A remark on elementary abelian groups

J.L. Hickman

Dr M.F. Newman has asked whether in the absence of the Axiom of Choice it is possible to have two non-isomorphic elementary abelian groups of the same (finite) exponent and of the same (infinite) cardinality. By means of an example, I show that this is in fact possible, if the exponent is at least five; I do not know the answer in the remaining two cases. The example given requires the construction of a Fraenkel-Mostowski model of set theory, and for this purpose I draw upon the terminology, constructions, and results contained in the first two sections of a previous paper, "The construction of groups in models of set theory that fail the Axiom of Choice" (Bull. Austral. Math. Soc. 14 (1976), 199-232), with which I assume familiarity.

Wherever possible, we use upper case script letters to denote algebraic or relational structures, and the corresponding upper case italic letters to denote their carriers. The letters "i", "j", ..., "q" denote natural numbers, "ω" denotes the first transfinite ordinal, and "| |" denotes set-theoretic cardinality.

Abelian groups will be written additively, and the identity element of an abelian group will be denoted by "0" (usually with an appropriate set of subscripts). If p is a prime number, then an abelian group all of whose nontrivial elements have order p will be called an "elementary abelian p-group".

Received 8 November 1976. The work contained in this paper was done whilst the author was a Research Fellow at the Australian National University.
We draw upon the terminology, constructions, and results contained in
the first two sections of [1]. A straightforward modification of Theorem
II.1 of that paper tells us that there is an FMC-model $M$ containing two
countably infinite elementary abelian $p$-groups $C_0$ and $C_1$ such that
$C_0 \cap C_1 = \emptyset$ and $C = C_0 \cup C_1$ is the set of urelemente of $M$,
and $p$ is an arbitrary but fixed prime. Henceforth we assume that $p \geq 5$,
and we work entirely within the model $M$; that is, we assume that $M$ is the
universe. The fact that we are now working in FMC set theory instead of
the more usual ZFC or VNB set theory should not cause us any concern, for
it is only at the foundational levels of mathematics that the technical
eccentricities of FMC set theory begin to make their presence felt. In
particular, the following constructions can be carried out in FMC set
theory just as well as in ZFC.

By the Axiom of Choice, we can show that any two elementary abelian
$p$-groups of the same cardinality are isomorphic; it follows that for each
$i < 2$ we can represent $C_i$ as the complete direct sum of an $\omega$-sequence
$\{C_i^j\}_{j<\omega}$ of groups $C_i^j$, where each $C_i^j$ is a copy of the cyclic group
of order $p$. We denote the elements of $C_i^j$ by $c_{i,j,k}$, $k < p$, and
we assume that the $c_{i,j,k}$ are subscripted in such a fashion that
$c_{i,j,0} = e_{i,j}$ and $c_{i,j,k} = k c_{i,j,1}$ for $0 < k < p$. Thus we may think of
the elements of $C_i$ as $\omega$-sequences $\{c_{i,j,k}\}_{j<\omega}$, with $k_j < p$ for each
$j < \omega$, and with addition being performed pointwise.

Let $i, j, k$ be given, with $i < 2$ and $k < p$. We denote by
$c_{i,j,k}$ the element $(c_{i,m,n})_{m<\omega}$ of $C_i$ defined by $n_j = k$ and $n_m = 0$
for $m \neq j$. We now put $C_i^{i,j} = \{c_{i,j,k} \in C_i; k < p\}$; the set $C_i^{i,j}$ is of
course the carrier of a subgroup $C_i^{i,j}$ of $C_i$ isomorphic to $C_i^j$.

Let the number $j$ be given. We define a bijection $f_j : C_{0j} \to C_{1j}$
by $f_j(c_{0j,m}) = c_{1j,m}$ and $f_j(k c_{0j,1}) = k c_{1j,1}$ for $k < p$. Since
$C_{0j}$, $C_{1j}$ are both cyclic of order $p$ and $p \geq 5$, these equations
completely define $f_j$. Using these functions $f_j$, we now define a

---

1 See note added in proof at end.
bijections \( f : C_0 \times C_1 \) by \( f((c_{0,j}, k_j))_{j<\omega} = (f_j(c_{0,j}, k_j))_{j<\omega} \) for each \( (c_{0,j}, k_j)_{j<\omega} \in C_0 \).

Once again let \( j \) be given, and for each \( i < 2 \), define the automorphism \( g_{ij} \) of \( C_i \) by \( g_{ij}(c_{i,j}) = c_{i,j,2+i} \), and \( g_{ij}(c_{im,1}) = c_{im,1} \) for \( m \neq j \). It is easily seen that these equations define \( g_{ij} \) completely, and moreover, for any \( j \) we have \( f(g_{0j}(c)) = g_{1j}(f(c)) \) for every \( c \in C_0 \).

Let \( I \) be the set of all finite subsets of \( C \), and let \( G \) be the group of all permutations \( g \) of \( C \) satisfying the following:

1. \( g^n C_i = C_i \) and \( g|C_i \) is an automorphism of \( C_i \), \( i < 2 \);
2. \( f(g(c)) = g(f(c)) \) for every \( c \in C_0 \).

From (1) we see that each \( g \in G \) can be expressed as an ordered pair \( (g_0, g_1) \), where \( g_i \) is an automorphism of \( C_i \), \( i < 2 \), and from (2) and the preceding remarks we see that \( g_j = (g_{0j}, g_{1j}) \in G \) for each \( j < \omega \).

It is easily seen that \( I \) is a normal ideal with respect to \( G \), and so by I.1, I.2 of [1] we have an FM-model \( V = V(G, I) \) such that for every \( x \) we have \( x \in V \) if and only if \( x \subseteq C \) and \( S_x \subseteq G_x \) for some \( X \in I \). It is \( V \) that is the FM-model we require.

We know from the general properties of \( V \) (see [1]) that \( C \in V \) and that \( V \) is a transitive class — that is, \( x \subseteq V \) for every \( x \in V \). Hence we have \( C_i \subseteq V \) for each \( i < 2 \). But from (1) above we have \( G_{C_i} = G \), and so \( S_\emptyset \subseteq G_{C_i} \). Thus \( C_i \in V \), and we must now show that the appropriate group structure on \( C_i \) is contained in the model \( V \).

We put \( K_i = \{(c_0, c_1, c_2) \in C_i \times C_i \times C_i \mid c_0 + c_1 = c_2 \} \), \( i < 2 \).

The set \( K_i \) represents the group structure of \( C_i \). Now \( V \) is an FM-model, and we have established that \( C_i \in V \). Hence \( C_i \times C_i \times C_i \in V \), and so \( C_i \times C_i \times C_i \subseteq V \). Thus \( K_i \subseteq V \). But for any \( g \in G \) and any
\((a_0, a_1, a_2) \in K_i\), we have \(g((a_0, a_1, a_2)) = (g(a_0), g(a_1), g(a_2))\) (see \([1]\), p. 204). It follows from this and from (1) that \(g''K_i = K_i\) for each \(g \in G\), that is, \(G_{K_i} = G\). Thus \(K_i \subseteq V\). Therefore \(V\) contains the group \(C_i\), and of course within \(V\) the group \(C_i\) is still an elementary abelian \(p\)-group.

We now turn our attention to the bijection \(f : C_0 \to C_1\). We have of course \(f \subseteq C_0 \times C_1\), and so as above we obtain \(f \subseteq V\). Take any \((a_0, a_1) \in f\) and any \(g \in G\); then \(g((a_0, a_1)) = (g(a_0), g(a_1))\). But by (2) we have \(g(a_1) = g(f(a_0)) = f(g(a_0))\), and so \((g(a_0), g(a_1)) \in f\).

It follows from this that \(g'' f = f\) for each \(g \in G\); thus \(f \notin V\). Since it is clear that within \(V\) the set \(f\) is still a bijection \(C_0 \to C_1\), it follows that within the model \(V\) we have \(|C_0| = |C_1|\).

It remains to show that within \(V\) there is no isomorphism \(C_0 \to C_1\). Suppose that \(h\) is such an isomorphism. By the rules of the game, there must exist \(X \subseteq I\) such that \(S_X \subseteq G_h\) — that is, for each \(g \in G\), if \(g(x) = x\) for every \(x \in X\), then \(g'' h = h\). Now \(X\) is finite, and so if we let \(D_i\) be the subgroup of \(C_i\) generated by \(X \cap C_i\), then we must have \(D_i \cap C_i^{*j} = \{0_i\}\) for all but a finite number of \(j\). Hence we can certainly choose \(j^*\) such that \(D_0 \cap C_0^{*j^*} = \{0_0\}\) and \(D_1 \cap C_1^{*j^*} = D_1 \cap h'' C_0^{*j^*} = \{0_1\}\).

Put \(g = (g_{0j^*}, g_{1j^*})\), where the \(g_{ij}\) are as defined previously. Then \(g \notin G\), and it is clear from our choice of \(j^*\) that \(g \in S_X\). Now put \(c = h(a_{0j^*}^{*j^*}, 1)\). Then \(g(a_{0j^*}^{*j^*}, 1) = 2a_{0j^*}^{*j^*}, 1\), whilst \(g(c) = 3^k c\) for some \(k < p\), and so \(g((a_{0j^*}^{*j^*}, 1, c)) \notin h\), whence \(g'' h \neq h\); that is, \(g \notin G_h\). This contradiction shows that no such isomorphism exists, and so our result is established for FM set theory; we now transfer it to ZF set theory by means of the Jech-Sochor Embedding Theorem (see \([1]\)).
Note added in proof [21 March 1977]. When a set theorist starts having delusions that he is an algebraist, he is sometimes aroused from his daydreams with a very nasty jolt. This act of awakening was performed upon me by Professor B.H. Neumann, who pointed out that the relation $f_j \subset C_{0j} \times C_{1j}$ defined at the bottom of p. 214 is a bijection if and only if 2 and 3 are both primitive roots of $p$; such of course is not always the case. In fact, in certain cases, $f_j$ is not even a function.

We correct this mistake by choosing, for a given prime $p \geq 5$, two distinct primitive roots $q, r$ of $p$, and replace 2 by $q$ and 3 by $r$ (such primitive roots always exist). The function $g_{ij}$ defined on p. 215 must now have the defining relations $g_{0j}(\alpha_{0j,1}^*) = \alpha_{0j,q}^*$, $g_{1j}(\alpha_{1j,1}^*) = \alpha_{1j,r}^*$, and $g_{ij}(\alpha_{im,1}^*) = \alpha_{im,1}^*$ for $i < 2$ and $m \neq j$.

Finally, the equations "$g(\alpha_{0j,1}^*) = 2\alpha_{0j,1}^*$" and "$g(\sigma) = 3^{k}\sigma$" in the final paragraph of p. 216 must be corrected appropriately. The proof now goes through as planned.

I am indebted to Professor Neumann for drawing the mistake to my attention, and for suggesting the above correction.

Reference