. Thus if $G = AB$ is a factorization, $|A| = |A'|$ and $\mathrm{Ann}(A) \subset \mathrm{Ann}(A')$, then $G = A'B$ is a factorization as well. In brief, A can be replaced by A'.

The consequences of the next result play an important role in the proof of Rédei's theorem.

LEMMA 1. *Let A be a subset of a finite abelian group G. If $1 \in A$ and $|A| = p$ is the smallest prime divisor of $|G|$, then $\chi(a|_{p'}) = 1$ for each $\chi \in \mathrm{Ann}(A)$ and $a \in A$.*

Proof. Let $\chi \in \mathrm{Ann}(A)$ and $A = \{1 = a_0, a_1, \ldots, a_{p-1}\}$. There exists a minimal nonnegative integer n such that all $\chi(a_i|_p)$ are p^nth roots of unity. If $n = 0$, then

$$0 = \chi(A) = \sum_{i=0}^{p-1} \chi(a_i) = \sum_{i=0}^{p-1} \chi(a_i|_p)\chi(a_i|_{p'}) = \sum_{i=0}^{p-1} \chi(a_i|_{p'}).$$

Since the least prime factor of p' is greater than p, this violates (2).

Thus $n \geq 1$. We may suppose that $\chi(a_1|_p)$ is a primitive p^nth root of unity, ρ, and that $\chi(a_i|_p) = \rho^{t_i}$, where

$$t_0 = 0, \quad t_1 = 1, \quad 0 \leq t_2 \leq \cdots \leq t_{p-1} \leq p^n - 1.$$

Consider the polynomials

$$A(x) = \sum_{i=1}^{p-1} x^{t_i}\chi(a_i|_{p'}), \qquad F(x) = \sum_{i=0}^{p-1} x^{ip^{n-1}}$$

and let $r_0, \ldots, r_{s-1}$ be all the different numbers among $t_0, \ldots, t_{p-1}$. Now

$$A(x) = \sum_{i=0}^{s-1} x^{r_i}\lambda_i,$$

where λ_i is a sum of at most p p'th roots of unity. So according to (2), $\lambda_i \neq 0$; hence $A(x)$ is not the zero polynomial.

Since $0 = A(\rho) = F(\rho)$ and since $F(x)$, the p^nth cyclotomic polynomial, is irreducible over the p'th cyclotomic field, $F(x)|A(x)$, that is, $A(x) = F(x)B(x)$. We know that $0 \leq \deg A(x) \leq p^n - 1$ and $\deg F(x) = (p-1)p^{n-1}$. Hence $0 \leq \deg B(x) \leq p^{n-1} - 1$. From this it follows that non-zero terms of $B(x)$ occur among terms of $A(x)$. If v denotes the number of non-zero terms of $B(x)$, then $s = pv$ which together with $p \geq s$ gives $s = p$ and $v = 1$. Further we have $1 = t_1 = p^{n-1}$, $t_2 = 2p^{n-1}, \ldots, t_{p-1} = (p-1)p^{n-1}$ and $\lambda_0 = \cdots = \lambda_{p-1}$. The first of these equations implies $n = 1$ and so $t_i = i$ for $0 \leq i \leq p-1$. Then $\lambda_i = \chi(a_i|_{p'})$ and $\chi(a_0|_{p'}) = 1$ imply that $\chi(a_i|_{p'}) = 1$ for $0 \leq i \leq p-1$, and this completes the proof.

COROLLARY 1. *Let $G = AB$ be a normed factorization of the finite abelian group G such that $|A| = p$ is the smallest prime factor of $|G|$. Then A can be replaced by*

(i) $[a^k, p]$ *for each $a \in A \setminus \{1\}$ provided k is prime to p.*

(ii) $A' = \{a|_p(a|_{p'})^{v(a)} \colon a \in A\}$ *for arbitrary exponents $v(a)$.*

Proof. Adopting the notation of the previous proof,

$$\begin{aligned} 0 = \chi(A) &= \sum_{i=0}^{p-1} \chi(a_i) = \sum_{i=0}^{p-1} \chi(a_i|_p)\chi(a_i|_{p'}) = \sum_{i=0}^{p-1} \chi(a_i|_p) \\ &= \sum_{i=0}^{p-1} \rho^i = \sum_{i=0}^{p-1} (\rho^j)^{ik} = \sum_{i=0}^{p-1} \chi(a_j^{ik}|_p) = \sum_{i=0}^{p-1} \chi(a_j^{ik}|_p)\chi(a_j^{ik}|_{p'}) \\ &= \sum_{i=0}^{p-1} \chi(a_j^{ik}) = \chi([a_j^k, p]) \end{aligned}$$

for each $1 \leq j \leq p-1$ provided k is prime to p. Therefore $\operatorname{Ann}(A) \subset \operatorname{Ann}([a_j^k, p])$, which proves (i). Similarly,

$$\begin{aligned} 0 = \chi(A) &= \sum_{a \in A} \chi(a|_p)\chi(a|_{p'}) = \sum_{a \in A} \chi(a|_p)\chi((a|_{p'})^{v(a)}) \\ &= \sum_{a \in A} \chi(a|_p(a|_{p'})^{v(a)}) = \chi(A'), \end{aligned}$$

i.e. $\operatorname{Ann}(A) \subset \operatorname{Ann}(A')$ which proves (ii).

The proof of the next lemma and its corollary is a routine consideration after the previous two proofs.

LEMMA 2. *Let A be a subset of a finite abelian group G. If $1 \in A$, $|A| = p$ is an odd prime and $A \setminus \{1\}$ contains only elements of order p and $2p$ then $\chi(a|_{p'}) = 1$ for each $a \in A$ and $\chi \in \operatorname{Ann}(A)$.*

COROLLARY 2. *Let $G = AB$ be a normed factorization of the finite abelian group G such that $|A| = p$ is an odd prime and $A \setminus \{1\}$ contains only elements of order p and $2p$. Then A can be replaced by*

$$A' = \{a|_p(a|_2)^{v(a)} \colon a \in A\}$$

for arbitrary exponents $v(a)$.

3. Hajós' theorem for p-groups. We need a lemma of L. Rédei. Although its proof can be found in **[3]**, pp. 372–373, for the sake of completeness we include it. Here $\langle A \rangle$ denotes the group generated by A.

LEMMA 3. *Let A be a subset of an abelian p-group such that $|\langle A \rangle| = p^{|A|}$ and $|\langle B \rangle| \geq p^{|B|}$ for all $B \subset A$. Then for each $a \in A$ there exists a* *power of p, say $s(a)$, such that $\langle A\rangle = \prod_{a\in A}[a^{s(a)},p]$ is a factorization in which one of the factors is a subgroup.*

Proof. There is nothing to prove when $|A| = 1$. We denote the order of a by $|a|$, and call $\prod_{a\in A}|a|$ the height of A. We will use induction on the height of A.

When $|\langle B\rangle| > p^{|B|}$ for each $B \neq A$, replace an element of A by its pth power. The conditions of the lemma are satisfied and the height of A is decreased.

In the remaining case there are proper subsets B in A with $|\langle B\rangle| = p^{|B|}$. Since both $\langle B\rangle$ and $\langle A\rangle/\langle B\rangle$ satisfy the inductive assumption, they have desired factorizations from which it is possible to construct a desired factorization for $\langle A\rangle$. This completes the proof.

Now we are ready to prove Hajós' theorem for finite p-groups.

THEOREM 2. *If G is a finite abelian p-group and*

$$G = [g_1,p]\cdots[g_n,p] \tag{3.1}$$

is a factorization, then at least one of the factors is a subgroup.

Proof. Note that the lemma is applicable to $A = \{g_1,\dots,g_n\}$. So there is a factorization

$$G = [g_1^{s_1},p]\cdots[g_n^{s_n},p]$$

in which one of the factors is a subgroup of G. If $s_1 = \cdots = s_n = 1$, then we are done. Otherwise for some $m \geq 1$ $s_1 \neq 1,\dots,s_m \neq 1$, $s_{m+1} = \cdots = s_n = 1$. The element $g_1g_2\cdots g_m$ can be expressed in the form

$$g_1g_2\cdots g_m = g_1^{s_1t_1}\cdots g_m^{s_mt_m}g_{m+1}^{t_{m+1}}\cdots g_n^{t_n},$$

where $0 \leq t_i \leq p-1$. So

$$1 = g_1^{s_1t_1-1}\cdots g_m^{s_mt_m-1}g_{m+1}^{t_{m+1}}\cdots g_n^{t_n}.$$

This violates the factorization

$$G = [g_1^{s_1t_1-1},p]\cdots[g_m^{s_mt_m-1},p][g_{m+1},p]\cdots[g_n,p]$$

which arises from (3.1) by replacing the simplex $[g_i,p]$ by $[g_i^{s_it_i-1},p]$ for $1 \leq i \leq m$. This replacement is possible because $p|s_i$ and therefore $s_it_i - 1$ is prime to p. The proof is complete.

4. Rédei's theorem for elementary groups of order p^2. The proof of this special case of Rédei's theorem was simplified in [4], on which our proof is based. In this section let G be an elementary abelian group of order p^2.

THEOREM 3. *If $G = AB$ is a normed factorization and $|A| = |B| = p$, then A or B is a subgroup of G.*

Proof. The theorem is clearly true for $p = 2$, so we can suppose that $p > 2$. The subset A has a nonidentity element u. The subset B must have an element v which is not in $\langle u\rangle$. The elements u and v form a basis for G. In this basis

$$A = \{u^{a_0}v^{\alpha_0}, u^{a_1}v^{\alpha_1}, \dots, u^{a_{p-1}}v^{\alpha_{p-1}}\},$$
$$B = \{u^{b_0}v^{\beta_0}, u^{b_1}v^{\beta_1}, \dots, u^{b_{p-1}}v^{\beta_{p-1}}\}.$$

Here $a_0 = \alpha_0 = b_0 = \beta_0 = \alpha_1 = b_1 = 0$, $a_1 = \beta_1 = 1$ and $0 \leq a_i, \alpha_i, b_i, \beta_i \leq p-1$. If $\alpha_2 = \cdots = \alpha_{p-1} = 0$ or $b_2 = \cdots = b_{p-1} = 0$, then we are done.

Let ρ be a pth primitive root of unity and consider characters χ_y defined by $\chi_y(u^iv^j) = \rho^{iy+j}$ for $0 \leq y \leq p-1$. Since $0 = \chi_y(G) = \chi_y(A)\chi_y(B)$, according to the pigeonhole principle, one of $\chi_y(A)$ and $\chi_y(B)$ must be zero for at least $(p+1)/2$ values of y. We may suppose for definiteness that $0 = \chi_y(A) = \sum_{i=0}^{p-1} \rho^{a_iy+\alpha_i}$ for at least $(p+1)/2$ values of y. Thus the exponents $a_iy + \alpha_i$ form a complete set of representatives modulo p for at least $(p+1)/2$ values of y. Let S be the set of these values of y.

Let $\alpha'_0, \dots, \alpha'_m$ be the different values occurring among $\alpha_0, \dots, \alpha_{p-1}$, and consider the following polynomials over GF(p):

$$D(x,y) = \sum_{i=0}^{p-1}(x - a_iy - \alpha_i), \quad E(x) = D(x,0),$$

and

$$F(x) = \prod_{i=0}^{m}(x - \alpha'_i).$$

We will study the coefficients e_i in $E(x) = \sum_{i=0}^{p} e_ix^i$.

Here $e_p = 1$, $e_0 = e_1 = 0$ since $\alpha_0 = \alpha_1 = 0$ are roots of $E(x)$ and

$$e_{p-i} = (-1)^iS_i(\alpha_0, \dots, \alpha_{p-1}),$$

where $S_i(\alpha_0, \dots, \alpha_{p-1})$ denotes the ith symmetric polynomial in $\alpha_0, \dots, \alpha_{p-1}$.

For a fixed $y \in S$ we have $D(x,y) = x^p - x$. Thus

$$d_{p-i}(y) = (-1)^iS_i(a_0y + \alpha_0, \dots, a_{p-1}y + \alpha_{p-1}) = 0$$

for each $1 \leq i \leq p-2$, $y \in S$. Since the degree of $d_{p-i}(y)$ is $\leq i$ and it has at least $(p+1)/2$ roots, it is the zero polynomial for each

$0 \le i \le (p-1)/2$. In particular $e_{p-i} = d_{p-i}(0) = 0$. Thus $E(x) = (\sum_{i=2}^{(p-1)/2} e_i x^i) + x^p$. Let $G(x) = E(x) - (x^p - x)$. From $F(x)|(x^p - x)$ and $F(x)|E(x)$ we have $F(x)|G(x)$ and $E(x)/F(x)|E'(x)$. $G'(x) = E'(x) + 1$ gives $E(x)|G(x)(G'(x) - 1)$. Comparing degrees in the last relation we see that $G(x)(G'(x) - 1)$ must be the zero polynomial. $G(x)$ cannot be the zero polynomial since x is one of its terms. Hence $1 = G'(x) = E'(x) + 1$, i.e. $E'(x)$ is the zero polynomial, from which it follows that $E(x) = x^p + c$. Here c must be 0, so $\alpha_0 = \cdots = \alpha_{p-1} = 0$ and the proof is complete.

5. Rédei's theorem for p-groups. In this section let p be a prime and let G be a finite abelian p-group.

THEOREM 4. *If $G = A_1 \cdots A_n$ is a normed factorization of G such that all factors have p elements, then one of the factors is a subgroup.*

Proof. We use induction on n. The case $n = 1$ is trivial so let $n \ge 2$. By Corollary 1(i) every factor can be replaced by a simplex.

If each factor contains element of order at least p^2 then using them we can construct a simplex factorization without subgroup factor. Thus there exists a factor, say A_1, whose nonindentity elements have order p. Consequently, A_1 can be replaced by a subgroup H. Since the partial products are subgroup, $K = HA_2 \cdots A_{n-1}$ is a subgroup of G. If $A_1 \subset K$, then $K = A_1 A_2 \cdots A_{n-1}$ is a factorization of K. By the inductive assumption we are done.

Thus A_1 is not in K. So A_1 can be replaced by a subgroup L such that $L \cap K = \{1\}$. From the factorization $G = LA_2 \cdots A_n$ we deduce that there is an index j such that LA_j is a subgroup. If $j \ne n$, then $K \cap LA_j = A_j$ is the desired subgroup. Therefore LA_n is a subgroup. If LA_n is cyclic then $L \subset \Phi(LA_n) \subset \Phi(G) \subset K$ is a contradiction. (Here $\Phi(G)$ denotes the Frattini subgroup of G.) Thus LA_n is noncyclic. So the nonidentity elements of A_n have order p. Consequently A_n can be replaced by a subgroup M. Note that $G = KM$ is a factorization and so $M \cap K = \{1\}$. From the factorization $G = MA_1 \cdots A_{n-1}$ it follows that there exists an index j such that MA_j is a subgroup. If $j \ne 1$, then $K \cap MA_j = A_j$ is the desired subgroup. Thus $N = MA_1$ is a subgroup. If A_n is not in N then A_n can be replaced by a subgroup T such that $T \cap N = \{1\}$. As before TA_1 is a subgroup so $N \cap TA_1 = A_1$ is a subgroup. Thus $A_n \subset N$. Hence $T = A_1 A_n$ is a factorization and this reduces the problem to the case of elementary p-groups of order p^2.

6. Rédei's theorem for non p-groups. In this section G is a finite abelian non p-group. The product of the heights of factors of a factorization will be called the height of the factorization.

THEOREM 5. *If $G = A_1 \cdots A_n$ is a normed factorization of G such that all factors have prime cardinality, then one of the factors is a subgroup.*

Proof. Assume the contrary and choose a counterexample such that $|G|$ is minimal and the height of the factorization is minimal for this G. Let p be the smallest prime divisor of $|G|$. If each factor of cardinality p has only p-elements, then these factors form a factorization for the p-Sylow subgroup of G. Thus we may suppose that there exists a factor of cardinality p having not only p-elements. Let it be A_1. By the minimality of the height of the factorization and Corollary 1(ii) we may suppose that there is only one non-p-element in A_1, say a. It means that there is a prime q with $q \neq p$ and $a|_q \neq 1$. Again by (ii) we may suppose that $a|_{p'} = a|_q$ and moreover $|a|_q| = q$. Elements of A_1 can be replaced by their p-parts. Now the height of the factorization is decreased. Consequently this replaced factor B_1 is a subgroup of G. Rearranging the factors of the new factorization, we have $G = B_1 \cdots B_n$, where $B_1, B_1B_2, \ldots, B_1B_2 \cdots B_n$ are subgroups of G. Let $H = B_1 \cdots B_{n-1}$. If $A_1 \subset H$, then $H = A_1B_2 \cdots B_{n-1}$ is a factorization and we are done. Thus $a \notin H$.

Since $a|_q \neq 1$, $|G : H| = q$. The factorization $G = HB_n$ concludes that B_n is a complete set of representatives for the cosets of H in G. Thus there exists an $x^{-1} \in B_n$ with $ax^{-1} \in H$.

Let $C = (B_1 \setminus \{a|_p\}) \cup \{ax^{-1}\}$. Note that $H = CB_2 \cdots B_{n-1}$ is a factorization. We should observe that products from $CB_2 \cdots B_{n-1}$ occur among the product of the factorization $A_1 \cdots A_n$. By the minimality of $|G|$ there is a subgroup among the factors. This must be C. If $|C| \geq 3$ then $a|_p = ax^{-1}$, that is, $x = a|_q$. Since $a|_q$ can be replaced by its powers, $B_n = \langle a|_q \rangle$ is a subgroup of G. If $|C| = 2$ then $|ax^{-1}| = 2$ and so $a^2 = x^2$. Now $p = 2$ and $q \neq 2$; hence $x|_q = a|_q$. Since $a|_q$ can be replaced by its powers, $B_n \setminus \{1\}$ contains only elements of order q and $2q$. By Corollary 2 we may repeat the whole consideration by B_n in place of B_1 and in addition now $|B_n| = q \geq 3$. This completes the proof.

REFERENCES

[1] G. Hajós, *Über einfache und mehrfache Bedeckung des n-dimensionalen Raumes mit einem Würfelgitter*, Math. Z., **47** (1942), 427–467.

[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] ——, *Algebra*, Vol. 1, Pergamon Press, Oxford-London, 1967.

[4] E. Wittman, *Einfacher Beweis des Hauptsatzes von Hajós-Rédei für elementare Gruppen von Primzahlquadratordnung*, Acta Math. Acad. Sci. Hung., **20** (1969), 227–230.

[5] ——, *Über verschwindende Summen von Einheitswurzel*, Elemente der Mathematik, Vol. 26/2, 1971.

Received April 27, 1987 and in revised form September 26, 1988.

DEPT. OF COMPUTER TECHN.
EÖTVÖS LORÁND UNIVERSITY
H-1088 BUDAPEST, MUZEUM KRT. 6-8, HUNGARY

AND

DEPT. OF CIVIL ENGINEERING MATH.
TECHN. UNIVERSITY BUDAPEST
H-1111 BUDAPEST, STOCZEK U.2, HUNGARY