BULL. AUSTRAL. MATH. SOC.
VOL. 14 (1976), 199-232.

02K05, 02K10, 20A99, 20F15
(02K20, 20F10, 20F55, 20K30)

The construction of groups in models of set theory that fail the Axiom of Choice

J.L. Hickman

The purpose of this paper is to show that a well-known method for constructing "queer" sets in models of ZF set theory is also applicable to certain algebraic structures. An infinite set is called "quasi-minimal" if every subset of it is either finite or cofinite. In Section 1 I set out the two systems of set theory to be used in this paper, and illustrate the technique in its most fundamental form by constructing a model of set theory containing a quasi-minimal set. In Section 2 I show that by choosing the parameters appropriately, one can use this technique to obtain models of set theory containing groups whose carriers are quasi-minimal. In the third section various independence results are deduced from the existence of such models: in particular, it is shown that it is possible in ZF set theory to have an infinite group that satisfies both the ascending and descending chain conditions. The quasi-minimal groups constructed in Section 2 were all elementary abelian; in Section 4 it is shown that this was not just chance, but that in fact all quasi-minimal groups must be of this type. Finally in Section 5 permutations and permutation groups on quasi-minimal sets are examined.

Received 25 November 1975. The work contained in this paper was done whilst the author was a Research Fellow at the Australian National University. He wishes to express his grateful thanks to Professor B.H. Neumann for initiating this piece of research and for many illuminating conversations subsequently; to Dr Chéryl E. Praeger for almost all the work contained in Section 4; and to Dr M.F. Newman for answering a variety of questions on group theory.

1.

An infinite set X is called "quasi-minimal" if for every subset Y of X, either Y or $X - Y$ is finite. In "ordinary" set theory in which the Axiom of Choice is assumed, quasi-minimal sets clearly do not exist; the situation changes, however, once Choice is jettisoned.

Perhaps the most familiar system of axiomatic set theory is that of Zermelo-Fraenkel (ZF). If the Axiom of Choice (AC) is adjoined, then the resulting theory is denoted by "ZFC" and constitutes - in the present author's opinion - an adequate foundation for classical analysis, algebra, and various other well-known branches of mathematics. Without AC, however, things become "sticky"; certain elementary theorems are no longer elementary, and in some cases are no longer true. By constructing quasi-minimal groups - groups whose carriers are quasi-minimal - we will show that various well-known results in elementary group theory are among those that must be dropped.

The construction of ZF models that fail Choice is a fairly complex process; hence we choose an indirect route and proceed via models of a system of set theory usually known as Fraenkel-Mostowski (or Fraenkel-Mostowski-Specker) set theory. We denote this by "FM", and by "FMC" when Choice is added. Because FM set theory is probably not as well-known as ZF, we shall set forth both systems in order that a comparison may be made. Firstly, however, we require some notational conventions.

Sets (and urelemente; see later) will in general be denoted by lower case Latin letters; there will, however, be occasions when it will seem more natural to use upper case letters. An algebraic structure will be denoted by an upper case script letter, and its carrier by the corresponding upper case Latin letter.

For any set x, the powerset $\{y; y \subseteq x\}$ is denoted by "$P(x)$", and the union $\{z; \exists y(y \in x \& z \in y)\}$ by "$\cup x$". The difference $\{z; z \in x \& z \notin y\}$ between two sets x and y is denoted by "$x - y$", and the empty set is denoted by "$\emptyset$".

If there exists an injection $f : x \to y$ from the set x to the set y, then we say that the cardinality of x is less than or equal to that of y, and write "$|x| \leq |y|$". It is provable in ZF that for any x, y, if $|x| \leq |y|$ and $|y| \leq |x|$, then there is a bijection $f : x \to y$.

https://doi.org/10.1017/S0004972700025041 Published online by Cambridge University Press

This last is naturally written "$|x| = |y|$" . It is not provable in ZF that for any x, y , either $|x| \leq |y|$ or $|y| \leq |x|$. If neither of these hold, then we say that the cardinalities are incomparable and write "$|x| \parallel |y|$" .

Since we do not wish to delve into the nature of cardinality in ZF and FM set theories, we shall not make formal use of the symbol "$|\ |$" outside those situations mentioned above. In practice, however, this will not deter us from using the notation "$|x|$" when the context renders our meaning clear.

A set x is said to be $\in$-well-ordered when the membership relation $\in$ induces a well-ordering upon x , and to be transitive when $\cup x \subseteq x$.

An ordinal is defined to be an $\in$-well-ordered, transitive set all of whose elements are sets. This last condition is superfluous in ZF but required in FM. Thus the first few ordinals are $0 = \emptyset$, $1 = \{0\}$, $2 = \{0, 1\}$, ...,, $\omega = \{0, 1, 2, \ldots\}$. We always denote the first transfinite ordinal by "ω" : ordinals in general are usually denoted by lower case Greek letters, although occasionally we find it convenient to denote finite ordinals (natural numbers) by "k", "m", "n", "p", "q" .

Let the set x be given. For each ordinal α we define the set $P^{\alpha}(x)$ by transfinite induction on α as follows:

$$P^{0}(x) = x \ ; \tag{1.1}$$

$$P^{\beta+1}(x) = P^{\beta}(x) \cup P\big(P^{\beta}(x)\big) \ ; \tag{1.2}$$

$$P^{\gamma}(x) = \cup\{P^{\alpha}(x);\ \alpha < \gamma\} \quad \text{for } \gamma \text{ a nonzero limit ordinal.} \tag{1.3}$$

We can now define the *class* $P^{\infty}(x)$ by

$$P^{\infty}(x) = \cup\{P^{\alpha}(x);\ \alpha \text{ is an ordinal}\} \ . \tag{1.4}$$

As we are taking the union of a proper class in (1.4), the above definition of $P^{\infty}(x)$ must be regarded as a purely informal one. Nevertheless, the intuitive meaning of $P^{\infty}(x)$ is clear, and is sufficient for our purposes.

In the two set theories that we are to present - and in most other set theories - the underlying logic is that of the normal predicate calculus enriched by the addition of the equality symbol and the appropriate

https://doi.org/10.1017/S0004972700025041 Published online by Cambridge University Press

equality axioms and axiom schemes.

ZF set theory is a first order axiomatic system with one nonlogical constant. This constant is a binary predicate, which we shall denote by "$\in$" ; of course from an intuitive point of view this is the membership relation. There are six axioms and one axiom scheme, which are set out below. In the scheme $A7_\Delta$, Δ is assumed to be a well-formed formula of the ZF language containing x, y as free variables but neither t nor z as free variables.

A1 (Extensionality). *For all* x, y , *we have* $x = y$ *if and only if*

$$\forall z(z \in x \Leftrightarrow z \in y) .$$

A2 (Nullset). *There exists* x *such that* $\forall y(y \notin x)$; $(x = \emptyset)$.

A3 (Union). *For every* x , *there exists* y *such that*

$$y = \{z; \exists t(t \in x \ \& \ z \in t)\} ; \quad (y = \cup x) .$$

A4 (Powerset). *For every* x , *there exists* y *such that*

$$y = \{z; \forall t(t \in z \Rightarrow t \in x)\} ; \quad \big(y = P(x)\big) .$$

A5 (Infinity). *There exists* x *such that*

$$\emptyset \in x \ \& \ \forall y(y \in x \Rightarrow y \cup \{y\} \in x) .$$

A6 (Foundation). *For every* $x \neq \emptyset$, *there exists* y *such that*

$$y \in x \ \& \ y \cap x = \emptyset .$$

$A7_\Delta$ (Replacement). *Assume that for every* x *there is at most one* y *such that* $\Delta(x, y)$.

Then for every z , *there exists* t *such that*

$$t = \{u; \exists v(v \in z \ \& \ \Delta(v, u)\} .$$

The Axiom of Choice may be formulated as follows.

AC. For every $x \neq \emptyset$ such that $\emptyset \notin x$, there exists a function $f : x \to \cup x$ with the property that $f(y) \in y$ for every $y \in x$.

As an immediate consequence of A1 and A2 we have the ZF-theorem $\forall x\big(x \neq \emptyset \Rightarrow \exists y(y \in x)\big)$. It is this result that lies at the heart of the difference between ZF and FM set theories. In FM we wish to allow the

https://doi.org/10.1017/S0004972700025041 Published online by Cambridge University Press

existence of "sets" that are distinct from the empty set - and from one another - and yet have no elements. FM set theory can be described in a variety of ways; we shall follow fairly closely the presentation given by Jech in Chapter 4 of [3].

The language of FM is obtained from that of ZF by adjoining one extra nonlogical constant; this constant, which we shall denote by "U" , is a unary predicate. The variables in ZF are supposed to range over sets; in FM, a variable x represents a "set" only if $U(x)$ does not hold; otherwise, x represents an "urelement". Intuitively, we think of urelemente as being sets having the property mentioned above.

FM set theory is now obtained from ZF by altering the ZF axioms in such a way that any contradiction that could be produced from the altered axioms in conjunction with the additional axiom $\exists x U(x)$ could have been produced from the original ZF system; in somewhat more technical parlance, we wish FM to be relatively consistent with ZF. Since we want ZF and FM to be allied theories, we do as little tampering with the ZF axioms as possible. This results in the following modifications being made to axioms A1, A2, and A6.

A1*. *For all* sets x, y , *we have* $x = y$ *if and only if*

$$\forall z(z \in x \iff z \in y) .$$

A2*. *There exists a* set x *such that* $\forall y(y \notin x)$.

A6*. *For every* set $x \neq \emptyset$, *there exists* y *such that*

$$y \in x \ \& \ y \cap x = \emptyset .$$

It is clear that if (intuitively) we take U to be the empty set, then ZF and FM are logically equivalent systems.

Let M be a set or class, and let E be a binary relation on M . The structure $\mathfrak{M} = (M, E)$ is said to be a ZF-model if all the ZF axioms hold in $\mathfrak{M}$ when $\in$ is interpreted by E . In a similar manner we can say what it means for a triple $\mathfrak{M}^0 = (M^0, E^0, U^0)$ to be an FM-model. We adopt the slovenly but highly convenient procedure of writing "$\in$" for "E" (or "E^0"), and of distinguishing different membership relations by subscripts in cases of ambiguity. A similar remark applies to the FM symbol "U" .

https://doi.org/10.1017/S0004972700025041 Published online by Cambridge University Press

Our aim, as avowed by the title of this paper, is to present a method for constructing groups in ZF-models that fail AC. We intend to obtain these ZF-models by first constructing special kinds of FM-models, called "permutation models", and then applying a result known as the Jech-Sochor Embedding Theorem, which enables one to transfer certain properties of a permutation model to a ZF-model. In particular, we shall be able to infer from the existence of a group with specified properties in a permutation model the existence of a group with similar properties in a ZF-model.

This of course still leaves us with the problem of constructing the required permutation models. Now permutation models are constructed as submodels of FM-models that *satisfy* AC. Hence, logically, our first task should be to construct an FMC-model that contains a specified group.

However, we defer this particular duty until the next section, and assume for the time being that we have an FMC-model M containing an infinite set U of urelemente. We wish to describe the method for obtaining permutation models as submodels of M, and throughout this description we assume that we are working entirely within M - to revert to set-theoretical jargon again, we are relativizing everything to M (see for example, [1], p. 98). This means, for instance, that for any set x (in M) we are taking the powerset $P(x)$ to be $\{y \in M;\ y \subseteq x\}$, which when expanded is the set $\{y \in M;\ \forall z(z \in M \Rightarrow (z \in y \Rightarrow z \in x))\}$. Other set-theoretical operations receive similar treatment.

Let G be a group of permutations of U. We can extend each $g \in G$ to a permutation (which we again denote by "g") of the class $P^{\infty}(U)$ in the following manner:-

$$g(\emptyset) = \emptyset \ ; \tag{1.5}$$

$$g(x) = \{g(y);\ y \in x\} \text{ , for } x \in P^{\infty}(U) - (U \cup \{\emptyset\}) \ . \tag{1.6}$$

This is a valid definition by transfinite induction on the rank $rk(x)$ of x, where $rk(x) = \min\{\alpha;\ x \in P^{\alpha}(U)\}$.

We note two invariance properties:

$$g(x) \in g(y) \iff x \in y \text{ , for all } x, y \in P^{\infty}(U) \text{ and } g \in G \ ; \tag{1.7}$$

$$g(x) = x \text{ for every } x \in P^{\infty}(\emptyset) \text{ and } g \in G \ . \tag{1.8}$$

Both these properties are easily proved by induction on rank; with regard

to (1.8), it is clear that $P^{\infty}(\emptyset) \subseteq P^{\infty}(U)$. In particular, (1.8) tells us that $g(\alpha) = \alpha$ for every ordinal α and every $g \in G$. Other invariance properties are given on p. 46 of [3].

Thus we may regard G as a group of permutations of the class $P^{\infty}(U)$. Let Γ be a filter of subgroups of G . We call Γ "normal" if

(1.9) $gFg^{-1} \in \Gamma$ for every $F \in \Gamma$ and every $g \in G$;

(1.10) $\{g \in G;\ g(u) = u\} \in \Gamma$ for every $u \in U$.

For each $x \in P^{\infty}(U)$, we define a subgroup G_x of G by $G_x = \{g \in G;\ g(x) = x\}$, and with respect to a group G and a normal filter Γ we say that x is symmetric if $G_x \in \Gamma$.

Finally, given G and Γ , we define the subclass $V = V(G, \Gamma)$ of $P^{\infty}(U)$ by

(1.11) $V = \{x \in P^{\infty}(U);\ G_x \in \Gamma \ \&\ x \subseteq V\}$.

Once again this is a valid definition by induction on $rk(x)$.

The fundamental theorem on permutation models is the following.

I.1. *Let* G, Γ *and* $V = V(G, \Gamma)$ *be as above, and put* $\mathcal{V} = (V, \in)$.

(i) V *is a transitive class and* $P^{\infty}(\emptyset) \subseteq V$.

(ii) $U \in V$.

(iii) $\mathcal{V}$ *is an* FM*-model with* U *as the set of urelemente.*

The FM-model $\mathcal{V}$ in I.1 is called a "permutation model", and its description was given in complete generality. For our purposes, however - and indeed for most practical purposes - this degree of generality is unnecessary, and we can narrow our range somewhat by placing some restrictions on the normal filter Γ .

Let $\mathcal{I}$ be an ideal on the powerset $P(U)$ of U . We say that $\mathcal{I}$ is normal if the following conditions are fulfilled:-

(1.12) $g''X \ (= \{g(x);\ x \in X\}) \in \mathcal{I}$ for every $X \in \mathcal{I}$ and $g \in G$;

(1.13) $\{u\} \in \mathcal{I}$ for every $u \in U$.

For each $x \in P^{\infty}(U)$, we define the subgroup $S_x \ (= S_{G,x})$ of G by

https://doi.org/10.1017/S0004972700025041 Published online by Cambridge University Press

$S_x = \{g \in G;\ \forall y \in x(g(y) = y)\}$. Now let Γ be the filter of subgroups of G generated by the set $\{S_X;\ X \in I\}$. It is not difficult to see that if I is a normal ideal, then Γ is a normal filter. In this manner we obtain an FM-model $V = V(G, I)$ from a group G of permutations of U and a normal ideal I on $P(U)$.

The following result, whose proof essentially consists of just looking at the appropriate definitions, is of considerable importance to us.

I.2. *Let* $V = V(G, I)$ *be the* FM-*model described above, and take* $x \in P^{\infty}(U)$. *Then* $x \in V$ *if and only if* $x \subseteq V$ & $\exists X \in I(S_X \subseteq G_x)$.

Proof. The result will follow once we show that $\Gamma = \{H \leq G;\ \exists X \in I(S_X \subseteq H)\}$. Now Γ is the smallest filter of subgroups of G such that $S_X \in \Gamma$ for every $X \in I$. Now if Γ° is any filter of subgroups of G containing each such S_X and H is any subgroup of G such that $S_X \subseteq H$ for some $X \in I$, then clearly $H \in \Gamma^{\circ}$. It follows at once that $\Gamma \supseteq \{H \leq G;\ \exists X \in I(S_X \subseteq H)\}$., and so all that we have to do is to show that the right hand side is indeed a filter.

Put $\Delta = \{H \leq G;\ \exists X \in I(S_X \subseteq H)\}$. Clearly if we have $H \leq H^{\circ} \leq G$ and $H \in \Delta$, then we must also have $H^{\circ} \in \Delta$. Thus take $H_0, H_1 \in \Delta$, and let H be their intersection. There exist $X_0, X_1 \in I$ such that $S_{X_i} \subseteq H_i$, $i = 0, 1$; put $X = X_0 \cup X_1$. Since I is an ideal, we have $X \in I$, and we claim that $S_X \subseteq H$.

For take $g \in S_X$. Then $g(x) = x$ for all $x \in X$, and so certainly $g \in S_{X_i}$, $i = 0, 1$. Thus $g \in H_i$, $i = 0, 1$, and so $g \in H = H_0 \cap H_1$. Hence $S_X \subseteq H$, whence $H \in \Delta$.

This shows that Δ is a filter.

Before we proceed any further, we must clarify our notations of finiteness and infinite. A set X is said to be finite if there is some natural number n for which we have an injection $f : X \to n$; X is otherwise said to be infinite. It is easily proved in ZF that X is

https://doi.org/10.1017/S0004972700025041 Published online by Cambridge University Press

infinite if and only if for each natural number n there is an injection $f : n \to X$.

We define X to be Dedekind-finite if there is no proper subset Y of X for which we have an injection $f : X \to Y$; otherwise X is called "Dedekind-infinite". In ZF we can show that every finite set is Dedekind-finite: in ZFC the converse is also provable. A very useful result (provable in ZF) is the following: a set X is Dedekind-finite if and only if there is no injection $f : \omega \to X$.

An infinite Dedekind-finite set is called "medial". Medial sets can be divided into two categories:

(i) medial sets X for which $P(X)$ is Dedekind-finite (and thus medial), and

(ii) medial sets X for which $P(X)$ is Dedekind-infinite.

It is readily provable in ZF that for any set X , we have X finite if and only if $P\big(P(X)\big)$ is Dedekind-finite.

Of those medial sets belonging to the first of the two categories above, the quasi-minimal sets are for our purposes the most important. As stated previously, a set X is said to be quasi-minimal if for every subset Y of X exactly one of Y and $X - Y$ is infinite. A proof of the fact that if X is quasi-minimal then $P(X)$ is medial may be found in [2] as a special case of a slight stronger result.

Quasi-minimal sets are called "amorphous" by Jech in [3].

A structure is said to be medial (quasi-minimal) if its carrier is medial (quasi-minimal).

The above results still hold when ZF and ZFC are replaced by FM and FMC respectively.

We conclude this section by constructing a permutation model that contains a quasi-minimal set. Our reasons for presenting this result, which is fairly well-known in set theory, are two-fold. Firstly, the construction that we shall set forth is perhaps the clearest possible demonstration of the method of permutation models; it illustrates the skeleton of the process, unadorned with any complicating algebraic structure. Hence it will assist in delineating the respective roles played

https://doi.org/10.1017/S0004972700025041 Published online by Cambridge University Press

by set theory and algebra in later sections. Our second reason is more prosaic, and is simply that later on in the paper we shall return to this model in order to demonstrate a rather interesting result about symmetric groups on quasi-minimal sets.

The construction of any model of set theory always presumes a "universal" set theory; in other words, we can only construct a model of set theory if we assume that everything is taking place within a larger model (not necessarily of the same type). Thus to save tedious repetitions, we make a blanket assumption for the remainder of this paper that we are working within a ZFC universe; in succeeding sections we shall be making assumptions concerning "subuniverses", and these will be made explicit at the relevant stages.

Since it is well-known that a ZFC-model can always be constructed from a ZF-model, our blanket assumption reduces to the one that ZF set theory is consistent.

Let T be some theory, $\mathcal{R}$ be some model of T, and Δ be a well-formed formula in the language of T. We use "$T \vdash \Delta$" and "$\mathcal{R} \models \Delta$" respectively to mean that Δ is provable in T and that Δ holds in $\mathcal{R}$.

I.3. *There is an* FM*-model containing a quasi-minimal set.*

Proof. Let M be an FMC-model containing an infinite set U of urelemente. (The existence of such a model will be proved in the next section.) Within M, let G be the symmetric group on U, and let I be the ideal on $P(U)$ consisting of all finite subsets of U. Clearly I is normal. Thus by I.1 we obtain an FM-model $V = V(G, I)$ with U as its set of urelemente.

We claim that $V \models$ "U is quasi-minimal". Firstly, we show that $V \models$ "U is infinite". Suppose that this is not the case. Then there must exist $f \in V$ such that for some natural number n, we have $V \models$ "$f : U \to n$ is an injection". (It follows from I.1 that $m \in V$ for every natural number m.) Now $V \subseteq M$, and thus $f \in M$. Moreover, from the construction of V it follows that $M \models$ "$f : U \to n$ is an injection". (We recall that from a set-theoretical point of view, f is a subset of $U \times n$.) Thus we have $M \models$ "U is finite", which contradicts our initial assumption. Therefore we must have $V \models$ "U is infinite".

https://doi.org/10.1017/S0004972700025041 Published online by Cambridge University Press

Now suppose that there is $U^\circ \in V$ such that $V \models U^\circ \subseteq U$ and $V \models$ "U° and $U - U^\circ$ are both infinite". By the same argument as above we obtain $U^\circ \in M$, $M \models U^\circ \subseteq U$ and $M \models$ "U° and $U - U^\circ$ are both infinite". By I.2 there is $E \in M$ such that $M \models$ "$E \subseteq U$ & E is finite & $S_E \subseteq G_{U^\circ}$". Then we can choose (in M) elements $u_0 \in U^\circ$ and $u_1 \in U - U^\circ$ such that $u_0, u_1 \notin E$, whence $M \models \exists g(g \in S_E \;\&\; g(u_0) = u_1 \;\&\; g(u_1) = u_0)$. Let g° be one such g. Then $g^\circ \in G_{U^\circ}$, and hence by (1.7) we have $M \models u_1 \in U^\circ$. But we chose u_1 such that $M \models u_1 \in U - U^\circ$.

This contradiction shows that there is no such $U^\circ \in V$. Thus we have $V \models$ "U is quasi-minimal".

2.

It is now necessary to justify our assertions in the preceding section concerning the existence of FMC-models. Since, however, we wish to construct models containing specific groups, we have to say first of all what we mean by the statement "A model M contains a group G".

Let G be a group. Then there exists a subset X of $G \times G \times G$ defined by $X = \{(g_0, g_1, g_2) \in G \times G \times G;\ g_0 g_1 = g_2\}$. We shall call X the "structure" of G. If now M is a model of set theory, we say that M contains the group G if $G \in M$ and $X \in M$.

II.1. *Let G be an infinite group. Then there is an isomorphic copy U of G and an* FMC*-model M containing U and such that U is the set of urelemente in M.*

REMARK. The isomorphism between G and U exists of course in the universe, and not necessarily in the model M.

Proof. Let α_0 be the smallest ordinal α for which there exists an injection $G \to \alpha$ (such ordinals exist by AC). We recall that $\alpha_0 = \{\beta;\ \beta < \alpha_0\}$, and put $B = \{x \subseteq \alpha_0;\ |x| = |\alpha_0|\}$. Let $b \in B$ be specified; b is going to play the role of the empty set in our FMC-model. Clearly $|\alpha_0| \leq |B - \{b\}|$, and so there exists an injection $G \to B - \{b\}$. We let t be such an injection, and put $U = t''G$ $(= \{t(g);\ g \in G\})$. If

https://doi.org/10.1017/S0004972700025041 Published online by Cambridge University Press

we now define $X \subseteq U \times U \times U$ by $X = \{(t(g_0), t(g_1), t(g_2)); g_0 g_1 = g_2\}$, it is obvious that X is a group structure for U and that the resulting group $\mathcal{U}$ is isomorphic to G.

For each ordinal α we define the set M_α by the following scheme:

(2.1) $M_0 = U \cup \{b\}$;

(2.2) $M_{\beta+1} = M_\beta \cup (P(M_\beta) - \{\emptyset\})$;

(2.3) $M_\gamma = \bigcup\{M_\delta; \delta < \gamma\}$ for each nonzero limit ordinal γ.

Put $M = \bigcup\{M_\alpha; \alpha \text{ is an ordinal}\}$, and denote the restriction $\in | (M \times M)$ of the membership relation $\in$ to the class M again by "$\in$". We claim that $\mathcal{M} = (M, \in)$ is the desired model.

Obviously $U \in M$; we wish to show that $x \cap M = \emptyset$ for each $x \in M_0$. Suppose that this is not the case; then we must have some $x \in M_0$ such that $t \in M$ for some $t \in x$. But $x \subseteq \alpha_0$. Thus $\beta \in M$ for some $\beta < \alpha_0$; we may assume that β is minimal in this respect. Since $\beta \in M$, we have $\beta \in M_\alpha$ for some α ; let δ be the smallest such α. Now if $\delta > 0$, then an easy induction argument on (2.1)-(2.3) shows that $\beta \cap M_\gamma \neq \emptyset$ for some $\gamma < \delta$; since this implies that $\psi \in M$ for some $\psi < \beta$, we have shown that $\beta \in M_0$. However, α_0 was the *smallest* ordinal α for which there was an injection $G \to \alpha$, and thus we must have $|\beta| < |\alpha_0|$. Since this implies $\beta \notin M_0$, we have the desired contradiction.

We have shown in particular that b has (with respect to $\mathcal{M}$) the property required of the empty set, and we decree that henceforth b *is* the empty set of $\mathcal{M}$; we denote it by "$\emptyset_M$".

Now for each $x \in M - M_0$ we have $y \in x$ for some $y \in M$; this again is proved very easily by induction. But this fact, combined with the preceding results, tells us that U can be taken as the set of urelemente in $\mathcal{M}$.

Consider Extensionality, and take $x, y \in M - U$. If $x = y$, then of

https://doi.org/10.1017/S0004972700025041 Published online by Cambridge University Press

course we have $\forall z \in M(z \in x \iff z \in y)$. Thus assume that $\forall z \in M(z \in x \iff z \in y)$. From this we conclude (by an argument similar to the one above) that $x = \emptyset_M \iff y = \emptyset_M$, and so we may assume that $x, y \in M\text{-}M_0$. Let δ be the smallest ordinal α for which $x \in M_\alpha$: then $\delta = \gamma + 1$ for some γ , and $x \subseteq M_\gamma \subseteq M$. Similarly we can show that $y \subseteq M$. But as we are assuming $\forall z \in M(z \in x \iff z \in y)$, this gives $x = y$. Hence $M \models A1$.

The verification of the other ZF axioms requires arguments no more complex than the one above, and so we shall consider only Replacement. Let Δ be a formula such that for each $x \in M$ there is at most one $y \in M$ for which $\Delta(x, y)$, and take $a \in M$.

If $a \in M_0$, then clearly $\emptyset_M$ satisfies Replacement in M . Thus we may assume that $a \notin M_0$, whence it follows (as above) that $a \subseteq M$. Define a formula Δ° as follows:-

$$\Delta^\circ(x, y) \equiv y = \emptyset \vee \big(x \in a \ \& \ \Delta(x, y)\big) .$$

Then Δ° satisfies Replacement in the universe, and so there is a set c given by $c = \{v; \exists u \in a(\Delta^\circ(u, v))\}$. Clearly $c \subseteq M$, and as c is a set in the universe, we must have $c \subseteq M_\alpha$ for some α .

Now if $c = \emptyset$, then once again $\emptyset_M$ satisfies $A7_\Delta$ in M . On the other hand, if $c \neq \emptyset$, then $c \in M_{\alpha+1}$ and is itself the required set.

We now show that $M \models AC$, and we do this by showing that every $x \in M$ has a well-ordering in M . Obviously we may assume x infinite in M , whence $x \notin M_0$. Now AC holds in the universe, and so there exists $w \subseteq x \times x$ such that w well-orders x . But $x \times x \subseteq M$, and so $w \subseteq M$. Since w is a set, we have $w \in M$.

Finally we must show that M contains U . Since $U \in M$, it suffices to show that $X = t''G \in M$. Now since we have just shown that M is an FMC-model, it follows from $U \in M\text{-}M_0$ that $U \times U \times U \in M\text{-}M_0$. Thus $X \subseteq M$. But X is a set and $X \neq \emptyset$; hence $X \in M$.

This proves our theorem.

https://doi.org/10.1017/S0004972700025041 Published online by Cambridge University Press

Just as in the proof of I.3, we can show that U is infinite in M; and so our assumption of the existence of an FM-model with an infinite set of urelemente that was made in the proof of I.3 has been justified.

For the benefit of those readers - if any - whose knowledge of group theory is not much superior to the author's, we recall that a group is called a "p-group" (where p is some prime) if the order of each nontrivial element is p^n for some n. In the special case in which n is always 1 and the group is moreover abelian, the group is called "elementary abelian".

II.2. *Let p be a prime. There exists an* FM*-model containing a quasi-minimal, elementary abelian p-group.*

Proof. By II.1 there exists an FMC-model M containing an infinite, elementary abelian p-group. Let this group be $\mathcal{U}$, with U as the set of urelemente in M. Let G be the automorphism group $\mathrm{aut}(\mathcal{U})$ of $\mathcal{U}$, and let $\mathcal{I}$ be the ideal on $P(U)$ consisting of all finite subsets of U; we define both $\mathcal{U}$ and $\mathcal{I}$ within M.

We see easily that $\mathcal{I}$ is normal, and so we obtain an FM-model $V = V(G, \mathcal{I})$ containing U as the set of urelemente in V. Let X be the structure of $\mathcal{U}$ in M; since each $g \in G$ is an automorphism of $\mathcal{U}$, it follows from (1.7) that $g(X) = X$. Thus $S_{\emptyset_M} \subseteq G_X$, and so by I.2 we have $X \in V$. Thus V contains $\mathcal{U}$.

Since the group $\mathcal{U}$ has the same structure X in V as in M, we see that $V \models$ "$\mathcal{U}$ is an elementary abelian p-group"; the proof that $V \models$ "U is infinite" is exactly as in the proof of I.3.

Suppose that there exists $U^\circ \in V$ such that we have

$$V \models \text{"}U^\circ \subseteq U \;\&\; U^\circ \text{ is infinite } \&\; U - U^\circ \text{ is infinite"}.$$

Then, as in I.3, we have $U^\circ \in M$ and

$$M \models \text{"}U^\circ \subseteq U \;\&\; U^\circ \text{ is infinite } \&\; U - U^\circ \text{ is infinite"}.$$

We now work entirely within M.

By I.2 there exists a finite subset E of U with $S_E \subseteq G_{U^\circ}$. Since $\mathcal{U}$ is locally finite, the subgroup $[E]$ of $\mathcal{U}$ generated by E is finite. By AC we can express $\mathcal{U}$ as the direct sum - we adopt the usual convention of writing abelian groups additively - of an infinite family

https://doi.org/10.1017/S0004972700025041 Published online by Cambridge University Press

$(C_j)_{j\in J}$ of cyclic groups of order p. Let J° be the finite subset of J such that $[E]$ is the direct sum of the family $(C_j)_{j\in J^\circ}$. Let the carrier of $[E]$ be E°. [See note added in proof.]

We abuse the language slightly and regard each C_j as a subset of U. Now since E° is finite whilst U° and $U - U^\circ$ are both infinite, there exist $j_0, j_1 \in J-J^\circ$ with $C_{j_0} \subseteq U^\circ - E^\circ$ and $C_{j_1} \subseteq (U-U^\circ) - E^\circ$. Let e_i be the identity of C_{j_i}, $i = 0, 1$, and choose $c_i \in C_{j_i} - \{e_i\}$. Then there exists $g \in G$ such that $g(c_0) = c_1$ and $g(u) = u$ for every $u \in E^\circ$.

It follows that $g \in S_E$, and so $g(U^\circ) = U^\circ$. However, c_0 was chosen so that $c_0 \in U^\circ$, and so by (1.7) we must have $c_1 = g(c_0) \in g(U^\circ) = U^\circ$, contradicting the fact that $c_1 \in U-U^\circ$.

We must therefore conclude that no such U° exists in V, whence we have $V \models$ "U is quasi-minimal".

We have shown thus far that it is relatively consistent with FM to assume the existence of a quasi-minimal group. In order to obtain the same consistency result relative to ZF, we apply the Jech-Sochor Embedding Theorem, which says - roughly speaking - that if we are given a bounded initial segment of a permutation model, then there is a ZF-model containing a set that is $\in$-isomorphic to this segment. The Embedding Theorem, its proof, and its variants, are set forth in Chapter 6 of [3].

Before stating the Embedding Theorem, we require some preliminary notation.

Within the universe, let N be a model of set theory, and let S be a set in N. Then by "$P(S)^N$" we mean the set $\{T \subseteq S;\ T \in N\}$. It can be shown - though we do not show it here - that $P(S)^N = P(S) \cap N$. Of course $P^\alpha(S)^N$ is defined similarly.

With this notation we may state the appropriate form of the Embedding Theorem as follows.

https://doi.org/10.1017/S0004972700025041 Published online by Cambridge University Press

II.3. *Let* M *be an* FMC*-model with* U *as its set of urelemente, and let* α *be an ordinal in* M. *Then for every permutation model* V *obtained from* M *in the usual manner, there is a* ZF*-model* N *and a set* $\overline{U}$ *in* N *such that*

(i) N *is a transitive class;*

(ii) $P^{\infty}(\emptyset_M)^M \subseteq N$;

(iii) $P^{\alpha}(U)^V$ *is* $\in$*-isomorphic to* $P^{\alpha}(\overline{U})^N$.

The $\in$-isomorphism mentioned in *(iii)* is of course defined in the universe. From this Embedding Theorem we can deduce our desired result.

II.4. *For any prime* p *, it is relatively consistent with* ZF *to assume the existence of a quasi-minimal, elementary, abelian* p*-group.*

Proof. We have seen that it is possible to construct an FMC-model M from which we can obtain a permutation model V containing a quasi-minimal, elementary, abelian p-group U , such that U is the set of urelemente in V . Let X be the structure of U in V .

Apply the Embedding Theorem with $\alpha = \omega$, and let $f : P^{\omega}(U)^V \to P^{\omega}(\overline{U})^N$ be the $\in$-isomorphism. It is clear that $X \in P^{\omega}(U)^V$ and that $f(X)$ defines a group structure for $\overline{U}$ in N , with the resulting group $\overline{U}$ being an elementary, abelian p-group.

Now finiteness is an absolute property; that is, the property of being finite is preserved between models. Thus for any $\overline{U}^{\circ} \in \overline{N}$ such that $N \models \overline{U}^{\circ} \subseteq \overline{U}$, we have $N \models$ "$\overline{U}^{\circ}$ is finite" if and only if $V \models$ "$f^{-1}(\overline{U}^{\circ})$ is finite".

It follows at once that $N \models$ "$\overline{U}$ is quasi-minimal", and so our theorem is proved.

3.

The result II.4 allows us to demonstrate that certain elementary theorems of group theory, provable in ZFC, are not provable in ZF alone. Firstly, however, we give a simple but useful result on quasi-minimal groups; the structure of quasi-minimal groups will be investigated more

https://doi.org/10.1017/S0004972700025041 Published online by Cambridge University Press

fully in the next section.

III.1. *Let G be a quasi-minimal group. Then:-*

(i) G is locally finite;

(ii) every proper subgroup of G is finite;

(iii) G has no independent set of generators.

Proof. *(i)* Let $S = \{g_0, g_1, \ldots, g_n\}$ be a finite subset of G, and suppose that the subgroup $[S]$ of G generated by S is infinite. Then $[S]$ of course is quasi-minimal; let the carrier of $[S]$ be S°. Consider the set T of all finite sequences whose terms belong to $S \cup S^{-1}$; formally, $T = \cup\{(S \cup S^{-1})^n; n < \omega\}$. Since S and hence $S \cup S^{-1}$ is finite, T can be well-ordered; let $<$ be a specified well-ordering of T.

Let $t_0 = (x_0, \ldots, x_m)$ and $t_1 = (y_0, \ldots, y_n)$ be two elements of T. We put $t_0 \sim t_1$ if $x_0 \ldots x_m = y_0 \ldots y_n$ in G. Obviously the binary relation $\sim$ thus defined on T induces a partition $\Theta = \{T_j; j \in J\}$ of T, and we can well-order Θ by setting $T_i < T_j$ if $\min T_i < \min T_j$. But the function $f : \Theta \to S^\circ$ defined by $f(T_j) = \min T_j$ is clearly bijective, and so we can well-order S°, which is absurd.

Thus S° must be finite.

(ii) Suppose that H is an infinite proper subgroup of G, and take $g \in G-H$. Then $gH = \{gh; h \in H\} \subseteq G - H$, and since H and gH are both infinite, this is a contradiction.

(iii) Let S be a set of generators for G; by *(i)*, we must have S infinite. Take $s \in S$; by *(ii)* we have $[S-\{s\}] = G$; thus S is not independent.

If a group G has a subgroup H, then what do we mean when we say that the order of G "divides" the order of H? Expressed in terms of cardinals, we mean that $|G| = |H|\kappa$ for some cardinal κ. And this, upon elimination of the concept of cardinal, means that there is a set X and a bijection $H \times X \to G$.

III.2. *Let G be a quasi-minimal group, and let H be a nontrivial,*

https://doi.org/10.1017/S0004972700025041 Published online by Cambridge University Press

proper subgroup of G .

Then the order of H *does not divide the order of* G .

Proof. Assume that there is some set X and some bijection $f : H \times X \to G$. Since H is proper, we must have H finite by III.1, and so X must be infinite. Furthermore, as H is nontrivial there must be $h_0, h_1 \in H$ with $h_0 \neq h_1$. But then $f''(\{h_0\} \times X)$ and $f''(\{h_1\} \times X)$ are disjoint infinite subsets of G , contradicting the fact that G is quasi-minimal.

III.3. *If* ZF *is consistent, then it is not provable within* ZF *that the order of any group is divisible by the orders of all its subgroups.*

III.4. *Let* G *be a quasi-minimal, elementary abelian* p*-group, for some prime* p . *Then* G *is not the direct sum of cyclic groups.*

Proof. Suppose that G is the direct sum of the family $(C_j)_{j \in J}$ of cyclic groups. Clearly each C_j has order p , whence it follows that J is infinite.

Now by assumption $?$ consists of all functions $f : J \to \cup\{C_j;\ j \in J\}$ such that

(3.1) $\qquad f(j) \in C_j$; for each $j \in J$;

(3.2) $\{j \in J;\ f(j) \neq O_j\}$ is finite, O_j being the identity of C_j .

Take a specific $j^\circ \in J$, and any $c_0, c_1 \in C_{j^\circ}$ with $c_0 \neq c_1$. Define $G_0, G_1 \subseteq G$ by $G_i = \{f \in G;\ f(j^\circ) = c_i\}$, $i = 0, 1$. Then G_0, G_1 are disjoint, infinite subsets of G , a contradiction.

III.5. *If* ZF *is consistent, then it is not provable within* ZF *that every elementary abelian group is the direct sum of cyclic groups.*

III.6. *Assume that* ZF *is consistent. Then*

(i) it is not provable within ZF *that a group satisfies the ascending chain condition if and only if every subgroup of it is finitely generated;*

(ii) it is not provable within ZF *that a group is finite if and*

https://doi.org/10.1017/S0004972700025041 Published online by Cambridge University Press

only if it satisfies both the ascending and descending chain conditions.

Proof. *(i)* Let G be a quasi-minimal group. Then G is infinite and by III.1 not finitely generated. On the other hand, $P(G)$ is medial, and so G satisfies both chain conditions.

This proves both *(i)* and *(ii)*.

It is a well-known ZFC theorem that a group satisfies the ascending chain condition if and only if every subgroup of it is finitely generated. It is only conjectured within ZFC, however, that a group is finite if and only if it satisfies both chain conditions.

We conclude this section with a result on coset representatives and factor groups of quasi-minimal groups.

III.7. *Let A be a disjointed set of finite sets such that*

(1) $|X| > 1$ *for each* $X \in A$;

(2) $S = \cup A$ *is quasi-minimal.*

Then A is quasi-minimal and $|S| \parallel |A|$.

Proof. Since S is infinite and each $X \in A$ is finite, we must have A infinite. However, if A_0 and A_1 are infinite disjoint subsets of A , then as A is disjointed $\cup A_0$ and $\cup A_1$ are infinite disjoint subsets of S , a contradiction. Thus A is quasi-minimal.

We must show that there is no injection $A \to S$, nor any injection $S \to A$. Suppose firstly that $f : A \to S$ is an injection, and define $g : A \to A$ by taking for each $X \in A$ the value $g(X)$ to be the unique $Y \in A$ such that $f(X) \in Y$.

Since A is quasi-minimal, there is no injection $\omega \to A$, and so for each $X \in A$ there is a smallest natural number $n = n(X) > 0$ such that $g^n(X) = g^m(X)$ for some $m < n$; we call the set

$$\{g^m(X), g^{m+1}(X), \ldots, g^{n-1}(X)\}$$

the "cycle" of X and denote it by "C_X" . Our first task is to show that for each $X \in A$ the set $\{Y \in A; C_Y = C_X\}$ is finite. Let $X \in A$ be

https://doi.org/10.1017/S0004972700025041 Published online by Cambridge University Press

given.

For each $p < \omega$, define the set $B_p \subseteq A$ by

$$B_p = \left\{Y \in A;\ g^{p+1}(Y) \in C_X \ \&\ g^p(Y) \notin C_X\right\} . \tag{3.3}$$

Then the sets B_p are pairwise disjoint, and so as $P(A)$ is medial we must have $B_m = \emptyset$ for all $m \geq q$, for some number q.

Take $Y \in B_0$; then by definition we have $g(Y) \in C_X$, that is, $f(Y) \in \cup C_X$. But C_X is finite; each $Z \in C_X$ is finite; and f is an injection. It follows that B_0 is finite.

Now assume that B_p is finite, and take $Y \in B_{p+1}$. Then $g(Y) \in B_p$, that is, $f(Y) \in \cup B_p$, and we can conclude exactly as above that B_{p+1} is finite. Thus B_p is finite for every p.

But clearly $\{Y \in A;\ C_Y = C_X\} = C_X \cup \cup\{B_p;\ p < \omega\}$. Since $B_m = \emptyset$ for every $m \geq q$, we see that $\{Y \in A;\ C_Y = C_X\}$ is finite.

For each cycle C, put $D_C = \{X \in A;\ C_X = C\}$; we have just seen that each D_C is finite. But A is infinite and $A = \cup\{D_C;\ C \text{ is a cycle}\}$; therefore the set $\{C;\ C \text{ is a cycle}\}$ must be infinite.

Let C_0, C_1 be two distinct cycles, and suppose that there exists $X \in C_0 \cap C_1$. It is easy to see that we must have

$$C_0 = \{g^m(X);\ m < \omega\} = C_1 ,$$

which is a contradiction. Thus C_0, C_1 are disjoint; as A is a disjointed set it follows that $\cup C_0$, $\cup C_1$ are disjoint.

For each cycle C, put $T_C = \{f(X);\ X \in C\}$. Now for any $X \in C$, we have $f(X) \in g(X) \in C$; thus $T_C \subseteq \cup C$, and of course $T_C \neq \emptyset$. Moreover, we have by assumption $|g(X)| > 1$ for each $X \in C$, and so if we put

https://doi.org/10.1017/S0004972700025041 Published online by Cambridge University Press

$T^{o} = \cup C - T_C$, then we have $T^{o}_C \neq \emptyset$.

Finally, put $T = \cup\{T_C;\ C \text{ is a cycle}\}$, and $T^{o} = \cup\{T^{o}_C;\ C \text{ is a cycle}\}$: it follows from the above results that T and T^{o} are disjoint, infinite subsets of S .

Since this contradicts the fact that S is quasi-minimal, we must conclude that no such injection $f : A \to S$ can exist.

Suppose now that we have an injection $h : S \to A$. We define a non-increasing sequence (A_n) of subsets of A by $A_0 = A$ and $A_{n+1} = A_n \cap h''(\cup A_n)$. It is an easy proof by induction to show that each A_n is quasi-minimal.

We have seen that A is quasi-minimal, whence $P(A)$ is medial, and thus there is no injection $\omega \to P(A)$. It follows that for some p we must have $A_{p+1} = A_p$, that is, $h''(\cup A_p) \supseteq A_p$.

Letting f be the function $A_p \to \cup A_p$ induced by the restriction $h^{-1}|A_p$, we see that we have obtained a disjointed set B of finite sets such that

(i) $|X| > 1$ for every $X \in B$;

(ii) $\cup B$ is quasi-minimal; and

(iii) there is an injection $B \to \cup B$.

We can now repeat the argument contained in the first part of this proof to obtain a contradiction. We therefore conclude that no such injection $h : S \to A$ can exist.

This result enables us to deduce that the orders of various factor groups of quasi-minimal groups are incomparable, and perhaps it might not be inappropriate at this stage to remember that we must use some care in handling factor groups in this setting, since without AC we are no longer assured of the existence of a complete set of coset representatives. Indeed, we shall show below that a complete set of coset representatives never exists for a nontrivial proper subgroup of a quasi-minimal group.

https://doi.org/10.1017/S0004972700025041 Published online by Cambridge University Press

Thus if G is a group with a normal subgroup H, then we can still set up the factor group G/H as consisting of cosets Hg, $g \in G$; and we can still prove the "ordinary" things about G/H; but we are not permitted to use any infinite set of coset representatives of H, unless such a set can be defined explicitly or shown to exist by some other means acceptable in ZF set theory.

III.8. *Let G be a quasi-minimal group, and let H be a nontrivial, proper subgroup of G. Then there is no subset K of G such that $\{Hg;\ g \in K\}$ is a partition of G.*

Proof. Suppose that such a set K exists. Now H is a proper subgroup of G, and so H is finite by III.1. On the other hand, H is nontrivial, and thus $|H| > 1$. Thus by III.7 we see that K is quasi-minimal and that there is no injection $K \to G$. But as $K \subseteq G$ this is absurd.

III.9. *Let G be a quasi-minimal group with nontrivial, proper, normal subgroups H_0, H_1 such that $H_0 < H_1$. Then G, G/H_0, G/H_1 have pairwise incomparable cardinals.*

Proof. We have $G = \bigcup(G/H_0) = \bigcup(G/H_1)$; since the hypotheses of III.7 are satisfied, we conclude that $|G| \parallel |G/H_0|$ and $|G| \parallel |G/H_1|$.

Take $K \in G/H_1$, whence $K \subseteq G$, and define $K^* \subseteq G/H_0$ by $K^* = \{J \in G/H_0;\ J \subseteq K\}$. Then of course K^* is finite, and since $H_0 < H_1$ it follows by elementary group theory that $|K^*| > 1$. Furthermore, if we have $K_0, K_1 \in G/H_1$ with $K_0 \neq K_1$, then $K_0^* \cap K_1^* = \emptyset$. Finally, it is easily seen that $G/H_0 = \bigcup\{K^*;\ K \in G/H_1\}$, and so by III.7 we have $|G/H_0| \parallel |G/H_1|$.

4.

In §2 we saw how to construct quasi-minimal groups from certain given groups. But in order to ensure the success of our method, we had to require the given groups to be infinite and elementary abelian; and owing to an inherent property of this method, the quasi-minimal groups that emerged were also elementary abelian.

https://doi.org/10.1017/S0004972700025041 Published online by Cambridge University Press

In this section we show that all quasi=minimal groups are elementary abelian. Our first step towards this goal is an immediate consequence of III.7, and was in fact used in the proof of III.9. Since in this section, however, it plays a role of greater importance, we state it explicitly.

IV.1. *If G is a quasi-minimal group and H is a proper normal subgroup of G, then the factor group G/H is quasi-minimal.*

Proof. If H is the trivial subgroup, then of course G and G/H are isomorphic, and so G/H is quasi-minimal. Thus we may assume H to be nontrivial, whence the result follows from III.1 and III.7.

IV.2. *No quasi-minimal group is simple.*

Proof. Suppose that G is a simple, quasi-minimal group. Let e be the identity of G, and take $g \in G-\{e\}$. Let C_g be the conjugacy class $\{hgh^{-1};\ h \in G\}$ of g in G, and let $[C_g]$ be the subgroup of G generated by C_g. Then $[C_g]$ is a nontrivial normal subgroup of G, and as G is simple it follows that $[C_g] = G$. But G is locally finite, by III.1, whence we see that C_g is infinite.

We claim that in fact $C_g = G - \{e\}$. For suppose not, and take $g' \in G-C_g$ with $g' \neq e$. Then as $g' \notin C_g$ we must have $C_g \cap C_{g'} = \emptyset$. However, the same argument that showed C_g to be infinite also proves that $C_{g'}$ is infinite. As this contradicts the quasi-minimality of G, we must have $C_g = G - \{e\}$.

Now of course all elements of any conjugacy class have the same order, and since there is no injection $\omega \to G$, the order $o(g)$ of g must be finite. We have therefore shown that all nontrivial elements of G must have the same finite order, and it follows very easily that this order is a prime p.

Let H be any proper subgroup of G; we claim that $N_G(H) > H$, where $N_G(H)$ is the normalizer $\{g \in G;\ gHg^{-1} = H\}$ of H in G. For since H is proper, III.1 tells us that H is finite; take $g \in G-H$ and put $H^\circ = [H \cup \{g\}]$. We have shown that G is a p-group; thus H° is

https://doi.org/10.1017/S0004972700025041 Published online by Cambridge University Press

a p-group containing H as a proper subgroup. Therefore H is not a Sylow p-subgroup of H^o, and so ([6], Theorem 6, p. 137) $N_{H^o}(H) > H$. But clearly $N_G(H) \geq N_{H^o}(H)$; hence our claim is proved.

Take any specific $g \in G-\{e\}$, and define a sequence (G_n) of subgroups of G by $G_0 = [g]$, $G_{m+1} = N_G(H_m)$. From what has just been shown, (G_n) is a strictly increasing infinite sequence of subgroups of G, whence (G_n) is a strictly increasing infinite sequence of subsets of G.

However, G is quasi-minimal, and so $P(G)$ is medial.

This contradiction shows that G cannot be simple.

IV.3. *Let G be a quasi-minimal group with centre Z. Then G/Z is simple.*

Proof. Let H be any proper normal subgroup of G, and let $C = C_G(H)$ be the centralizer $\{g \in G;\ \forall h \in H(ghg^{-1} = h)\}$ of G in H. We will show that $C = G$, and to this end we define a map $f : G/C \to \mathrm{aut}(H)$, where $\mathrm{aut}(H)$ is the automorphism group of the group H - this clearly makes sense, since C is normal in G.

Take $K \in G/C$; then $K = gC$ for some $g \in G$, and we put $f(K) = a_g \in \mathrm{aut}(H)$, where $a_g(h) = ghg^{-1}$ for each $h \in H$. To show that f is well-defined and that its definition does not depend upon AC, we take any $g' \in G$ such that $K = g'C$, and consider $a_{g'}$. Since $g'C = K = gC$, there is $c \in C$ such that $g' = gc$; and of course c is unique. Now take any $h \in H$; by definition of C we have $chc^{-1} = h$, and it follows that

$$a_{g'}(h) = g'hg'^{-1} = gchc^{-1}g^{-1} = ghg^{-1} = a_g(h) .$$

We have thus shown that f is well-defined, and we claim that in fact f is injective. For take $K, K' \in G/C$ with $K \neq K'$; then $K = gC$, $K' = g'C$ for some $g, g' \in G$ with $g^{-1}g' \notin C$. But then there is $h \in H$ such that $g^{-1}g'h \neq hg^{-1}g'$, that is, $g'hg'^{-1} \neq ghg^{-1}$, and so ,

https://doi.org/10.1017/S0004972700025041 Published online by Cambridge University Press

$a_g \neq a_{g'}$.

Now H is a proper subgroup of G and so by III.1 is finite. Thus $\mathrm{aut}(H)$ is finite, and therefore, since we have just shown $f : G/C \to \mathrm{aut}(H)$ to be injective, we see that G/C is finite. But by IV.1 we have that G/C is quasi-minimal if C is a proper subgroup of G . Hence we conclude that $C = G$.

We have shown thus far that for every proper normal subgroup H of G , we have $C_G(H) = G$, whence it follows at once that $H \leq Z$. Therefore there is no normal subgroup H of G such that $Z < H < G$.

Consider the factor group G/Z . Without using AC we can define the usual homomorphism $f : G \to G/Z$, and show that if K is a normal subgroup of G/Z , then $\{g \in G;\ f(g) \in K\}$ is (the carrier of) a normal subgroup H of G such that $Z \leq H$.

Since we have just shown that for such a subgroup H we must have either $H = Z$ or $H = G$, it follows that G/Z is simple.

From IV.1, IV.2, and IV.3 we conclude very easily that every quasi-minimal group is abelian, and it remains to show that all nontrivial elements of such a group have order p , where p is some fixed prime. We shall show that all but a finite number of elements of a quasi-minimal group have the same (finite) order. It has been proved (in [5]) that if K is any infinite group in which all but a finite number of elements have the same order m , where m is some natural number, then all nontrivial elements of K have order m , and consequently m is prime. The proof uses a result of Miller's, given in [4], concerning the number of elements of prime order in a finite abelian group.

In this particular case we shall make use of the facts already proved about quasi-minimal groups to simplify the argument given in [5].

IV.4. *Every quasi-minimal group is an elementary abelian p-group for some prime p .*

Proof. Let G be a quasi-minimal group, and let the centre of G be Z . If $Z \neq G$, then by IV.1 and IV.3, we see that G/Z is a simple quasi-minimal group. Since this contradicts IV.2, we must have $Z = G$; that is, G is abelian.

https://doi.org/10.1017/S0004972700025041 Published online by Cambridge University Press

For each $g \in G$, let $o(g)$ be the order of g; we know that $o(g)$ is finite. For each $n \geq 1$, define the subset X_n of G by $X_n = \{g \in G;\ o(g) = n\}$. These sets X_n are pairwise disjoint, and since $P(G)$ is medial, there must be a natural number n° such that $X_n = \emptyset$ for every $n \geq n^\circ$. Since G is infinite, we must have X_n infinite for at least one $n < n^\circ$; since G is quasi-minimal, we must have X_n infinite for at most one $n < n^\circ$. We conclude that there is a natural number $n \geq 2$ and an infinite subset Y of G such that $o(g) = n$ for every $g \in Y$. We now show that $n = p^m$ for some prime p and some $m \geq 1$.

Put $T = G - Y$; since Y is infinite and G is quasi-minimal, we must have T, and hence $[T]$, finite. Let T° be the carrier of $[T]$. Suppose that p, q both divide n, where p and q are distinct primes, and take $g \in Y - T^\circ$. Then $o(pg)$, $o(qg) < n$, and so we must have pg, $qg \in T \subseteq T^\circ$. But $gcd(p, q) = 1$, and so there exist integers a, b such that $ap + bq = 1$. But then we have $g = (ap+bq)g \in T^\circ$, which is a contradiction.

This shows that $n = p^m$ for some prime p and some $m \geq 1$; we now show that in fact $m = 1$. Put $k = |T|$, and let S be any subset of Y such that $|S| = p^{mk}$; let S° be the carrier of $[S]$. We know that $[S]$ is a finite abelian p-group, and hence can be expressed as the direct sum of a family $(C_j)_{j \in J}$ of cyclic groups. Since each C_j has order at most p^m, we see that $|J| \geq k$. It follows from this that S° contains at least k elements of order p. However, $k = |T|$ and $0 \in T$, where 0 is the identity element of G. Hence $o(g) = p$ for some $g \in Y$, and so we must have $m = 1$.

We have shown that $o(g) = p$ for every $g \in Y$. But G is abelian; hence $Y \cup \{0\}$ is the carrier of a subgroup Y of G. Since Y is infinite, III.1 tells us that $Y = G$.

This proves our result.

We now use the fact that every quasi-minimal group is elementary abelian to prove a purely group-theoretic result. We make no claim regarding the usefulness or even interest of this result from the point of

https://doi.org/10.1017/S0004972700025041 Published online by Cambridge University Press

view of group theory: in our eyes its interest resides in the manner of its proof, which indicates that the method described in the first two sections may have a certain potential for obtaining results in classical group theory.

Let us for the moment return to the proofs of I.3 and II.2. If we compare these, we see that the only group-theoretic property of the infinite group U that was used in the proof of II.2, was the following:-

(4.1) for every subset U' of U with U, $U - U'$ both infinite, and for every finite subset E of U, there exists $a \in \mathrm{aut}(U)$ such that $a(u) = u$ for every $u \in E$ and $a(u') \notin U'$ for some $u' \in U'$.

IV.5. *Let U be an infinite group. Then within* ZFC *it is provable that U has property* (4.1) *if and only if U is elementary abelian.*

Proof. If U is elementary abelian, then it is a routine problem in group theory to show that U has property (4.1). Conversely, suppose that U has property (4.1). Then there is an FM-model V containing S such that $V \models$ "U is quasi-minimal". Since III.1 and IV.1-4 can all be proved in FM set theory, we have $V \models$ "U is elementary abelian". But U has the same structure in V as in the universe. Thus U must be elementary abelian.

5.

In this concluding section we wish to look at permutations on quasi-minimal sets and some of the properties of the corresponding groups. In particular we shall obtain some results on the factor groups $T_X/T_{\mathfrak{f},X}$, where X is a quasi-minimal set, T_X is the symmetric group on X, and $T_{\mathfrak{f},X}$ is the finitary symmetric group on X, that is, the subgroup of T_X consisting of all permutations $f : X \to X$ such that the set $\{x \in X;\ f(x) \neq x\}$ is finite. We shall show that by choosing X suitably, the factor group $T_X/T_{\mathfrak{f},X}$ can be trivial, cyclic of order 2, or infinite. Whether these three possibilities are exhaustive is, as far as we know, still an open question.

If X is a quasi-minimal set, then clearly T_X is infinite but not

https://doi.org/10.1017/S0004972700025041 Published online by Cambridge University Press

quasi-minimal; for one thing, T_X is not abelian. We remain, however, in the realm of medial groups; this is an immediate consequence of the following purely set-theoretic result.

V.1. *Let X, Y be medial sets. Then X^Y is medial if and only if $P(Y)$ is medial.*

Proof. In one direction this is obvious, for we have $|P(Y)| = |2^Y| \leq |X^Y|$, and so if X^Y is medial, then $P(Y)$ is also medial.

Therefore we suppose that $P(Y)$ is medial whilst X^Y is not. Since X^Y is certainly infinite, there must be an infinite sequence (f_n) of pairwise distinct functions $Y \to X$. For each $y \in Y$, we define the subset R_y of X by $R_y = \{f_n(y); n < \omega\}$. We define an enumeration $\Sigma(y) = (y_0, y_1, \ldots, y_{l(y)})$ of R_y without repetitions in the following manner:

(5.1) (i) $y_0 = f_0(y)$;

(ii) if $y_0, \ldots, y_k$ are defined and for some n we have $f_n(y) \notin \{y_0, \ldots, y_k\}$, then we let n° be the smallest such n and put $y_{k+1} = f_{n^\circ}(y)$: otherwise y_{k+1} is undefined.

Since $R_y \subseteq X$ and X is medial, it is clear that $\Sigma(y)$ is finite. For each n, put $Q_n = \{y \in Y; l(y) = n\}$. These sets Q_n are pairwise disjoint, and so, since $P(Y)$ is medial, there must exist m such that $Q_n = \emptyset$ for every $n \geq m$; let p be the smallest such m. Thus we have $l(y) < p$ for every $y \in Y$.

We now define a function $g : \omega \to p^Y$ in the following manner (we recall that according to our conventions we have $p = \{0, 1, \ldots, p\text{-}1\}$):-

(5.2) take $n < \omega$. Then the function $g(n) : Y \to p$ is defined as follows.

https://doi.org/10.1017/S0004972700025041 Published online by Cambridge University Press

Given $y \in Y$, let y_k be the unique term of $\Sigma(y)$ such that $y_k = f_n(y)$. Then $k \leq l(y) < p$, and we put $g(n)(y) = k$.

We see that g is validly defined, since for each $y \in Y$, $\Sigma(y)$ enumerates R_y without repetitions. Moreover, g is injective. To see this, take $m, n < \omega$, and suppose that $g(m) = g(n)$. Then $g(m)(y) = g(n)(y)$ for every $y \in Y$, from which it follows that $f_m(y) = f_n(y)$ for every $y \in Y$. Hence $f_m = f_n$, and so $m = n$.

Let k be any natural number such that $p \leq 2^k$. Since there is a bijection $P(Y) \to 2^Y$, it is clear that there is an injection $p^Y \to P(Y)^k$. Hence there is an injection $\omega \to P(Y)^k$, and so $P(Y)^k$ is not medial.

But medial sets are closed under finite cartesian products. This is well-known, and so we just sketch the proof. Let A, B be medial sets, and assume that $A \times B$ is not medial. Then there must be an infinite sequence $\langle (a_n, b_n) \rangle$ of pairwise distinct elements of $A \times B$. But then $A^\circ = \{a_n; n < \omega\}$ and $B^\circ = \{b_n; n < \omega\}$ are countable subsets of A, B respectively, and hence must both be finite. This gives a contradiction.

Since $P(Y)$ is medial, it follows that $P(Y)^k$ is also medial. This contradiction proves our result.

V.2. *Let X be a quasi-minimal set. Then T_X and $T_{\mathfrak{h},X}$ are medial groups.*

Proof. Since X is infinite, it is clear that $T_{\mathfrak{h},X}$ and hence T_X is infinite. On the other hand, since X is quasi-minimal, $P(X)$ is medial, and so X^X is medial by V.1. But of course $T_{\mathfrak{h},X} \subseteq T_X \subseteq X^X$.

V.3. *Let $f : X \to X$ be a permutation on the quasi-minimal set X. Then f can be expressed as the product of a family of finite pairwise disjoint cycles of bounded length.*

Proof. Take any $x \in X$. Since X is quasi-minimal, the infinite sequence $\langle f^n(x) \rangle$ can have only a finite number of pairwise distinct

https://doi.org/10.1017/S0004972700025041 Published online by Cambridge University Press

terms, ans so we must have $f^m(x) = x$ for some m.

This shows that if we now define a binary relation $\sim$ on X by setting $x \sim y$ if and only if $y = f^n(x)$ for some n, then $\sim$ is an equivalence relation and thus induces a partitioning $(X_j)_{j \in J}$ of X. Furthermore, it is clear that for each j, the permutation f induces a cycle $X_j \to X_j$ of finite length.

For each n, define $J_n \subseteq J$ by $J_n = \{j \in J;\ |X_j| = n\}$. These sets J_n are pairwise disjoint, and since it is clear that J is quasi-minimal, there must exist m such that $J_n = \emptyset$ for every $n \geq m$. Thus the cycles occurring in the decomposition of f have bounded length.

We call an element of $T_{\mathfrak{f},X}$, where X is some infinite set, a "finitary permutation". We come now to the results concerning $T_X/T_{\mathfrak{f},X}$ that were mentioned at the start of this section.

V.4. *It is relatively consistent with* ZF *to assume the existence of a quasi-minimal set* X *such that the factor group* $T_X/T_{\mathfrak{f},X}$ *is trivial.*

Proof. We take the FMC model M, the permutation model V, and the set U that were defined in the proof of I.3. We know that $V \models$ "U is quasi-minimal"; we claim that $V \models T_U = T_{\mathfrak{f},U}$.

For suppose that there is $f \in V$ with $V \models f \in T_U - T_{\mathfrak{f},U}$. Then of course we have $M \models$ "f is not finitary"; furthermore, by I.2 there exists a finite subset E of U such that $S_E \subseteq G_f$. Choose $(u_0, u_1) \in f \subseteq U \times U$ with $u_0 \neq u_1$ and $u_0, u_1 \notin E$. Now take any $u_2 \in U - E$ with $u_2 \neq u_1$, and let g be the transposition $(u_1 u_2)$. Then $g \in S_E$ but $g(f) \neq f$. This contradiction shows that no such f can exist, and hence that $V \models T_U = T_{\mathfrak{f},U}$.

Now apply the Embedding Theorem.

V.5. *It is relatively consistent with* ZF *to assume the existence of a quasi-minimal set* X *such that* $T_X/T_{\mathfrak{f},X}$ *is cyclic of order* 2.

https://doi.org/10.1017/S0004972700025041 Published online by Cambridge University Press

Proof. Again let M be the FMC model defined in the proof of I.3, and let U be its set of urelemente. Since AC holds in M and U is infinite in M, we can within M partition U into a family $(U_b)_{b \in B}$ of sets U_b such that $|U_b| = 2$ for each $b \in B$. The index set B is of course infinite.

As in I.3 we let I be the ideal on $P(U)$ consisting of all finite subsets of U, but this time we let G_0 be the group of all permutations $g : U \to U$ satisfying the following condition:-

(5.3) for each $b \in B$, there exists $b^\circ \in B$ such that $U_{b^\circ} = g"U_b$.

Clearly G_0 is a group and I is normal with respect to G_0. Hence we obtain a permutation model $V_0 = V_0(G_0, I)$ containing U as its set of urelemente.

In the usual manner we show that $V_0 \models$ "U is quasi-minimal". Suppose that for some $U^\circ \in V_0$ we have

$$V_0 \models \text{"}U^\circ \subseteq U \text{ and } U^\circ,\ U - U^\circ \text{ are both infinite"}.$$

Then there exists in M a finite subset E of U such that $S_E \subseteq G_{0,U^\circ}$. Since U° and $U - U^\circ$ are both infinite in M as well as in V_0, there exist $b, b' \in B$ such that $U_b \subseteq U^\circ - E$ and $U_{b'} \subseteq (U - U^\circ) - E$. Choose $g \in G_0$ such that $g"U_b = U_{b'}$, $g"U_{b'} = U_b$, and $g(u) = u$ for every $u \notin U_b \cup U_{b'}$. Then $g \in S_E$ but $g(U^\circ) \neq U^\circ$.

This contradiction shows that $V_0 \models$ "U is quasi-minimal".

Temporarily we work within M. For each $b \in B$, let u_{b0} and u_{b1} be the two elements of U_b. Define the permutation $f : U \to U$ by putting $f(u_{b0}) = u_{b1}$ and $f(u_{b1}) = u_{b0}$ for each $b \in B$.

We claim that $f \in V_0$. For clearly $f \subseteq V_0$, and so it suffices to show that $G_{0,f} \in \Gamma$, where Γ is the appropriate normal filter obtained from I. But from (5.3) we see that $g(f) = f$ for every $g \in G_0$. Hence

https://doi.org/10.1017/S0004972700025041 Published online by Cambridge University Press

$G_{0,f} = G_0$, and thus $f \in V_0$.

Clearly $V_0 \models \forall u \in U(f(u) \neq u)$, and so $V_0 \models T_U \neq T_{\emptyset,U}$.

Now suppose that for some permutation $h : U \to U$ we have $h \in V_0$ and $V_0 \models$ "h is not finitary". By I.2 there is in M a finite subset E of U such that $S_E \subseteq G_{0,h}$; and of course we have $M \models$ "h is not finitary".

Choose any $(u_0, u_1) \in h$ with $u_0 \neq u_1$ and $u_0, u_1 \notin E$. We claim that $u_0, u_1 \in U_b$ for some $b \in B$. For suppose that $u_0 \in U_b$ and $u_1 \in U_{b^\circ}$ for some $b, b^\circ \in B$ with $b \neq b^\circ$. Choose $b' \in B - \{b, b^\circ\}$ with $U_{b'} \subseteq U - E$; then there exists $g \in S_E$ such that $g"U_{b^\circ} = U_{b'}$, $g"U_{b'} = U_{b^\circ}$, and $g"U_c = U_c$ otherwise. Then $g(h) \neq h$, and we have a contradiction.

Thus $h"U_b = U_b$ for every $b \in B$ with $U_b \subseteq U - E$. Since we have $V_0 \models$ "U is quasi-minimal" and $V_0 \models$ "h is not finitary", it follows easily that $V_0 \models$ "$\{u \in U; h(u) \neq f(u)\}$ is finite".

From this we deduce at once that $V_0 \models |T_U/T_{\emptyset,U}| = 2$, and can now just apply the Embedding Theorem.

It is interesting to note that the condition $|U_b| = 2$ is crucial; if we try the same trick with $|U_b| = k$, for some $k \neq 2$, then we end up with $V_0 \models T_U = T_{\emptyset,U}$. We omit the proof of this.

V.6. *It is relatively consistent with* ZF *to assume the existence of a quasi-minimal set* X *such that the factor group* $T_X/T_{\emptyset,X}$ *is infinite.*

Proof. Let G be a quasi-minimal group; we claim that there is an injection $f : G \to T_G/T_{\emptyset,G}$. To see this, take any $g \in G$ with $g \neq 0$, where 0 is the identity of G , and define the map $a_g : G \to G$ by $a_g(h) = g + h$. Clearly a_g is a nonfinitary permutation, and for any $g' \in G - \{g, 0\}$ we have $a_g(h) \neq a_{g'}(h)$ for every $h \in G$. Thus if we

https://doi.org/10.1017/S0004972700025041 Published online by Cambridge University Press

define $f : G \to T_G/T_{\emptyset,G}$ by $f(0) = T_{\emptyset,G}$ and $f(g) = a_g T_{\emptyset G}$ for $g \in G - \{0\}$, we see that f is injective.

Hence $T_G/T_{\emptyset,G}$ is infinite.

We remark once again that we do not know whether V.4–V.6 exhaust the possibilities. In particular, we do not know whether it is possible to have a quasi-minimal set X such that $T_X/T_{\emptyset,X}$ is medial.

Within ZFC we can show that every (nonempty) set is capable of carrying a group structure. Since the proof of this relies heavily upon AC, it is not surprising that this result does not hold in ZF.

V.7. *It is relatively consistent with* ZF *to assume the existence of a quasi-minimal set that is not the carrier of any group.*

Proof. By V.4 we may assume the existence of a quasi-minimal set X such that $T_X = T_{\emptyset,X}$. But by V.6 if X was the carrier of a group, then we would have $T_X \neq T_{\emptyset,X}$.

Note added in proof, 5 March 1976. It has been pointed out to the author by Dr B.H. Neumann that as it stands the proof of II.2 is not correct, for we cannot guarantee the existence of $j_0, j_1 \in J-J^\circ$ satisfying the conditions $C_{j_0} \subseteq U^\circ - E^\circ$ and $C_{j_1} \subseteq (U-U^\circ) - E^\circ$ (see p. 213 for notation).

In order to obtain the required automorphism, therefore, we must proceed as follows. Since E° is finite whilst U° and $U - U^\circ$ are both infinite, there exist $u_0 \in U^\circ$ and $u_1 \in U-U^\circ$ such that K, the subgroup generated by u_0 and u_1, has trivial intersection with $[E]$.

But we can express U as a direct sum $K + L$, where L contains $[E]$. It is a well-known fact of group theory that there exists $g \in G$ such that $g(u_0) = u_1$ and $g(u) = u$ for every element u of L. We now proceed as in the text.

https://doi.org/10.1017/S0004972700025041 Published online by Cambridge University Press

References

[1] Frank R. Drake, *Set theory: an introduction to large cardinals* (Studies in Logic and the Foundations of Mathematics, 76. North-Holland, Amsterdam, London; American Elsevier, New York; 1974).

[2] J.L. Hickman and B.H. Neumann, "A question of Babai on groups", *Bull. Austral. Math. Soc.* 13 (1975), 355-368.

[3] Thomas L. Jech, *The Axiom of Choice* (Studies in Logic and the Foundations of Mathematics, 75. North Holland, Amsterdam, London; American Elsevier, New York; 1973).

[4] G.A. Miller, "On an important theorem with respect to the operation groups of order p^{α}, p being any prime number", *Messenger Math.* 27 (1898), 119-121; see also, *The collected works of George Abram Miller*, Volume I, 303-304 (University of Illinois, Urbana, Illinois, 1935).

[5] B.H. Neumann, Private communication.

[6] Hans J. Zassenhaus, *The theory of groups*, second edition (Chelsea, New York, 1958).

Department of Mathematics,
Institute of Advanced Studies,
Australian National University,
Canberra,
ACT.

https://doi.org/10.1017/S0004972700025041 Published online by Cambridge University Press