SOME PROBLEMS IN GROUP THEORY

R. D. KOPPERMAN AND A. R. D. MATHIAS

Except as noted, notation is as defined in [3] group-theoretic notions as in [1].

DEFINITION. A class $\mathfrak{N}$ of groups is called bountiful if and only if for every group G with $\omega \leq c(G)$ (ω the first infinite cardinal, $c(G)$ the cardinality of G), if there is an $H \in \mathfrak{N}$ such that $G \subset H$, then there is an $H' \in \mathfrak{N}$ such that $G \subset H' \subset H$ and $c(G) = c(H')$.

The following are examples of bountiful classes of groups:

(1) $\mathfrak{A}$, the class of abelian groups

(2) $\mathfrak{S}$, the class of simple groups

(3) $\mathfrak{C}$, the class of characteristically simple groups, where G is said to be characteristically simple if and only if $\{e\}$ and G are the only subgroups closed under every automorphism of G

(4) $\mathfrak{J}$, the class of groups G for which if $K \lhd H \lhd G$ then $K \lhd G$ (where $A \lhd B$ means that A is a normal subgroup of B, $A < B$ means that A is a subgroup of B)

(5) $\mathfrak{F}$, the class of groups G such that if $H, K < G$ are finitely generated and $H \cong K$, then for some $g \in G$, $g^{-1}Hg = K$.

We also have the following open questions:

(a) Is $\mathfrak{I}$, the class of groups G with center $\{e\}$ and such that every automorphism is inner, bountiful?

(b) Can we find a useful general criterion for a class $\mathfrak{N}$ of groups to be bountiful?

We note that our first bountiful class $\mathfrak{G} = M(\sigma)$ (the class of models of σ) for some $\sigma \in L$ (the usual [finite] first-order language of groups), and that the Löwenheim-Skolem theorem immediately yields the fact that this class is bountiful. The infinitary downward Löwenheim-Skolem theorem provides a partial answer to open question (b), by telling us that if $\mathfrak{A} = M(\sigma)$ for some $\sigma \in L_{\omega_1\omega}$ (the language of group theory extended by allowing countable conjunctions and disjunctions), then $\mathfrak{A}$ is a bountiful class. We use this partial answer to (b) to give model-theoretic proofs that $\mathfrak{S}$, $\mathfrak{C}$, $\mathfrak{I}$, and $\mathfrak{F}$ are bountiful.

LEMMA 1. G <u>is simple if and only if for every</u> $a \in G - \{e\}$, $[\{a\}] = G$, <u>where</u>:

DEFINITION. Let $A \subset G$, G a group. $[A]_G = \bigcap \{H \mid A \subset H \lhd G\}$ (and is called the normal subgroup generated by A in G), and $\langle A \rangle_G = \bigcap \{H \mid A \subset H < G\}$ (and is called the subgroup generated by A in G). If it is apparent which group is meant, the subscript $_G$ may be removed from either of these notations.

<u>Proof of the lemma</u>. Clearly if G is simple and $a \neq e$, $[\{a\}] = G$. Also if G has the property that $[\{a\}] = G$ and $H \neq \{e\}$ is a normal subgroup of G, let $a \in H - \{e\}$. Then $G = [\{a\}] \subset H \subset G$, so $H = G$, thus G is simple.

It will be convenient from now on to denote by $\mathfrak{G}$ the class of all groups, $\mathfrak{G} = M(\gamma)$, where γ is the conjunction of the group axioms, $\gamma \in L$.

COROLLARY 1. $\mathfrak{S} = M(\sigma)$ <u>for some</u> $\sigma \in L_{\omega_1\omega}$. <u>Thus</u> $\mathfrak{S}$ <u>is bountiful</u>.

<u>Proof</u>. It is well-known and simple to check that $[\{a\}] = \{g_1 a^{m_1} g_1^{-1} \cdots g_n a^{m_n} g_n^{-1} \mid n \in \omega, m_i \in Z$ (the set of integers) for $1 \leq i \leq n$, $g_i \in G$ for $1 \leq i \leq n\}$. Let $\tau = (\forall x)(x \neq e \rightarrow (\forall y) \bigvee_{i \in \omega - \{0\}} (\exists v_1 \cdots v_i)[\bigvee_{m_1 \ldots m_i \in Z} v_1 x^{m_1} v_1^{-1} \cdots v_i x^{m_i} v_i^{-1} = y])$. Clearly $\tau \in L_{\omega_1\omega}$, and if $\sigma = \tau \,\&\, \gamma$, then so is σ. By the lemma, $\mathfrak{S} = M(\sigma)$.

LEMMA 2. <u>Let</u> G <u>be a group</u>, $a \in G$. <u>Set</u> $G_a = \{f_1(a^{m_1}) \cdots f_n(a^{m_n}) \mid f_1, \ldots, f_n$ <u>automorphisms of</u> G, $n \in \omega - \{0\}$, $m_1, \ldots, m_n \in Z\}$. <u>Then</u> G <u>is characteristically simple if and only if for every</u> $a \in G - \{e\}$, $G_a = G$.

<u>Proof</u>. We note that for every $a \in G$, G_a is a subgroup closed under every automorphism of G. G_a is clearly closed under the group operation, and $(f_1(a^{m_1}) \cdots f_n(a^{m_n}))^{-1} = f_n(a^{-m_n}) \cdots f_1(a^{-m_1}) \in G_a$.

Finally, if f is an automorphism of G, $f(f_1(a^{m_1}) \cdots f_n(a^{m_n})) = (ff_1)(a^{m_1}) \cdots (ff_n)(a^{m_n}) \in G_a$. Thus if G is characteristically simple, $a \in G - \{e\}$, $G_a = G$. Conversely, let H be a subgroup of G closed under every automorphism, $H \neq \{e\}$, let $a \in H - \{e\}$. Then $G = G_a \subset H \subset G$, so $H = G$, and G must be characteristically simple.

The use for the lemma above is not quite so straightforward as that of Lemma 1, since our language $L_{\omega_1\omega}$ lacks the predicates necessary to discuss automorphisms. We therefore consider structures of the form $\langle S,G,M,A,\cdot,e\rangle$, with $\langle G,\cdot,e\rangle$ a group, $G \cup M = S$, $G \cap M = \emptyset$, and A a ternary relation (corresponding to $f(x) = y$) such that,

(1) $(\forall f)(\forall x)(\forall y)(A(f,x,y) \rightarrow M(f) \ \& \ G(x) \ \& \ G(y))$ (A relates a "member" of M and two "members" of G)

(2) $(\forall f)(\forall x)(\forall y)(\forall x')(\forall y')(A(f,x,y) \ \& \ A(f,x',y') \rightarrow (x = x' \leftrightarrow y = y'))$ (each "element" of M is a one-to-one function)

(3) $(\forall f)(\forall y)(G(y) \rightarrow (\exists x)A(f,x,y))$ (each "map" has range = G)

(4) $(\forall f)(\forall x)(\forall y)(\forall x')(\forall y')(\forall x")(\forall y")(A(f,x,y) \ \& \ A(f,x',y') \ \& \ xx' = x" \ \& \ yy' = y" \rightarrow A(f,x",y"))$ (our "maps" are homomorphisms)

(5) $(\exists g)(\forall x)(G(x) \rightarrow A(g,x,x))$ (the "identity" is in M)

(6) $(\forall f)(\exists g)(\forall x)(\forall y)(A(f,x,y) \rightarrow A(g,y,x))$ ("elements" of M have "inverses" in M)

(7) $(\forall f)(\forall g)(\exists h)(\forall x)(\forall y)(\forall z)(A(f,x,y) \ \& \ A(g,y,z) \rightarrow A(h,x,z))$ (M is closed under "composition").

Every model of (1)-(7) must be a group together with a subgroup of its group of automorphisms, and that all these axioms are in L^t, the (finitary) language of structures of type $t = \langle 1,1,3,3,0\rangle$. In the extension $L^t_{\omega_1\omega}$ of this language by the use of countable conjunctions and disjuntions, we can write: $(\forall y)(\forall x)(x \neq e \rightarrow \bigvee_{i\in\omega-\{0\}} (\exists f_1)(\exists f_2) \cdots (\exists f_i)(\exists z_1) \cdots (\exists z_i)(\exists v_2) \cdots (\exists v_{i-1})[\bigvee_{m_1,\ldots,m_i\in Z} A(f_1,x^{m_1},z_1) \ \& \cdots \& \ A(f_i,x^{m_i},z_i) \ \& \ z_1z_2 = v_2 \ \& \cdots \& \ v_{i-2}z_{i-1} = v_{i-1} \ \& \ v_{i-1}z_i = y] \vee \neg G(y)) = \tau$. Now let $\sigma = \tau \ \& \ \gamma \ \& \ (1) \ \& \cdots \& \ (7) \in L^t_{\omega_1\omega}$, A(G) stand for the group of automorphisms of G.

COROLLARY 2. C is bountiful.

Proof. Let $G \in \mathcal{G}$ $G \subset H \in \mathcal{C}$. Then $\langle A(H) \cup H, H, A(H), R, \cdot, e\rangle \in M(\sigma)$, where $R(f,x,y) \leftrightarrow f(x) = y$. $G \subset A(H) \cup H$, thus by downward Löwenheim-Skolem $\langle S, S \cap H, S \cap A(H), S^3 \cap R, S^3 \cap \cdot, e\rangle \in M(\sigma)$, with $c(S) = c(G)$, and since $G \subset H$, $G \subset S$, we have $G \subset H \cap S$, and $H \cap S$ must be a characteristically simple group since the automorphisms in $S \cap A(H)$ "already" make it such.

LEMMA 3. $G \in \mathcal{J}$ *if and only if* (*) *for* $K \lhd H \lhd G$, *with* $H = [S]_G$, $K = [S']_H$, S, S' *finite, we have* $K \lhd G$.

Proof. Clearly for $G \in \mathcal{J}$ (*) holds. Conversely, assume (*). We first show (**) if $K \lhd H \lhd G$, $K = [S]_H$, S finite, then $K \lhd G$. But if $H \lhd G$, $[S]_G \subset H$ for any $S \subset H$. Thus $K \lhd [S]_G \lhd G$, with S finite, so by (*), $K \lhd G$.

Using (**) we now establish the theorem. Let $K = [A]_H$, and assume that the theorem has been established for all $[B]_H$ with $c(B) < c(A)$. We now write A as an ascending union of B_i's with $c(B_i) < c(A)$ (this may be done by putting A in one-to-one correspondence with its cardinal $c(A)$ and setting $B_i = \{a_j \mid j < i\}$). Now note that $K = \bigcup_{i<c(A)} [B_i]_H$, an ascending chain of normal subgroups of G. Thus $K \lhd G$.

COROLLARY 3. $\mathcal{J} = M(\sigma)$ *for some* $\sigma \in L_{\omega_1\omega}$, *thus* $\mathcal{J}$ *is a bountiful class*.

Proof. Let $\tau = \bigwedge_{m,n\in\omega-\{0\}}(\forall a_1)\cdots(\forall a_n)(\forall b_1)\cdots(\forall b_m)(\forall x)(H(a_1,\ldots,a_n,x) \leftrightarrow J(a_1,\ldots,a_n,b_1,\ldots,b_m,x))$, where we define $H(a_1,\ldots,a_n,x) \leftrightarrow \bigvee_{p\in\omega\{0\}}(\exists z_1)\cdots(\exists z_p)\bigvee_{i_{11},\ldots,i_{pn}\in Z}(x = z_1 a_1^{i_{11}} \cdots a_n^{i_{1n}} z_1^{-1} \cdots z_p a_1^{i_{p1}} \cdots a_n^{i_{pn}} z_p^{-1})$ (and this corresponds to $x \in [\{a_1,\ldots,a_n\}]_G$) and we define $J(a_1,\ldots,a_n,\ldots,b_m,x) \leftrightarrow \bigvee_{p\in\omega-\{0\}}(\exists z_1)\cdots(\exists z_p)(H(b_1,\ldots,b_m,z_1) \& \cdots \& H(b_1,\ldots,b_m,z_p) \& [\bigvee_{i_{11},\ldots,i_{pn}\in Z}(x = z_1 a_1^{i_{11}} \cdots a_n^{i_{1n}} z_1^{-1} \cdots z_p a_1^{i_{p1}} \cdots a_n^{i_{pn}} z_p^{-1})])$ (corresponding to $x \in [\{a_1,\ldots,a_n\}][\{b_1,\ldots,b_m\}]$).

Then by Lemma 3, $\sigma = \tau \,\&\, \gamma$ is our statement since σ states that the normal subgroup generated by $a_1,\ldots,a_n$ in the normal subgroup generated by $b_1,\ldots,b_m$ is the same as the normal subgroup generated by $a_1,\ldots,a_n$ in the entire group. Thus a finitely-generated normal subgroup of a finitely-generated normal subgroup is normal.

PROPOSITION 1. $\mathfrak{F} = M(\sigma)$ for some $\sigma \in L_{\omega_1\omega}$, thus $\mathfrak{F}$ is a bountiful class.

Proof. We define $G(a_1,\ldots,a_n,x) \leftrightarrow \bigvee_{p\in\omega-\{0\},i_{11},\ldots,i_{pn}\in Z}(a_1^{i_{11}} \cdots a_n^{i_{1n}} a_1^{i_{21}} \cdots a_n^{i_{2n}} \cdots a_n^{i_{pn}} = x)$ (corresponding to $x \in \langle\{a_1,\ldots,a_n\}\rangle$), $I(a_1,\ldots,a_n,b_1,\ldots,b_n) \leftrightarrow (\exists z_1)\cdots(\exists z_n)(\forall x)([G(b_1,\ldots,b_m,x) \leftrightarrow G(z_1,\ldots,z_n,x)] \;\&\; \bigwedge_{p\in\omega-\{0\},i_{11},\ldots,i_{pn}\in Z}(z_1^{i_{11}} \cdots z_n^{i_{1n}} z_2^{i_{21}} \cdots z_2^{i_{2n}} \cdots z_n^{i_{pn}} = e \leftrightarrow a_1^{i_{11}} \cdots a_n^{i_{1n}} \cdots a_n^{i_{pn}} = e))$. It is simple to check that $I(a_1,\ldots,a_n,b_1,\ldots,b_m)$ holds if and only if $\langle\{a_1,\ldots,a_n\}\rangle \cong \langle\{b_1,\ldots,b_m\}\rangle$, (where the isomorphism $f_1\langle\{a_1,\ldots,a_n\}\rangle \to \langle\{b_1,\ldots,b_m\}\rangle$ is defined by $f(a_1^{i_{11}} \cdots a_n^{i_{pn}}) = z_1^{i_{11}} \cdots z_n^{i_{pn}}$).

Thus if $\tau = \bigwedge_{m,n\in\omega-\{0\}}(\forall a_1)\cdots(\forall a_n)(\forall b_1)\cdots(\forall b_m)(I(a_1,\ldots,a_n,b_1,\ldots,b_m) \leftrightarrow (\exists g)(\forall x)(G(a_1,\ldots,a_n,x) \leftrightarrow G(b_1,\ldots,b_m,gxg^{-1}))$, then τ says that if any two finitely-generated subgroups are isomorphic, they are conjugate. If $\sigma = \tau \;\&\; \gamma$, then $\mathfrak{F} = M(\sigma)$.

The question of whether $\mathfrak{I}$ is bountiful remains open. A major difficulty seems to be the fact that structures of the form $\langle G \cup A(G), G, A(G), A, \cdot, e\rangle$ cannot be characterized in any language $L^s_{\alpha\beta}$ (for any type s, any regular cardinals α, β). This can be shown by use of infinitary downward Löwenheim-Skolem.

The following considerations suggest a problem on the border between group theory and logic:

Recall that for $a \in G$, $\mathrm{ord}(a) = \begin{cases} \text{the least } n > 0 \text{ such that } a^n = e \\ \infty \text{ if no such } n > 0 \text{ exists} \end{cases}$.

If G is an abelian group and if $\mathrm{ord}(a) \neq 1, 2$, then $a \neq a^{-1}$, thus the map $f: G \to G$ by $f(x) = x^{-1}$, an automorphism in this case, does not leave a fixed. Therefore, for any formula $F \in L$, if $G \models F[a]$, then $G \models F[a^{-1}]$, so it is impossible to distinguish a from all other elements of G by a set of formulas $S \subset L$ with one free variable.

We may now ask if for any group G whether every first-order-definable element of G is of order 1 or 2.

For G non-abelian, $a \notin C(G)$, we have an element $b \in G$ such that $ab \neq ba$, thus $a \neq bab^{-1}$. Therefore the (inner) automorphism $f_b, G \to G$ defined by $f_b(x) = bxb^{-1}$ does not fix a, and since a cannot be distinguished from its image under an automorphism, no $a \notin C(g)$ is first-order-definable. We have shown:

PROPOSITION 2. Let $a \in G$. If

(1) $\text{ord}(a) \neq 1,2$ and G is abelian, or

(2) if $a \notin C(G)$,

then a is not first-order-definable.

The answer to the proposed question, however, is negative. In fact for every $n < \infty$ there are an infinite number of groups with first-order-definable elements of order n. To see this, suppose G is finite. Then two elements $a,b \in G$ cannot be distinguished by a set of first-order-formulas in one free variable if and only if $\langle G,\cdot,e,a\rangle \equiv \langle G,\cdot,e,b\rangle$ in the language L^c of groups with a constant (i.e. if and only if the two structures satisfy the same sentences in that language). But since G is finite this implies $\langle G,\cdot,e,a\rangle \equiv \langle G,\cdot,e,b\rangle$, i.e., there is an automorphism f of G such that $f(a) = b$. It will therefore do to show that for every $n > 2$ there is an infinite number of finite groups, each with an element of order n fixed under every automorphism. The following is due to Stephen Meskin:

LEMMA. If $1 < n < \infty$ then there is an infinite number of finite groups with elements of order n fixed under every automorphism.

Proof. By Dirichlet's theorem (a statement of which may be found on p. 20 of [4], a proof on p. 49 of [2]) there are infinitely many primes p such that n divides $p - 1$. For each such p, consider the group generated by a, b with $a^p = b^{n^2} = e$ $bab^{-1} = a^t$, where $0 < t < p$ and the order of t in the multiplicative group of z mod p is n (the existence of such a t under these circumstances is shown on p. 54 of [4], the fact that this group exists is shown as on p. 148 of [1]).

The following facts may be established by induction on m:

(1) $b^m a^s b^{-m} = a^{t^m s}$ (thus $b^m a^s = a^{t^m s} b^m$)

(2) $(b^x a^y)^m = a^{(t^x + \cdots + t^{mx})y} b^{mx}$ (the proof of this uses (1))

and (1) can also be used to show that every element of our group can be written uniquely in the form $b^x a^y$ (or $a^r b^s$). Call our group H and let f be an automorphism of H. $f(a)$ must be of order p, but any element of order p must be in the subgroup $\langle\{a\}\rangle$ (since by (1), $\langle\{a\}\rangle$ is normal, and if $g : H \to H/\langle\{a\}\rangle$ is the natural homomorphism, $c \in H$ of order p, then $\text{ord}(g(c))$ divides p, but also must divide the order of the group $H/\langle\{a\}\rangle = n^2$, and since p, n^2 are relatively

prime, $\mathrm{ord}(g(c)) = 1$. Thus $g(c) = e$, so $c \in \langle\{a\}\rangle$). Thus for some k, $f(a) = a^k$ and $(k,p) = 1$ (i.e., k, p are relatively prime), and we may also write $f(b) = b^x a^y$.

Thus $f(bab^{-1}) = f(b)f(a)f(b)^{-1} = b^x a^y a^k a^{-y} b^{-x} = b^x a^k b^{-x} = a^{t^x k}$. But $f(bab^{-1}) = f(a^t) = f(a)^t = a^{kt}$, so $a^{t^x k} = a^{tk}$, thus $t^x k \equiv tk \pmod p$, thus since $(k,p) = 1$, $t^{x-1} \equiv 1 \pmod p$, so $x \equiv 1 \pmod n$. Now note that $\mathrm{ord}(b^n) = n$, and $f(b^n) = f(b)^n = (b^x a^y)^n = a^{(t^x+\cdots+(t^x)^n)y} b^{nx} = a^{(t+\cdots+t^n)y} (b^n)^x = a^{[(1-t^n)/(1-t)]ty} b^n = a^{0ty} b^n = b^n$ (the third equation from the end uses the fact that $x \equiv 1 \pmod n$, so $t^x \equiv t \pmod p$). Thus b^n is also fixed under every automorphism.

COROLLARY 4. <u>For any positive</u> n <u>there is a group</u> G <u>with an element</u> c <u>of order</u> n <u>which is first-order-definable</u>.

The question remains open for order ∞.*

The problems in the first part arose in the course of lectures given by Philip Hall in Cambridge in 1966. Hall showed that the classes $\mathfrak{S}$, $\mathfrak{C}$, $\mathfrak{I}$, and $\mathfrak{F}$ are bountiful, and asked whether the same is true of $\mathfrak{J}$. The term "bountiful" is due to Mathias, who noticed the similarity of Hall's theorems to that of Löwenheim and Skolem, and raised the second question. The answer given here, that the four classes are (with some sleight of hand) axiomatisable in $L_{\omega_1\omega}$, was found by Kopperman in the Westwood Village Delicatessen, Los Angeles, at 7:32 p.m. on December 30, 1967.

The problem of first-order definable elements was raised by Mathias.

---

*This question has been solved in part. Mathias and Meskin have independently discovered a group with an element of infinite order which is first-order-distinguishable from all other elements of the group. It is distinguishable, however, only by an infinite set of sentences, rather than a single sentence. (The example is much like those given in the text, with b "made" infinite in order.) Let D be of order 5, d a generator. Let C be cyclic of infinite order, c a generator. Form the split extension G of D by C defined by setting $d^c = d^2$, $d^{c-1} = d^3$. Then c^4 centralises D. We assert that c^4 is definable in G by the following infinite set of formulae:
$(\exists x)(\exists w)(\forall y)(wy = yw \;\&\; x \neq e \;\&\; x^5 = e \;\&\; x^w = x^2 \;\&\; z = w^4)$ for each $m \in Z$, $m \neq 0$:
$\neg(\exists w)(\forall y)(wy = yw \;\&\; w^{4m+1} = z)$. The argument is similar to that of Meskin, and is omitted. ($g^h = h^{-1}gh$.)

REFERENCES

[1] Fraleigh, J., A First Course in Abstract Algebra, Addison-Wesley, 1967.

[2] Gelfond, A. and Linnik, Y., Elementary Methods in the Analytic Theory of Numbers, (Translation by D. Brown). M. I. T. Press, 1966.

[3] Kopperman, R., The $L_{\omega_1\omega_1}$-theory of Hilbert spaces, J. Symbolic Logic, 32 (1967), 295-304.

[4] Niven, I. and Zuckerman, H., An Introduction to the Theory of Numbers, (Second Edition), Wiley, 1966.