MATHEMATICA, Tome 50 (73), N° 2, 2008, pp. 159–168

THE NUMBER OF REMAK DECOMPOSITIONS OF A FINITE ABELIAN GROUP

SIMION BREAZ

Abstract. Although the fundamental theorem of finite Abelian groups states that every finite Abelian group has a decomposition into a direct sum of primary cyclic groups which is unique up to isomorphisms and the order of terms, this decomposition is not unique up to equalities and the order of terms. We present here a way to count the number of direct decompositions into a direct sum of primary cyclic groups for a finite Abelian group up to the order of terms, i.e. the number of Remak decompositions of a finite Abelian group.

MSC 2000. 20K01.
Key words. Abelian group, Remak decomposition, direct summand, type.

1. INTRODUCTION

An obvious induction on the order of a finite group G leads us to the conclusion that we can decompose every finite group G into an internal direct product of indecomposable (normal) subgroups. Such a direct decomposition whose factors are not trivial groups is said to be a *Remak decomposition*, [6]. The order of the direct factors is such a direct decomposition is not important, so it is usual to look at Remak decompositions up to the order of factors. Many authors call such a direct decomposition a Krull-Schmidt decomposition, but we prefer here the terminology of [3] and [6] since we consider these direct decompositions only up to the order of factors (and not up to isomorphisms; see Theorem 1 and the discussion which comes after it). The fundamental result concerning Remak decompositions for finite groups was proved by J. Wedderburn and R. Remak in the beginning of XX-century:

THEOREM 1. [6, Theorem III.7] *Every two Remak decompositions of a finite groups have the same numbers of factors and these factors can be renumbered to obtain that they are pairwise isomorphic (in other terminology: every finite group has a unique Krull-Schmidt decomposition).*

Despite this theorem, there are groups G such that the Remak decomposition is not unique. For example the Klein group $K = \{0, a, b, c\}$ with $a + a = b + b = c + c = 0$ and $x + y = z$ for all nonzero elements $x \neq y \neq z \neq x$ (we shall use the additive notation for Abelian groups) has three Remak decompositions: $K = \{0, a\} \oplus \{0, b\} = \{0, a\} \oplus \{0, c\} = \{0, b\} \oplus \{0, c\}$.

In this paper we shall answer to the question "How many Remak decomposition has a finite Abelian group $G \neq 0$?". If G is a finite group, we denote by R_G the number of Remak decompositions of G.

Theorem 1 gives for Abelian groups a version of the well-known fundamental theorem of finite Abelian groups [5, Theorem 1.12.2 and Theorem 1.12.3]. It says us that every finite Abelian group $G \neq 0$ is a direct sum of non-zero cyclic indecomposable groups

$$(\star)\ G = C_1 \oplus \cdots \oplus C_k$$

and that such a decomposition is unique up to isomorphisms and the order in which the cyclic groups appear in $(\star)$, i.e. if

$$(\star')\ G = C'_1 \oplus \cdots \oplus C'_l$$

is another direct decomposition of in a direct sum of non-zero indecomposable groups then $k = l$, and there exists a bijection $\sigma \in S_k$ such that $C_i \cong C'_{\sigma(i)}$ for all $i \in \{1, \dots, k\}$.

If m is a positive integer we denote, as in [5, Section 1.1], by $\mathbb{Z}(m)$ the group of all residues modulo m with the addition modulo m. We recall here that every non-zero finite cyclic group is isomorphic to a group $\mathbb{Z}(m)$ for some positive integer m, and every non-zero finite indecomposable Abelian group is primary cyclic, hence it is isomorphic to $\mathbb{Z}(p^n)$ for some prime p and some positive integer n. Hence every non-zero finite Abelian group A is isomorphic to a direct sum

$$G \cong \mathbb{Z}(p_1^{n_1})^{k_1} \oplus \cdots \oplus \mathbb{Z}(p_s^{n_s})^{k_s},$$

where $p_1, \dots, p_s$ are primes and $n_1, \dots, n_s, k_1, \dots, k_s$ are positive integers, uniquely determined by G.

The paper is divided into three sections. In the first we study the general case of finite Abelian groups, and we show that the calculation of R_G for such a group can be reduced to the calculation of R_{G_p} for all primary components G_p of G.

In the next two sections we are concerned with Abelian p-groups. Let $G \neq 0$ be a finite Abelian p-group. By the fundamental theorem there exists a unique family of positive integers $n_1 > \cdots > n_s$ and $k_1, \dots, k_l$ such that

$$G \cong \mathbb{Z}(p^{n_1})^{k_1} \oplus \cdots \oplus \mathbb{Z}(p^{n_s})^{k_s}.$$

If $s = 1$ then we say that G is *homogeneous*. If $B \cong \mathbb{Z}(p^{n_j})^{k_j}$ is a direct summand of G, then we call it a *homogeneous component* of G. In Section 3 we reduce the calculation of R_G to the homogeneous case. Theorem 14 together with the last part of Lemma 13 do this job. In the last section we obtain the number R_G for a homogeneous p-group G. As an additional result we obtain the number of automorphisms of a homogeneous Abelian p-group G. This is a particular case of the general result of Shoda [4, Section 1]. In order to do this we use a method similar to the classical way of counting the number of all bases of a finite dimensional vector space over a finite field. I want to mention that this method can be extended to the case of non-homogeneous Abelian p-groups, but a little more care is required.

2. THE GENERAL CASE: REDUCTION TO PRIMARY GROUPS

If G is a finite Abelian group and p is a prime then the set $G_p = \{x \in G \mid \operatorname{ord}(x) \text{ is a power of } p\}$ is a subgroup of G. Moreover A has a direct decomposition

$$(\sharp)\ G = G_{p_1} \oplus \cdots \oplus G_{p_l}$$

where $p_1, \dots p_l$ are primes, [5, Theorem 1.12.1]. Since every indecomposable Abelian group is a primary group, every subgroup C_i which appears in a decomposition $(\star)$ is a subgroup of a primary component G_{p_j}. For all $j \in \{1, \dots, l\}$ we obtain direct decompositions

$$(\star_j)\ G_{p_j} = \bigoplus_{C_i \text{ is a } p_j-\text{group}} C_i.$$

If $(\star')$ is another direct decomposition of G then it induces direct decompositions

$$(\star'_j)\ G_{p_j} = \bigoplus_{C'_i \text{ is a } p_j-\text{group}} C'_i.$$

Therefore, if we have two different direct decomposition of G, $(\star)$ and $(\star')$, then there exists a prime p_j such that these two direct decompositions induce different direct decompositions of G_{p_j}, $(\star_j)$ and $(\star'_j)$.

Conversely, if we want to obtain a decomposition $(\star)$ for a finite Abelian group G we can proceed in the following way: first consider the direct decomposition $(\sharp)$, which is unique; then we decompose each primary component G_{p_j} into a direct sum of cyclic groups $(\star_j)$. Therefore, in order to obtain two different decomposition of G it is necessarily and sufficient to consider two different direct decompositions $(\star_j)$ and $(\star'_j)$ for a primary component of G. All these give us a first formula, which reduces our calculation to primary groups:

Proposition 2. *If $G = G_{p_1} \oplus \cdots \oplus G_{p_l}$ is a finite Abelian group then*

$$R_G = R_{G_{p_1}} \cdots R_{G_{p_l}}.$$

Corollary 3. *For a finite Abelian group G we have $R_G = 1$ if and only if G is a cyclic group.*

Proof. If G is cyclic of order $m = p_1^{k_1} \cdots p_s^{k_s}$ then $G \cong \mathbb{Z}(p_1^{k_1}) \oplus \cdots \oplus \mathbb{Z}(p_s^{k_s})$, hence $R_G = R_{\mathbb{Z}(p_1^{k_1})} \cdots R_{\mathbb{Z}(p_s^{k_s})} = 1$.

If G is not cyclic, then it has a direct summand isomorphic to $H = \mathbb{Z}(p^m) \oplus \mathbb{Z}(p^n)$ for a prime p and two integers $m, n > 0$. Therefore it is enough to prove that $R_H > 1$, and this is obvious since $H = \langle(1,0)\rangle \oplus \langle(0,1)\rangle = \langle(1,0)\rangle \oplus \langle(1,1)\rangle = \langle(1,1)\rangle \oplus \langle(0,1)\rangle$. □

From the proof of this corollary we obtain:

Corollary 4. *If G is a finite Abelian group then $R_{G^2} \geq 3$.*

Corollary 4 is not valid for groups which are not Abelian.

Example 5. *If $n \geq 5$ then $R_{S_n^2} = 1$.*

Proof. First, we observe that S_n is indecomposable, hence every factor of a Remak decomposition of S_n^2 should be isomorphic to S^n. We denote by $\pi_i : S_n^2 \to S_n$, $i \in \{1,2\}$, the canonical projections of the direct product, and we suppose that $K \cong S_n$ is a normal subgroup of S_n^2. We shall prove that $K = S_n \times \{1\}$ or $K = \{1\} \times S_n$.

Suppose that $K \neq S_n \times \{1\}$ and $K \neq \{1\} \times S_n$. Then for $i \in \{1,2\}$ the subgroup $\pi_i(K) \leq S_n$ is not $\{1\}$ and it is normal, hence $\pi_i(K) \in \{A_n, S_n\}$. Moreover, since K has not normal subgroups of order 2, $\pi_i(K) \neq A_n$ (otherwise, the kernel of the restriction $\pi_{i|K} : K \to S_n$ would be of order 2). Therefore, $\pi_i(K) = S_n$ and the restrictions $\pi_{i|K} : K \to S_n$ are isomorphisms for all $i \in \{1,2\}$. Then for every element $x = (\sigma_1, \sigma_2) \in K$ the permutations σ_1 and σ_2 have the same order.

Let $(\tau_1, \tau_2) \in K$ be a pair of two transpositions. Since the subgroup $\langle \tau_2 \rangle \leq S_n$ is not normal, there exists $\sigma \in S_n$ such that $\tau = \sigma^{-1}\tau_2\sigma \neq \tau_2$. Since K is a normal subgroup of S_n^2, $(1, \sigma^{-1})(\tau_1, \tau_2)(1, \sigma) \in K$, hence $(\tau_1, \tau) \in K$ and the restriction $\pi_{1|K}$ is not injective, a contradiction. The proof is complete. □

Remark 6. *The property stated in Example 5 is valid for all powers of the symmetric groups S_n, $n \geq 3$, as a consequence of the general result presented in* [6, Theorem III.14].

3. THE PRIMARY CASE: REDUCTION TO HOMOGENEOUS GROUPS

In this section G shall be a nonzero finitely Abelian p-group. Hence there exists an isomorphism

$$G \cong \mathbb{Z}(p^{n_1})^{k_1} \oplus \cdots \oplus \mathbb{Z}(p^{n_s})^{k_s},$$

where $n_1, \ldots, n_s, k_1, \ldots, k_s$ are positive integers and $n_1 > \cdots > n_s$. We say that G is of *type* $\tau = ((n_1, k_1), \ldots, (n_s, k_s))$.

At this point we need to recall some notions and properties concerning elements of a finite p-group G. If $g \in G$ is an element of order p^e then e is called *the exponent* of g, and it is denoted by $\exp_G(g)$. If $g \neq 0$, *the height* of g is the maximal positive integer t such that the equation $p^t x = g$ has a solution in G. It is denoted by $h^G(g)$. By definition, $h^G(0) = \infty$.

Lemma 7. *Let G be an finite Abelian p-group, $G_1, \ldots, G_s \leq G$ and $g \in G$.*

a) *$G = G_1 \oplus \cdots \oplus G_s$ if and only if for all $g \in G$ there exists a unique s-uple $(g_1, \ldots, g_s) \in G_1 \times \cdots \times G_s$ such that $g = g_1 + \cdots + g_s$.*

b) *If $G = G_1 \oplus \cdots \oplus G_s$ and $g = g_1 + \cdots + g_s \in G$ are like in a) then*

i) $\exp_G(g) = \max(\exp_{G_1}(g_1), \ldots, \exp_{G_s}(g_s))$;

ii) $h^G(g) = \min(h^{G_1}(g_1), \ldots, h^{G_s}(g_s))$.

Proof. a) is well known (see, for example, [5, Lemma 1.10.2]), and b) is a consequence of a). □

LEMMA 8. *If C is a cyclic p-group of order p^n and $c \in C$ then*

$$\exp_C(c) = \max(0, n - h^C(c)).$$

Proof. We can suppose $C = \mathbb{Z}(p^n)$. If $c = 0$ the equality is obvious (here $n - \infty = -\infty$). If $c \neq 0$ then $c = p^l d$ with $l < n$ and $\gcd(p, d) = 1$. Then $\exp_C(c) = n - l > 0$ and $h^C(c) = l$. □

PROPOSITION 9. *Suppose that $\tau = ((n_1, k_1), \ldots, (n_s, k_s))$ is the type of a finite Abelian p-group G. If A is a (homogeneous) direct summand of G of type $((n_1, k_1))$ and B is a direct summand of G of type $\tau = ((n_2, k_2), \ldots, (n_s, k_s))$ then $G = A \oplus B$.*

Proof. It is enough to prove $A \cap B = 0$ since in this case the subgroup $A + B = A \oplus B$ of G has the same cardinality as G. Let $x \in A \cap B$. By Lemma 7 we have $\exp_G(x) = \exp_A(x) = \exp_B(x)$ and $h^G(x) = h^A(x) = h^B(x)$.

We consider a direct decomposition $A = C_1 \oplus \cdots \oplus C_{k_1}$ with $C_i \cong \mathbb{Z}(p^{n_1})$ for all $i \in \{1, \ldots, k_1\}$, and we write $x = c_1 + \cdots + c_{k_1}$ with $c_i \in C_i$ for all $i \in \{1, \ldots, k_1\}$. Using Lemma 7 and Lemma 8 we obtain

$$\begin{aligned}
\exp_A(x) &= \max(\exp_{C_1}(c_1), \ldots, \exp_{C_{n_1}}(c_{k_1})) \\
&= \max(\max(0, n_1 - h^{C_1}(c_1)), \ldots, \max(0, n_1 - h^{C_{k_1}}(c_{k_1}))) \\
&= \max(0, \max(n_1 - h^{C_1}(c_1), \ldots, n_1 - h^{C_{k_1}}(c_{k_1}))) \\
&= \max(0, n_1 - \min(h^{C_1}(c_1), \ldots, h^{C_{k_1}}(c_{k_1}))) \\
&= \max(0, n_1 - h^A(x)) = \max(0, n_1 - h^G(x)).
\end{aligned}$$

In a similar way, we consider a direct decomposition $B = D_1 \oplus \cdots \oplus D_t$, where D_i are cyclic groups of order $p^{m_j} < p^n$ for all $j \in \{1, \ldots, t\}$. We write $x = d_1 + \cdots + d_t$ with $d_j \in D_j$ for all $i \in \{1, \ldots, t\}$. Using again Lemma 7 and Lemma 8 we obtain

$$\begin{aligned}
\exp_B(x) &= \max(\exp_{D_1}(d_1), \ldots, \exp_{D_t}(d_t)) \\
&= \max(\max(0, m_1 - h^{D_1}(d_1)), \ldots, \max(0, m_t - h^{D_t}(d_t))) \\
&\leq \max(\max(0, n_1 - h^{D_1}(d_1)), \ldots, \max(0, n_1 - h^{D_t}(d_t))) \\
&= \max(0, n_1 - \min(h^{D_1}(d_1), \ldots, h^{D_t}(d_t))) \\
&= \max(0, n_1 - h^B(x)) = \max(0, n_1 - h^G(x)),
\end{aligned}$$

and we observe that the equality holds if and only if $d_1 = \cdots = d_t = 0$, hence $x = 0$, and the proof is complete. □

From the first part of the proof we obtain a generalization of Lemma 8.

COROLLARY 10. *If G is a finite Abelian p-group which is homogeneous of type (n, k) and $g \in G$ then* $\exp_G(g) = \max(0, n - h^G(g))$.

If A is a direct summand of a group G, we denote by

$$\mathcal{C}(A) = \{B \leq G \mid A + B = A \oplus B = G\},$$

the set of all complements of A.

Corollary 11. *Let $\tau = ((n_1, k_1), \ldots, (n_s, k_s))$ be the type of a finite Abelian p-group G. If $G = A \oplus B$ such that A is (homogeneous) of type $((n_1, k_1))$ and B is of type $((n_2, k_2), \ldots, (n_s, k_s))$ then*

$$R_G = |\mathcal{C}(B)| R_A |\mathcal{C}(A)| R_B.$$

Proof. By Proposition 9 we observe that $G = A' \oplus B'$ or all $A' \in \mathcal{C}(B)$ and $B' \in \mathcal{C}(A)$. The conclusion is now obvious. □

In order to count the cardinalities of the sets $\mathcal{C}(B)$ and $\mathcal{C}(A)$ we need a reformulation of [1, Lemma 9.5]. We present here a complete proof for reader's convenience.

Let us recall that every direct decomposition $G = A \oplus B$ induces a pair (π, ρ) of idempotent orthogonal endomorphisms of A such that $\pi + \rho = 1_G$. These endomorphisms are constructed in the following way: if $g \in G$, there exists a unique pair $(a_g, b_g) \in A \times B$ such that $g = a_g + b_g$; then $\pi(g) = a_g$ and $\rho(g) = b_g$. Hence $A = \pi(G)$ and $B = \rho(G)$. Conversely, every such a pair of endomorphisms induces a direct decomposition $G = \pi(G) \oplus \rho(G)$. We remark that if we restrict the ranges of π and ρ to A, respectively B, then we obtain *the canonical projections* associated to the direct decomposition $G = A \oplus B$. Moreover, as in the classical linear algebra, every element $g \in G$ can be viewed as a column $g = \begin{pmatrix} a_g \\ b_g \end{pmatrix}$ and every endomorphism α of G can be identified with a matrix $\alpha = [\alpha] = \begin{bmatrix} \alpha_{AA} & \alpha_{BA} \\ \alpha_{AB} & \alpha_{BB} \end{bmatrix}$, where $\alpha_{XY} \in \mathrm{Hom}(X, Y)$ are obtained as compositions of the canonical projection onto Y, α and the inclusion map $X \hookrightarrow G$ $(X, Y \in \{A, B\})$. This matrix is called *the standard matrix form* of α with respect the direct decomposition $G = A \oplus B$. The image $\alpha(g)$ is obtained as a matrices multiplication $\alpha(g) = [\alpha] \begin{pmatrix} a_g \\ b_g \end{pmatrix}$. We also recall that the map

$$\mathrm{End}(G) \to \begin{bmatrix} \mathrm{End}(A) & \mathrm{Hom}(B, A) \\ \mathrm{Hom}(A, B) & \mathrm{End}(B) \end{bmatrix}, \ \alpha \mapsto [\alpha]$$

is a ring isomorphism: it is bijective, $[\alpha + \beta] = [\alpha] + [\beta]$ and $[\beta \circ \alpha] = [\beta][\alpha]$ for all $\alpha, \beta \in \mathrm{End}(G)$.

Proposition 12. *If $G = A \oplus B$ is direct decomposition of an Abelian group then*

$$|\mathcal{C}(A)| = |\mathrm{Hom}(B, A)|.$$

Proof. Let $G = A \oplus B'$ be a direct decomposition of G with the corresponding pair of idempotent endomorphisms (π', ρ'). We consider the standard matrix form $\rho' = [\rho'] = \begin{bmatrix} \rho'_{AA} & \rho'_{BA} \\ \rho'_{AB} & \rho'_{BB} \end{bmatrix}$ with respect the direct decomposition $G = A \oplus B$. Since $\rho'(a) = 0$ for all $a \in A$, we obtain immediately $\rho'_{AA} = 0$ and $\rho'_{AB} = 0$. If (π, ρ) is the pair of idempotent endomorphisms of A associated to the direct decomposition $G = A \oplus B$ then $\rho\pi' = 0$ since $\pi'(G) \subseteq A$. Hence

$$\rho\rho' = \rho\rho' + \rho\pi' = \rho(\rho' + \pi') = \rho.$$

Using the standard matrix form $\rho = [\rho] = \begin{bmatrix} 0 & 0 \\ 0 & 1_B \end{bmatrix}$, we obtain $\rho'_{BB} = 1_B$. Therefore the standard matrix form for ρ' is

$$(\natural) \quad [\rho'] = \begin{bmatrix} 0 & \rho'_{BA} \\ 0 & 1_B \end{bmatrix},$$

where $\rho'_{BA} \in \mathrm{Hom}(B, A)$. Conversely, every endomorphism ϕ of A which has a standard matrix form with respect the decomposition $G = A \oplus B$ as in $(\natural)$ is idempotent and it determines a complement of A: $G = A \oplus \psi(G)$ since $(1_G - \psi)(G) = A$.

Now we define a bijective function $\Psi : \mathcal{C}(A) \to \mathrm{Hom}(B, A)$. If $B' \in \mathcal{C}(A)$ with the corresponding pair of idempotents (π', ρ') then $\Psi(B') = \rho'_{BA}$. Let us remark that Φ is well defined since every decomposition in a direct sum with two terms determines a unique pair of idempotent endomorphisms. Conversely, we consider the function $\Phi : \mathrm{Hom}(B, A) \to \mathcal{C}(A)$, $\Phi(\alpha) = \rho_\alpha(G)$ where ρ_α is the idempotent endomorphism of G for which $[\rho_\alpha] = \begin{bmatrix} 0 & \alpha \\ 0 & 1_B \end{bmatrix}$ is the standard matrix form with respect the direct decomposition $G = A \oplus B$. It is not hard to verify that $\Psi\Phi = 1_{\mathrm{Hom}(A,B)}$ and $\Phi\Psi = 1_{\mathcal{C}(A)}$. □

LEMMA 13. *If $\tau = ((n_1, k_1), \ldots, (n_s, k_s))$ is a type, the groups*

$$\mathrm{Hom}(\mathbb{Z}(p^{n_1})^{k_1}, \mathbb{Z}(p^{n_2})^{k_2} \oplus \cdots \oplus \mathbb{Z}(p^{n_s})^{k_s})$$

and

$$\mathrm{Hom}(\mathbb{Z}(p^{n_2})^{k_2} \oplus \cdots \oplus \mathbb{Z}(p^{n_s})^{k_s}, \mathbb{Z}(p^{n_1})^{k_1})$$

have the same cardinality, and this is

$$m_\tau = p^{k_1 \sum_{i=2}^{s} n_i k_i}.$$

Proof. Since $\mathrm{Hom}(-,-)$ commutes with finite direct products (sums) of Abelian groups by [5, Problems 1.10.2, 1.10.3], and we have group isomorphisms

$$\mathrm{Hom}(\mathbb{Z}(p^{n_1}), \mathbb{Z}(p^{n_i})) \cong \mathrm{Hom}(\mathbb{Z}(p^{n_i}), \mathbb{Z}(p^{n_1})) \cong \mathbb{Z}(p^{n_i})$$

for all $i \in \{2, \ldots, s\}$, we obtain

$$\begin{aligned} m_\tau &= |\mathrm{Hom}(\mathbb{Z}(p^{n_1})^{k_1}, \mathbb{Z}(p^{n_2})^{k_2} \oplus \cdots \oplus \mathbb{Z}(p^{n_s})^{k_s})| \\ &= \prod_{i=2}^{s} |\mathrm{Hom}(\mathbb{Z}(p^{n_1})^{k_1}, \mathbb{Z}(p^{n_i})^{k_i})| \\ &= \prod_{i=2}^{s} |\mathrm{Hom}(\mathbb{Z}(p^{n_1}), \mathbb{Z}(p^{n_i}))|^{k_1 k_i} = \prod_{i=2}^{s} p^{k_1 n_i k_i}, \end{aligned}$$

and a analogous calculation for $\mathrm{Hom}(\mathbb{Z}(p^{n_2})^{k_2} \oplus \cdots \oplus \mathbb{Z}(p^{n_s})^{k_s}, \mathbb{Z}(p^{n_1})^{k_1})$ gives the same result. The proof is complete. □

Theorem 14. *Let $G \cong \mathbb{Z}(p^{n_1})^{k_1} \oplus \cdots \oplus \mathbb{Z}(p^{n_s})^{k_s}$, be a finite Abelian p-group of type $\tau = ((n_1, k_1), \ldots, (n_s, k_s))$. If $\tau_i = ((n_i, k_i), \ldots, (n_s, k_s))$ for all $i \in \{1, \ldots, s-1\}$ then*

$$R_G = R_{\mathbb{Z}(p^{n_1})^{k_1}} \cdots R_{\mathbb{Z}(p^{n_s})^{k_s}} m_{\tau_1}^2 \cdots m_{\tau_{s-1}}^2.$$

Proof. Using Corollary 11, Proposition 12 and Lemma 13 we obtain

$$\begin{aligned} R_G &= R_{\mathbb{Z}(p^{n_1})^{k_1}} R_{\mathbb{Z}(p^{n_2})^{k_2} \oplus \cdots \oplus \mathbb{Z}(p^{n_s})^{k_s}} m_{\tau_1}^2 = \cdots \\ &= R_{\mathbb{Z}(p^{n_1})^{k_1}} \cdots R_{\mathbb{Z}(p^{n_i})^{k_i}} R_{\mathbb{Z}(p^{n_{i+1}})^{k_{i+1}} \oplus \cdots \oplus \mathbb{Z}(p^{n_s})^{k_s}} m_{\tau_1}^2 \cdots m_{\tau_i}^2 \\ &= R_{\mathbb{Z}(p^{n_1})^{k_1}} \cdots R_{\mathbb{Z}(p^{n_s})^{k_s}} m_{\tau_1}^2 \cdots m_{\tau_{s-1}}^2, \end{aligned}$$

and the proof is complete. □

4. THE HOMOGENEOUS CASE

Let $G \cong \mathbb{Z}(p^n)^k$ be a homogeneous finite Abelian group. In order to decompose G we need a few lemmas.

Lemma 15. *If $g_1, \ldots, g_l$ are elements of maximal order in a finite Abelian p-group G such that $\langle g_1, \ldots, g_l \rangle = \oplus_{i=1}^{l} \langle g_i \rangle$, then $\langle g_1, \ldots, g_l \rangle$ is a direct summand of G.*

Proof. Let $K = \langle g_1, \ldots, g_l \rangle = \oplus_{i=1}^{l} \langle g_i \rangle$ and $\mathrm{ord}(g_1) = \cdots = \mathrm{ord}(g_l) = p^n$. We consider a subgroup $H \leq G$ which is maximal with the property $K \cap H = 0$ and suppose $K + H \neq G$. Therefore the p-group $G/(K+H)$ is not trivial, hence there exists an element $g + (K+H)$ of order p. Therefore $g \notin K + H$ and $pg \in K + H$. If $pg = k + h$ with $h \in H$ and $k \in K$, then $0 = p^{n-1}pg = p^{n-1}k + p^{n-1}h$. Since $K + H = K \oplus H$, we obtain $p^{n-1}k = 0$, hence $\mathrm{ord}(k) < p^n$. By Corollary 10, it follows that there exists $k_0 \in K$ such that $k = pk_0$.

Let $g_0 = g - k_0$. Then $pg_0 = p(g - k_0) = pg - pk_0 = h \in H$. Suppose that $x \in K \cap (H + \langle g_0 \rangle)$. Then $x = h_0 + mg_0$ and $mg_0 \in K + H$, hence $p \mid m$ since the element $g_0 + (K+H) = g + (K+H) \in G/(K+H)$ is of order p. But, in these conditions $mg_0 = m'pg_0 \in H$, hence $x \in H$. From $x \in K$ we deduce $x = 0$. Therefore $K \cap (H + \langle g_0 \rangle) = 0$. This contradicts the choice of H, and the proof is complete. □

Remark 16. *The case $l = 1$ is often used in proofs of fundamental theorem for finite abelian groups, see* [5, Lemma 1.12.3] *or* [2].

Remark 17. *The hypothesis $\langle g_1, \ldots, g_l\rangle = \oplus_{i=1}^{l}\langle g_i\rangle$ is essential. If $G = \mathbb{Z}(4)\oplus\mathbb{Z}(4)$, $g_1 = (1,0)$, $g_2 = (1,2)$ then $\langle g_1, g_2\rangle = \mathbb{Z}(4)\oplus 2\mathbb{Z}(4)$ is not a direct summand of G.*

Recall that for any abelian group G and any integer q, $G[q] = \{g \in G \mid qg = 0\}$ is a subgroup of G.

Lemma 18. *Let $G = K \oplus H \cong \mathbb{Z}(p^n)^k$ be a homogeneous finite Abelian group. An element $x \in G$ has the properties:*
(i) $K + \langle x\rangle = K \oplus \langle x\rangle$ and
(ii) $K \oplus \langle x\rangle$ is a direct summand of G
if and only if $x \notin K \oplus H[p^{n-1}]$.

Proof. ($\Rightarrow$) We write $x = k+h$ with $k \in K$ and $h \in H$. Since $\langle x\rangle$ is a direct summand of G, the order of x is p^n, hence $k \notin K[p^{n-1}]$ or $h \notin H[p^{n-1}]$. Using (i) we observe that $\mathrm{ord}(h) \geq \mathrm{ord}(k)$, since if we suppose the contrary then $0 \neq \mathrm{ord}(h)k = \mathrm{ord}(h)x \in \langle x\rangle \cap K$. Therefore $h \notin H[p^{n-1}]$, and $x \notin K \oplus H[p^{n-1}]$.
($\Leftarrow$) If $x \notin K \oplus H[p^{n-1}]$ then $x = k + h$ with $\mathrm{ord}(h) = p^n$. Then $mx \in K$ if and only if $p^n \mid m$ and this proves (i).
(ii) is a consequence of the Lemma 15. □

We are ready to decompose G and to count the possibilities:
Step 1: We choose an element $x_1 \in G$ such that $\langle x_1\rangle$ is a direct summand of G. Using Lemma 15 for the case $l = 1$, x_1 has this property if and only if $x_1 \in G \setminus G[p^{n-1}] = G \setminus pG$. Therefore we have

$$a_1 = p^{kn} - p^{k(n-1)} = p^{k(n-1)}(p^k - 1)$$

possibilities. But for each cyclic direct summand C of G we have $C = \langle x\rangle$ for all $x \in C \setminus pC$. Hence the number of possibilities for the choice a first direct summand is

$$b_1 = \frac{a_1}{p^n - p^{n-1}} = \frac{p^{(n-1)(k-1)}(p^k - 1)}{p - 1}.$$

Step $i + 1$: Suppose that after i steps we have a direct decomposition $G = C_1\oplus\cdots\oplus C_i\oplus H_i$ with $C_1 \ldots, C_i$ cyclic groups. By Lemma 18, we observe that $x_{i+1} \in G$ has the property $(C_1\oplus\cdots\oplus C_i)+\langle x_{i+1}\rangle = C_1\oplus\cdots\oplus C_i\oplus\langle x_{i+1}\rangle$ and this is a direct summand of G if and only if $x_{i+1} \notin C_1\oplus\cdots\oplus C_i\oplus H_i[p^{n-1}]$. Since $C_1 \oplus\cdots\oplus C_i \oplus H_i[p^{n-1}] \cong \mathbb{Z}(p^n)^i \oplus \mathbb{Z}(p^{n-1})^{k-i}$, we have

$$a_{i+1} = p^{kn} - p^{k(n-1)+i} = p^{k(n-1)}(p^k - p^i)$$

possibilities for the choice of x_{i+1} and

$$b_i = \frac{a_{i+1}}{p^n - p^{n-1}} = \frac{p^{(n-1)(k-1)}(p^k - p^i)}{p - 1}$$

possibilities to choose a subgroup C_{i+1} such that $C_1 \oplus \cdots \oplus C_i \oplus C_{i+1}$ is a direct summand of G.

Since we need exactly k-steps to obtain a direct decomposition of G into a direct sum of cyclic subgroups, we have

$$b = b_1 \cdots b_k = \frac{p^{(n-1)k(k-1)}(p^k - 1) \cdots (p^k - p^{k-1})}{(p-1)^k}$$

direct decompositions for G. But these b direct decompositions depend on the order of direct summands, hence we have

Theorem 19. *If $G \cong \mathbb{Z}(p^n)^k$ then*

$$R_G = \frac{p^{(n-1)k(k-1)}(p^k - 1) \cdots (p^k - p^{k-1})}{(p-1)^k k!}$$

Remark 20. *The number $a = a_1 \cdots a_k = p^{k^2(n-1)}(p^k - 1) \cdots (p^k - p^{k-1})$ equals the number of bases for the free $\mathbb{Z}(p^n)$-module G* ([4, p.678]). *It also represents the cardinality of the general linear group $GL_k(\mathbb{Z}(p^n))$.*

Remark 21. *It is not hard to see that if $G \cong \mathbb{Z}(p^{n_1})^{k_1} \oplus \cdots \oplus \mathbb{Z}(p^{n_s})^{k_s}$ then every isomorphism $\mathbb{Z}(p^{n_1})^{k_1} \oplus \cdots \oplus \mathbb{Z}(p^{n_s})^{k_s} \xrightarrow{\cong} G$ induces a Remak decomposition for G. It is an open problem to characterize the following equivalence relation: for two isomorphisms $f, g : \mathbb{Z}(p^{n_1})^{k_1} \oplus \cdots \oplus \mathbb{Z}(p^{n_s})^{k_s} \xrightarrow{\cong} G$, we define $f \sim g$ if and only if f and g induce the same Remak decomposition for G.*

Acknowledgements. I would like to thank Andrei Marcus and Septimiu Crivei for useful discussions on the subject. The author is supported by the grant CEEX ET-47/2006–2008

REFERENCES

[1] Fuchs, L., *Infinite Abelian Groups I/II*, Academic Press (1970/1973).
[2] Navarro, G., *On the fundamental theorem of finite Abelian groups*, Am. Math. Monthly, **110** (2003), 153–154.
[3] Paris, L., *Irreducible Coxeter groups*, Internat. J. Algebra Comput., in press.
[4] Shoda, K., *Über die Automorphismen einer endliehen Abelschen Gruppe*, Math. Ann., **100** (1928), 674–686.
[5] Wickless, W. J., *A first graduate course in abstract algebra*, Pure and Applied Mathematics **266**, Marcel Dekker, (2004).
[6] Zassenhaus, H. J., *The Theory of Groups*, Chelsea Publisihng Company (1958).

Received June 15, 2008

„Babeş-Bolyai" University
Faculty of Mathematics and Computer Science
Str. Mihail Kogălniceanu Nr. 1
400084 Cluj-Napoca, Romania
E-mail: bodo@math.ubbcluj.ro