Alexander Abian

On the lengths of bases of a finitely generated abelian group.

Bollettino dell'Unione Matematica Italiana, Serie 3, Vol. **19** (1964), n.1, p. 12–15.

Zanichelli

<http://www.bdim.eu/item?id=BUMI_1964_3_19_1_12_0>

On the lengths of bases of a finitely generated abelian group

Nota di ALEXANDER ABIAN (a Columbus, Ohio) (*) (**)

Summary. - *In this paper the lower and the upper bounds of the lengths of the bases of a finitely generated abelian group are determined.*

A subset $\mathfrak{B}$ of an abelian group $\mathfrak{F}$ is called a basis of $\mathfrak{F}$ if $\mathfrak{F}$ is the direct sum of cyclic groups generated by the elements of $\mathfrak{B}$. The cardinality of $\mathfrak{B}$ shall be called the *length* of the basis $\mathfrak{B}$. Below we determine the lengths of a longest and of a shortest basis of a finitely generated abelian group.

In what follows (X) shall represent a cyclic group generated by X and x the order of (X). Moreover, α, β, ... shall represent integers. Furthermore, $(X) \oplus (Y)$ shall represent the direct sum of the two cyclic groups (X) and (Y).

LEMMA 1. - *Let* A, B *and* C *be three elements of a finite abelian group. Then*

$$(A) = (B) \oplus (C)$$

if and only if $(A) = (B + C)$ *and* $(b, c) = 1$.

PROFF. - Suppose $(A) = (B) \oplus (C)$. Clearly, $B + C$ is an element of the highest order bc of (A). Therefore, $(A) = (B + C)$. Now assume the contrary that $(b, c) = \alpha > 1$ so that $b = \alpha\beta$ and $c = \alpha\sigma$. But then

$$\alpha\beta\sigma(B + C) = 0 \quad \text{so that} \quad \alpha\beta\sigma \geq bc = \alpha^2\beta\sigma$$

(*) Pervenuta alla Segreteria dell'U. M. I. il 22 ottobre 1963.
(**) Formely SMBAT ABIAN.

Consequently, $\alpha = 1$ which contradicts the assumption $\alpha \neq 1$. Thus, indeed, $(a, b) = 1$.

Next, suppose $(A) = (B + C)$ and $(b, c) = 1$. Clearly, $(B + C) \subset \subset (B) \oplus (C)$. Now, since $(b, c) = 1$, there exist γ and δ such that $\gamma b + \delta c = 1$ and hence

$$\delta c(B + C) = (1 - \gamma b)B = B$$

and similarly,

$$\gamma b(B + C) = (1 - \delta c)C = C.$$

Consequently, $(B) \oplus (C) \subset (B + C)$. Thus, indeed $(A) = (B) \oplus (C)$, as desired.

From Lemma 1, by induction, we derive

COROLLARY. - *Let* A, A_1, A_2, ..., A_n *be elements of a finite abelian group. Then*

$$(A) = (A_1) \oplus (A_2) \oplus \dots \oplus (A_n)$$

if and only if

$$(A) = (A_1 + A_2 + \dots + A_n) \quad \textit{and} \quad (a_i, a_j) = 1, \qquad \textit{for } i \neq j.$$

If $\mathfrak{G}$ is a finite group then it is well known [1] that $\mathfrak{G}$ admits a *primitive* decomposition into a direct sum of (indecomposable) cyclic groups of prime power orders. Such a primitive decomposition of $\mathfrak{G}$ is unique up to isomorphism. The lenght of a basis corresponding to a primitive decomposition of $\mathfrak{G}$ is an invariant of $\mathfrak{G}$ and shall be denoted by $L_p(\mathfrak{G})$. Moreover, in a primitive decomposition of $\mathfrak{G}$, the number of the direct summands whose orders are powers of a given prime p shall be denoted by $n(p)$

LEMMA 2. - *Let $\mathfrak{G}$ be a finite abelian group such that*

$$\mathfrak{G} = (G_1) \oplus (G_2) \oplus \dots \oplus (G_n) \tag{1}$$

then $n \leq L_p(\mathfrak{G})$.

PROOF. - It is sufficient to observe [1] that a decomposition of $\mathfrak{Z}$ such as (1), can be refined to a primitive decomposition of $\mathfrak{Z}$.

LEMMA 3. - *Let* (X) *be a finite cyclic group and* p *a given prime Then* (X) *has at most one direct summand whose order is a power of* p.

PROOF. Assume the contrary that

$$(X) = (A) \oplus (B) \quad \text{and} \quad (X) = (A') \oplus (B')$$

with $a = p^\alpha$ and $a' = p^{\alpha'}$ and $(A) \neq (A')$. Since a finite cyclic group has at most one subgroup of a given order, hence, if $\alpha = \alpha'$ then $(A) = (A')$ which contradicts our assumption. On the other hand, if $\alpha \neq \alpha'$, say, $\alpha' > \alpha$, then clearly, $(a, b) \neq 1$, which contradicts Lemma 1. Thus, aur assumption is false and the Lemma is proved.

If $\mathfrak{Z}$ is a finite abelian group then it is well known [1] that $\mathfrak{Z}$ admits a canonical decomposition into a direct sum of cyclic groups such that the order of one of every two direct summands divides the order of the other. As it can be easily seen from below (and as is well known) such a canonical decomposition of $\mathfrak{Z}$ is unique up to isomorphism. The lenght of a basis corresponding to a canonical decomposition of $\mathfrak{Z}$ is an invariant of $\mathfrak{Z}$ and shall be denoted by $L_c(\mathfrak{Z})$.

LEMMA 4. - *Let* $\mathfrak{Z}$ *be a finite abelian group. Then*

$$L_c(\mathfrak{Z}) = \max_p n(p).$$

PROOF. - It is enough to observe that if

$$\mathfrak{Z} = (C_1) \oplus (C_2) \oplus \dots \oplus (C_k), \quad \text{with} \quad c_i = 0 \qquad (\text{mod } c_{i+1})$$

is a canonical decomposition of $\mathfrak{Z}$ then (C_1) is isomorphic to the direct sum of those summands of a primitive decomposition of $\mathfrak{Z}$ whose orders are of the form p^α with α maximum and p a prime.

LEMMA 5. - *Let $\mathfrak{J}$ be a finite abelian group such that*

$$\mathfrak{J} = (A_1) \oplus (A_2) \oplus \dots \oplus (A_n).$$

Then

$$L_c(\mathfrak{J}) \leq n \leq L_p(\mathfrak{J}).$$

PROOF. - The fact that $n \leq L_p(\mathfrak{J})$ is secured by lemma 2. The fact that $L_c(\mathfrak{J}) \leq n$ is secured by Lemmas 3 and 4.

Finally, let $\mathfrak{A}$ be a finitely generated abelian group. It is well known [1] that $\mathfrak{A}$ admits a finite basis and that the number r (called the *rank* of $\mathfrak{A}$) of the elements of infinite order of a basis of $\mathfrak{A}$ is an invariant of $\mathfrak{A}$. Moreover, in an arbitrary decomposition of $\mathfrak{A}$ into a direct sum of cyclic groups the direct sum of all the finite summands is equal to the torsion subgroup of $\mathfrak{A}$. Consequently, in view of Lemma 5 we have:

THEOREM. *Let $\mathfrak{A}$ be a finitely generated abelian group of rank* r. *Let* $L_c(\mathfrak{A})$ *and* $L_p(\mathfrak{A})$ *denote respectively the lengths of a canonical and of a primitive decomposition of the torsion subgroup of $\mathfrak{A}$. If* n *denotes the length of a basis of $\mathfrak{A}$ then*

$$r + L_c(\mathfrak{A}) \leq n \leq r + L_p(\mathfrak{A}).$$

REFERENCE

[1] A. G. KUROSH, *The Theory of Groups*, Chelsea, New York, vol 1 (1955), pp. 137-151.