LINEAR INDEPENDENCE IN ABELIAN GROUPS

MARY-ELIZABETH HAMSTROM

Alexandroff and Hopf\(^1\) offer a proof of the following theorem.\(^2\)
If \(U\) is a sub-group of an Abelian group \(J\) and \(m\) is an integer such that \(m = 0\) or \(m \geq 2\), then \(r_m(J) \geq r_m(U) + r_m(J-U)\). The proof is incorrect and the following example shows that the theorem is, in fact, not true.

**Example 1.** Let \(J\) be the group of integers mod 4, and \(U\) the sub-group generated by 2; \(r_2(J) = 1\), \(r_2(U) = 1\), \(r_2(J-U) = 1\).

The proof referred to is correct if \(m = 0\), and the authors, in fact, prove that \(r_0(J) = r_0(U) + r_0(J-U)\). In what follows we shall assume this, and that all groups considered are finitely generated and Abelian.\(^3\)

**Theorem 1.** If

1. The group \(V = \sum_{j=1}^{\infty} N_j\) is the direct sum of indecomposable cyclic sub-groups, \(N_j\),
2. \(m = p_1^{q_1} \cdot p_2^{q_2} \cdots \cdot p_n^{q_n}\), where for each \(i\), \(p_i\) is a prime number, and
3. for each \(i\), \(q_i\) is the number of the \(N_j\) whose orders are divisible by \(p_i^{q_i}\),

then \(r_m(V) = k\), where \(k\) is the least of the \(q_i\).\(^4\)

**Proof.** We can assume, without loss of generality, that \(q_1 \leq q_2 \leq \cdots \leq q_n\). The problem, then, is to show that \(r_m(V) = q_1 = k\).

Clearly, \(V\) is a direct sum \(V = \sum_i V_i + \sum_{i=k+1}^{\infty} V_i\) where for each \(i\), \(V_i\) is cyclic and (1) if \(1 \leq i \leq k\), \(V_i\) has order divisible by \(m\), (2) if \(k+1 \leq i \leq l\), \(V_i\) has order not divisible by \(p_i^{q_i}\). For each \(i\), let \(x_i\) be a generating element for \(V_i\). The \(x_i\) form a basis for \(V\) and \(k = r_m(V)\).

Suppose \(y_1, y_2, \ldots, y_{k+1}\) is a set of \(k+1\) elements in \(V\). For each \(i\),

\[
y_i = \sum_{j=1}^{k} a_{ij} x_j + \sum_{j=k+1}^{l} a_{ij} x_j.
\]

For each \(i\), the order of \(\sum_{j=k+1}^{l} a_{ij} x_j\) is not divisible by \(p_i^{q_i}\), so there exist constants \(r_1, r_2, \ldots, r_{k+1}\), no one of which is divisible by \(p_i^{q_i}\).

Received by the editors May 9, 1949 and, in revised form, May 8, 1950.


\(^2\) The elements \(x_1, x_2, \ldots, x_n\) of an Abelian group \(J\) are said to be linearly independent mod \(m\) if \(\sum_{i=1}^{n} a_i x_i = 0\), where the \(a_i\) are integers, implies that \(a_i = 0\) mod \(m\) for each \(i\). The rank mod \(m\) of \(J\), \(r_m(J)\), is the largest integer \(n\) such that there exists a set of \(n\) elements in \(J\) which are linearly independent mod \(m\); \(r_0(J)\) denotes ordinary rank.

\(^3\) We shall assume, further, that \(r_0(J)\) is finite. Theorems 2 and 3 of this paper are true without the condition that \(J\) be finitely generated. This follows without too much difficulty from the proofs of these theorems.

\(^4\) We assign order 0 to infinite cyclic groups.

487
such that for each $i$, $r_i \sum_{j=k+1}^t a_{ij}x_j = 0$. Clearly, for each $i$,

$$r_i y_i = r_i \sum_{j=1}^{k} a_{ij}x_j \neq 0.$$  

Since we have $k+1$ equations in $k$ indeterminates, there exist constants $t_1, t_2, t_3, \ldots, t_{k+1}$, relatively prime, and such that for each $j$, $\sum_{i=1}^{k} t_i a_{ij} = 0$. Therefore,

$$\sum_{i=1}^{k+1} t_i r_i y_i = 0.$$  

At least one of the $t_i$ is not divisible by $p_1$. Therefore, at least one of the $t_i r_i$ is not divisible by $p_1^m$, and is, therefore, not divisible by $m$. It follows that the $y_i$ are linearly dependent mod $m$. Therefore, $r_m(V) = k$.

The following are direct consequences of the above proof.

**Corollary 1.** If $r_m(J) = k$ there exists a set of $k$ linearly independent elements mod $m$ each element of which has order $m$ or 0.

**Corollary 2.** The rank of $J$, $r_0(J)$, is the number of the $V_i$ whose order is 0, and if $R_m(J)$ denotes the number of the $V_i$ whose order is divisible by $m$, but is not 0, then $r_m(J) = r_0(J) + R_m(J)$.

**Theorem 2.** If $J$ is a finitely generated Abelian group and $U$ is a sub-group with division\textsuperscript{6} of $J$, then $r_m(J) = r_m(U) + r_m(J - U)$.

**Proof.** By Corollary 2 above, $r_m(U) = r_0(U) + R_m(U)$. Since $U$ is a sub-group with division, each element of $(J - U)$ has order 0, and $r_m(J - U) = r_0(J - U)$. Clearly, $R_m(U) = R_m(J)$. Therefore, since $r_m(U) + r_m(J - U) = r_0(U) + R_m(U) + r_m(J - U) = r_0(U) + R_m(U) + R_m(J) = r_0(J) + R_m(J) = r_m(J)$.

The same authors\textsuperscript{6} attempt to prove that if $p$ is a prime number and $U$ is a sub-group of the group $J$, then $r_p(J) \leq r_p(U) + r_p(J - U)$. The proof is incorrect. I offer in its place a valid proof.

**Theorem 3.** If $p$ is a prime and $U$ is a sub-group of the group $J$, then $r_p(U) + r_p(J - U) \geq r_p(J)$.

**Proof.** There is a set of $r_p(U)$ elements of $U$, $x_1, x_2, \ldots, x_{r_p(U)}$ linearly independent mod $p$. $R_p(U)$ of these form a basis for the sub-group of $U$ consisting of all elements in $U$ of order $p$. There is a set

\textsuperscript{6} The sub-group $U$ of $J$ is said to be a sub-group with division of $J$ provided $px \in U$, $p \neq 0$, implies that $x \in U$.

\textsuperscript{6} Alexandroff and Hopf, loc. cit., p. 573.
\[ y_1, y_2, \ldots, y_k \text{ of elements of } J \text{ such that (1) for each } i, y_i \text{ is of order } p, \]
\[ (2) \quad k = R_p(J) - R_p(U), \text{ and } (3) \quad x_1, x_2, \ldots, x_{R_p(U)}, y_1, y_2, \ldots, y_k \]
\[ \text{is a basis for the sub-group of } J \text{ consisting of all elements of order } p. \]
Clearly, \( U + y_1, U + y_2, \ldots, U + y_k \) are independent mod \( p \) in \( J - U \), and \( R_p(J - U) \geq k \).

\[ r_p(U) + r_p(J - U) = r_0(U) + R_p(U) + r_0(J - U) + r_p(J - U) \]
\[ \geq r_0(J) + R_p(U) + k \]
\[ = r_0(J) + R_p(J) = r_p(J). \]

Example 1 shows that the inequality can hold. The following example shows that Theorem 3 is not true for composite numbers.

**Example 2.** Let \( J \) be the group of integers mod 12, and \( U \) the sub-group generated by 2. Then, \( r_4(J) = 1, r_4(U) = 0, r_4(J - U) = 0. \)

It can be proved by methods quite similar to those in this paper that the equality in Theorem 3 holds if and only if \( pU \) equals the common part of \( U \) and \( pJ \), but this lies outside the purpose of this paper.

**University of Texas**