SUBGROUPS OF THE MULTIPLICATIVE GROUP OF A DIVISION RING

BY

R. J. FAUDREE[1]

Introduction. The general question of what groups can be embedded in the multiplicative group of a division ring is an unsolved problem, but some parts of the problem have been completely solved. It is well known that an abelian group can be embedded in a division ring if and only if its torsion subgroup is locally cyclic (see [4]). B. H. Neumann (see [10]) and A. I. Malcev (see [9]) showed that all ordered groups can be embedded in a division ring and Amitsur solved the problem for finite groups (see [2]). These results exhaust the major work that has been done on the problem to date.

Iwasawa showed that any torsion-free nilpotent group can be ordered (see [7]); therefore, by Neumann's and Malcev's result any torsion-free nilpotent group can be embedded in a division ring. This paper will extend this result by showing that certain torsion-free solvable groups can be embedded in a division ring. This paper will also extend the results on abelian, finite and ordered groups by giving an embedding theorem for a group G which has an abelian, finite or ordered group H as a normal subgroup and a certain normal structure between H and G.

An embedding theorem. Let Γ denote a fixed division ring, x an indeterminate over Γ and θ an automorphism of Γ. $\Gamma\langle x;\theta\rangle$ will denote the Hilbert division ring of all formal power series in x over Γ (see [9]) $\Gamma\langle x;\theta\rangle = \{\sum_{i=n}^{\infty} a_i x^i \mid a_i$ in Γ and n any integer$\}$, where addition and equality are defined as in a commutative power series ring and multiplication is determined by the equation $x \cdot a = \theta(a) \cdot x$ for all a in Γ. Let $\Gamma[x;\theta]$ denote the ring of polynomials in $\Gamma\langle x;\theta\rangle$, that is the ring generated by Γ and x; and let $\Gamma(x;\theta)$ denote the division ring generated by Γ and x. $\Gamma[x;\theta]$ is an Ore polynomial ring (see [11]) and thus has a quotient field which is uniquely determined up to isomorphism. Therefore $\Gamma(x;\theta) = \{f(x)g^{-1}(x) \mid f(x), g(x) \neq 0$ in $\Gamma[x;\theta]\} = \{g^{-1}(x)f(x) \mid f(x), g(x) \neq 0$ in $\Gamma[x;\theta]\}$. This structure of $\Gamma(x;\theta)$ is of importance.

Received by the editors April 4, 1965.

[1] This represents a portion of the author's Doctoral dissertation for the Ph.D. at Purdue University.

In the following discussion G will denote a group, H and H_i subgroups of G; and D will denote a division ring and D_i subdivision rings of D. The multiplicative group of D will be denoted by D^*, and if G is a subgroup of D^* then $D_i = \{H_i\}$ will mean that D_i is the division ring generated by H_i.

An ascending normal series $\{H_i \mid 0 \leqq i \leqq \alpha,\ H_0 = H \text{ and } H_\alpha = G\}$ will be called a *completely infinite supercyclic series from H to G* if each factor group H_{i+1}/H_i is infinite cyclic. If such a series exists G is said to be *completely infinite supercyclic from H to G*. In the case where $H = \{e\}$, the identity subgroup, G is a *completely infinite supercyclic group.*

The class of completely infinite supercyclic groups is a large one. Let G be a solvable group, say $G^{(n)} = \{e\}$, where $G^{(i)}$ is the ith derived group. If $G^{(i)}/G^{(i+1)}$ is a free abelian group for each i, then there obviously is a completely infinite supercyclic series from $G^{(i+1)}$ to $G^{(i)}$; hence such a series exists from $\{e\} = G^{(n)}$ to G. The free solvable groups comprise an important subclass of the above class. Let F be a free group. By Schreiers Theorem $F^{(i)}$ is also a free group so $F^{(i)}/F^{(i+1)}$ is a free abelian group; hence $F/F^{(n)}$ is a completely infinite supercyclic group for any positive integer. J. F. Bowers discussed a class of groups which he called completely infinite polycyclic groups (see [3]) which are also completely infinite supercyclic groups. A finitely generated torsion-free nilpotent group has a completely infinite supercyclic series, in fact one of finite length (see [13, p. 241]).

Let G be a subgroup of D^* such that $D = \{G\}$, let $\{H_i \mid 0 \leqq i \leqq \alpha\}$ be a completely infinite supercyclic series from H to G with $H_{i+1} \cdot H_i = (x_{i+1} \cdot H_i)$ for x_{i+1} in H_{i+1}, and let $D_i = \{H_i\}$. If x_{i+1} is transcendental over D_i $(0 \leqq i < \alpha)$ then we call D an *Ore extension of D_0 determined by the completely infinite supercyclic series $\{H_i \mid 0 \leqq i \leqq \alpha\}$.*

We will now give some elementary properties of Ore extensions. The following proposition is an easy consequence of elementary Ore polynomial ring theory:

PROPOSITION 1. *Let Γ be a subdivision ring of a division ring D and x an element of D which is transcendental over Γ. If $x\Gamma x^{-1} = \Gamma$, then D_1, the division ring generated by Γ and x, is isomorphic to $\Gamma(x;\theta)$ where θ is the automorphism of Γ induced by x.*

Thus if D is an Ore extension of D_0 determined by the completely infinite supercyclic series $\{H_i \mid 0 < i < \alpha\}$, then D_{i+1} is isomorphic to $D_i(x_{i+1};\theta_{i+1})$ where θ_{i+1} is the automorphism of D_i induced by x_{i+1}.

PROPOSITION 2. *Let θ and τ be automorphisms of a division ring D, and x and y indeterminates over D. Then θ can be extended to be an automorphism of $D(x;\tau)$ onto $D(y;\theta\tau\theta^{-1})$ which takes x into y.*

Since $x \cdot d = \tau(d)x$ and $y \cdot \theta(d) = \theta\tau(d) \cdot y$ for all d in D, the map determined by $x \to y$ and $d \to \theta(d)$ for all d in D is an automorphism of $D(x;\tau)$ onto $D(y;\theta\tau\theta^{-1})$.

PROPOSITION 3. *Let G be a group with a normal subgroup H and two completely infinite supercyclic series* $\{H_i \mid 0 \leqq i \leqq \alpha_1\}$ *and* $\{H'_i \mid 0 \leqq i \leqq \alpha_2\}$ *from H to G. If D is an Ore extension of* D_0 *determined by the series* $\{H_i \mid 0 \leqq i \leqq \alpha_1\}$, *then D is an Ore extension of* D_0 *determined by the series* $\{H'_i \mid 0 \leqq i \leqq \alpha_2\}$.

Proposition 3 is obvious if $\alpha_1 = 1$ and the proof can be completed by a straightforward application of transfinite induction and Proposition 1.

THEOREM 1. *Let* $\{H_i \mid 0 \leqq i \leqq \alpha\}$ *be a completely infinite supercyclic series from H to G and let D be an Ore extension of* D_0 *determined by the series* $\{H_i \mid 0 \leqq i \leqq \alpha\}$. *If* θ *is an automorphism of G such that* $\theta \mid H$ *can be extended to an automorphism of* D_0, *then* θ *can be extended to an automorphism of D.*

If $\alpha = 1$, then Propositions 1 and 2 imply that the Theorem is true. With Proposition 3 the proof can be completed by means of transfinite induction.

THEOREM 2. *Let G be a group with a normal subgroup H and a completely infinite supercyclic series* $\{H_i \mid 0 \leqq i \leqq \alpha\}$ *from H to G with* $H_{i+1}/H_i = (x_{i+1} \cdot H_i)$ *for* x_{i+1} *in* H_{i+1}. *If H can be embedded in a division ring* D_0 *with* $D_0 = \{H\}$ *such that the automorphism of H induced by* x_{i+1} *can be extended to an automorphism of* D_0, *then G can be embedded in a division ring D which is an Ore extension of* D_0 *determined by the completely infinite supercyclic series* $\{H_i \mid 0 \leqq i \leqq \alpha\}$.

Consider the division ring $D_1 = D_0(y_1; \theta_1)$ where θ_1 is the automorphism of D_0 induced by x_1 and y_1 an indeterminate over D_0. Since $y_1 h y_1^{-1} = \theta_1(h) = x_1 h x_1^{-1}$ for all h in H, the map of H_1 into D_1^* determined by $x_1 \rightarrow y_1$ and $h \rightarrow h$ for all h in H is an isomorphism onto $Gp(H, y_1)$. This completes the first step of an induction proof. Using Theorem 1 to extend automorphisms the proof of Theorem 2 can be completed by transfinite induction.

For a detailed look at a construction of a division ring like the one used in Theorems 1 and 2 look at a paper by M. Ikeda (see [6]).

Before stating some consequences of Theorems 1 and 2 some definitions will given. A group G is said to have *property E* if G can be embedded in a division ring. A group G has *property EE* if G can be embedded in some division ring D such that any automorphism of G can be extended to an automorphism of D; and an ordered group G has *property EE** if G can be embedded in some division ring D such that any order automorphism of G can be extended to D.

It is important to note that the above definition just requires the existence of one such division ring with the extending property for every automorphism, not every division in which G can be embedded.

In view of these definitions we have:

COROLLARY 1. *If a group G has a normal subgroup H with property EE and a* *completely infinite supercyclic series from H to G, then G has property E. If in addition H is a characteristic subgroup, then G has property EE.*

COROLLARY 2. *Let G be a group with a normal subgroup H with property EE^* and a completely infinite supercyclic series $\{H_i \mid 0 \leqq i \leqq \alpha\}$ from H to G with $H_{i+1}/H_i = (H_{i+1} \cdot H_i)$. If each x_{i+1} induces an order automorphism on H, then G has property E.*

Since the identity group has property EE, we have the following:

COROLLARY 3. *If G is a completely infinite supercyclic group, then G has property EE.*

COROLLARY 4. *Let G be a solvable group, say $G^{n+1} = 1$. If $G^{(i)}/G^{(i+1)}$ is a free abelian group $(0 \leqq i \leqq n)$, then G has property EE. In particular if $F^{(n)}$is a free group then $F/F^{(n)}$ has property EE.*

COROLLARY 5. *A finitely-generated torsion-free nilpotent group has property EE.*

The results of Neumann and Malcev (see [10] and [9]) prove that the groups of Corollaries 3, 4, and 5 have property E since they can be ordered. But it is not true that all completely infinite supercyclic groups can be ordered, for the group $G_p(x, y \mid yxy^{-1} = x^{-1})$ is such a group.

The construction of Theorem 2 is not sufficient to completely determine which torsion-free solvable groups have property E. $G^{(i)}/G^{(i+1)}$ may not be free abelian, even though G is a torsion-free solvable group; for example the additive rationals Q^+, has this property. This is not really a difficulty for by a modification of the proofs, the assumption in Theorem 2 that H_i/H_{i+1} is infinite cyclic can be replaced by the condition that H_i/H_{i+1} is a subgroup of Q^+, since any such group is a union of a countable tower of infinite cyclic groups. A difficulty still arises since there are finitely-generated torsion-free solvable groups which are not completely infinite supercyclic groups. $G = G_p(b_1, b_2, c \mid b_i = b_i^c = b_i^{-1}, [b_1, b_2] = C^{2x}, i = 1$ or 2) is a supersolvable torsion-free group, but every supersolvable series of G has a factor of order 2 (see [3] and [5]).

The remainder of the paper will be devoted to determining which finite, abelian or ordered groups have property EE or EE^*.

Property EE for finite groups. In this section we will prove that all finite groups with property E have property EE using Amitsur's classification for such groups (see [2]). First some notation will be given.

Let m and r be relatively prime integers. Put $s = (r-1, m)$, $t = m/s$ and $n =$ minimal integer satisfying $r^n \equiv 1 \pmod{m}$. Denote by $G_{m,r}$ group generated by two elements A and B satisfying the relations $A^m = 1, B^n = A^t$ and $BAB^{-1} = A^r$. Let Q denote the rational field and e_m a fixed primitive mth root of unity. σ_r will represent the automorphism of $Q(e_m)$ determined by $e_m \to e_m^r$. $\mathfrak{A}_{m,r} = (Q(e_m), \sigma_r, e_s)$

will denote the cyclic algebra determined by the field $Q(e_m)$, automorphism σ_r, and element $e_s = e_m^t$, as defined by Albert (see [1, p. 74]).

If G is a group $A(G)$, $I(G)$, $Z(G)$ and $|G|$ will denote the automorphism group, inner-automorphism group, center of group and order of group respectively. $\mathfrak{T}$, $\mathfrak{D}$ and $\mathfrak{J}$ will denote the binary tetrahedral, binary octahedral and binary iscosahedral group respectively. They are isomorphic to G_1, G_2 and G_3 respectively where $G_i = G_p(A, C \mid A^{2(i+2)} = 1,\ C^3 = A^{(i+2)}$ and $CAC^{-1} = A^{-1}C)$. Also $\mathfrak{T}$, $\mathfrak{D}$ and $\mathfrak{J}$ have order 24, 48 and 120 respectively, have center of order 2 and have automorphism groups of order 24, 48 and 60 respectively. These groups are discussed in an article by Vincent (see [12]) and in Amitsur's paper (see [2]).

With these definitions we can state an important theorem proved by Amitsur (see [2]).

THEOREM 3. *A finite group G has property E if and only if G is one of the following types*:

(1) *A group $G_{m,r}$ with property E*;

(2) *A group $\mathfrak{T} \times G_{m,r}$, where $G_{m,r}$ has property E, $(6, |G_{m,r}|) = 1$, and other conditions hold* (*see* [2]);

(3) *The groups $\mathfrak{D}$ and $\mathfrak{J}$.*

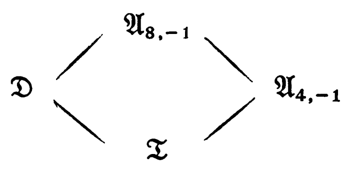
We will use this theorem to prove that a finite group with property E has property EE. First we will prove some lemmas.

LEMMA 1. *If $G_{m,r}$ has property E, then $G_{m,r}$ has property EE.*

Proof. If $G_{m,r}$ has property E then $A \to e_m$ and $B \to \sigma_r$ defines an embedding of $G_{m,r}$ into the division ring $\mathfrak{A}_{m,r} = (Q(e_m), \sigma_r, e_s)$, (see[2]). Using this identification we have $\mathfrak{A}_{m,r} = (Q(A), B^t, A)$. Let θ be an automorphism of G. Direct calculation verifies that $A \to \theta(A)$ and $B \to \theta(B)$ defines an automorphism of $\mathfrak{A}_{m,r}$ which extends the automorphism θ.

LEMMA 2. *$\mathfrak{T}$ has property EE.*

Proof. $\mathfrak{T}$ can be embedded in $\mathfrak{A}_{4,-1}$ and $\mathfrak{D}$ can be embedded in $\mathfrak{A}_{8,-1}$. $\mathfrak{D}$ has an isomorphic copy of $\mathfrak{T}$ as a normal subgroup. Thus with appropriate identification we have the following diagram (see [2]).



Since $\mathfrak{T}$ is normal in $\mathfrak{D}$ there is an element x in $\mathfrak{D}$ which induces an outer-automorphism θ on $\mathfrak{T}$. But $x\mathfrak{T}x^{-1} = \mathfrak{T}$ implies $x\mathfrak{A}_{4,-1}x^{-1} = \mathfrak{A}_{4,-1}$, so θ can be extended to $\mathfrak{A}_{4,-1}$. Since $|A(\mathfrak{T})/I(\mathfrak{T})| = 2$ the proof is complete, for any inner-automorphism can be extended.

LEMMA 3. *$\mathfrak{O}$ has property E.*

Proof. Since $|A(\mathfrak{O})/I(\mathfrak{O})| = 2$ it is sufficient to show that one outer-automorphism of $\mathfrak{O}$ can be extended to $\mathfrak{A}_{8,-1} \cdot \mathfrak{A}_{8,-1} \cong Q(2^{1/2}) \otimes_Q \mathfrak{A}_{4,-1}$ and $\mathfrak{A}_{4,-1}$ is isomorphic to the rational quarternions. Identifying elements under the isomorphisms mentioned above we have

$$\mathfrak{O} = \{\pm (1 \pm i \pm j \pm k)/2, \ \pm \{1, i, j, k\},$$
$$\pm(1 \pm \{i, j, k\})/2^{1/2}, \ \pm (i \pm \{j, k\})/2^{1/2}, \ \pm (j \pm k)/2^{1/2}\}$$

is a subgroup of $\mathfrak{A}_{8,-1}$ which generates $\mathfrak{A}_{8,-1}$ (see [2]). The map $2^{1/2} \to -2^{1/2}$ obviously defines an automorphism θ of $\mathfrak{A}_{8,-1}$ and $\theta | \mathfrak{O} = \mathfrak{O}$. θ is an outer automorphism since $2^{1/2}$ is in the center of $\mathfrak{A}_{8,-1}$, thus an outer-automorphism of $\mathfrak{O}$ can be extended to $\mathfrak{A}_{8,-1}$.

LEMMA 4. *$\mathfrak{J}$ has property EE.*

Proof. $\mathfrak{J}$ can be embedded in $\mathfrak{A}_{10,-1} \cong Q(5^{1/2}) \otimes_Q \mathfrak{A}_{4,-1}$ and with appropriate identification we have that $\mathfrak{J}$ is the subgroup of $\mathfrak{A}_{10,-1}$ generated by j, i_1, and e where e is a primitive 5th root of unity and $i_1 = (e^2 - e^3 + (e - e^4)j)5^{1/2}$ (see [2]). $\mathfrak{J}$ also generates $\mathfrak{A}_{10,-1}$. Obviously the map $5^{1/2} \to -5^{1/2}$ defines an outer-automorphism θ of $\mathfrak{A}_{10,-1}$ since $5^{1/2}$ is in the center of $\mathfrak{A}_{10,-1}$. Direct calculation verifies that $\theta | \mathfrak{J} = \mathfrak{J}$. Therefore θ is an extension of an outer-automorphism of $\mathfrak{J}$, which completes the proof since $|A(\mathfrak{J}) | I(\mathfrak{J})| = 2$.

With these lemmas we are prepared to prove

THEOREM 4. *A finite group with property E also has property EE.*

Proof. Groups of type (1) and (3) of Theorem 3 have property EE by Lemmas 1, 3 and 4. If $G = \mathfrak{T} \times G_{m,r}$ has property E, then G can be embedded in $\mathfrak{A}_{4,-1} \otimes_Q \mathfrak{A}_{m,r}$ in the natural way (see [2]). There is no loss of generality in assuming $\mathfrak{T}$ is in $\mathfrak{A}_{4,-1}$ and $G_{m,r}$ is $\mathfrak{A}_{m,r}$. If θ is an automorphism of G then $\theta = \theta | \mathfrak{T}$ and $\theta_2 = \theta | G_{m,r}$ are automorphisms of $\mathfrak{T}$ and $G_{m,r}$ respectively since $(6, |G_{m,r}|) = 1$. θ_1 and θ_2 can be extended to automorphism θ_1' and θ_2' of $\mathfrak{A}_{4,-1}$ and $\mathfrak{A}_{m,r}$ respectively by lemmas 1 and 2. Thus $\theta_1' \otimes \theta_2'$ is an automorphism of $\mathfrak{A}_{4,-1} \otimes_Q \mathfrak{A}_{m,}$ which extends θ. This completes proof of Theorem 4.

Property *EE* for abelian groups.

THEOREM 5. *If G is an abelian group with property E, then G has property EE.*

Proof. Let G be an abelian group generated by elements x_i $(i \in I)$ which is embeddable in a field. The construction of Cohn (see [4]) yields a field K which is generated by the x_i as a field, with the multiplicative relations holding between the x_i as defining relations. Thus every relation Φ holding in K between the x_i follows from the defining relations in G. Hence if $\theta: x_i \to x_i'$ is an automorphism of G, any relation Φ between the x_i also holds between the x_i' and conversely. Therefore $x_i \to x_i'$ defines an automorphism of K which extends θ.

Property EE^* for ordered groups. An ordered group G can be embedded in the formal power series ring D of G over any division ring K (see [10]). An element ψ of D is a map on G into K such that the subset of G on which ψ takes nonzero values is a well-ordered subset. If ψ and ϕ are in D and g in G, then addition and multiplication in D are defined componentwise as follows:

$$(\psi + \phi)(g) = \psi(g) + \phi(g),$$

$$\psi \cdot \phi(g) = \sum_{rs = g} \psi(r)\,\phi(s).$$

THEOREM 6. *If G is an ordered group, then G has property EE^*.*

Proof. Let Γ be the formal power series ring of G over the rational field Q. If ψ is in Γ, then ψ is a function of G into Q such that $\psi(g) \neq 0$ if and only if g is in S_ψ, a well ordered subset of G. Let π_g be the function defined as follows:

$$\pi_g(h) = 1 \text{ if } g = h \text{ and zero otherwise.}$$

The map

$$\sigma:\ G \to \Gamma$$

$$g \to \pi_g \text{ for all } g \text{ in } G$$

is the embedding of G into Γ (see [12]).

Under this identification G is a subset of Γ. Let D be the division ring in Γ generated by G, and let θ be an order automorphism of G. Define the following map:

$$\theta' : D \to \Gamma$$

$$\theta'(\psi)(g) = \psi(\theta^{-1}(g)) \text{ for all } g \text{ in } G.$$

$\theta'(\psi)(g) = 0$ if and only if $\theta^{-1}(g)$ is in S_ψ, or equivalently if g is in $\theta(S_\psi)$. Since θ is an order automorphism, $\theta(S_\psi)$ is a well-ordered subset of G; since θ' is well defined. Direct calculation verifies that if ψ and ζ are in D then

$$\theta'(\psi + \zeta)(g) = \theta'(\psi)(g) + \theta'(\zeta)(g)$$

and

$$\theta'(\psi \cdot \zeta)(g) = (\theta'(\psi) \cdot \theta'(\zeta))(g).$$

Therefore θ' is an isomorphism of D into Γ. Also obviously $\theta'(\pi G) = \pi_{\theta(g)}$, hence $\theta' \mid G = \theta$. Since $\theta(G) = G$ and $D = \{G\}$, $\theta(D) = D$, thus θ is an automorphism of D extending θ.

In conclusion we summarize some of the results of Theorems 1, 2, 4, 5 and 6.

THEOREM 7. *Let G be a group with a normal subgroup H and a completely infinite supercyclic series from H to G.*

(i) *If H is finite or abelian, then G has property E if and only if H has property E.*

(ii) *If H is finite or abelian and characteristic in G, then G has property EE if and only if G has property E.*

(iii) *If H is an ordered subgroup of G such that every automotomorphism of H induced by an element of G is an order automorphism, then G has property E.*

BIBLIOGRAPHY

1. A. A. Albert, *Structure of algebras*, Amer. Math. Soc. Colloq. Publ. Vol. 24, Amer. Math. Soc., Providence, R. I., 1939.
2. S. A. Amitsur, *Finite subgroups of division rings*, Trans. Amer. Math. Soc. **80** (1955), 361–386.
3. J. F. Bowers, *On composition series of polycyclic groups*, J. London Math. Soc. **35** (1960), 433–444.
4. P. M. Cohen, *Eine Bemerkung über die multiplicative Gruppe eines Korpers*, Arch. Math. **13** (1962), 344–348.
5. K. A. Hirsch, *On infinite soluble groups*. IV, J. London Math. Soc. **27** (1952), pp. 81–85.
6. M. Ikeda, *Schiefkorper unendlichen Ranges über dem Zentrum*, Osaka Math. J. **14** (1962), 135–144.
7. K. Iwasawa, *On linearly ordered groups*, J. Math. Soc. Japan **1** (1948), 1–9.
8. N. Jacobson, *Structure of rings*, Amer. Math. Soc. Colloq. Publ. Vol. 37, Amer. Math. Soc., Providence, R. I., 1956.
9. A. I. Malcev, *On the embedding of group algebras in division algebras*, Dokl. Akad. Nauk SSSR **60** (1948), 1499–1501.
10. B. H. Neumann, *On ordered division rings*, Trans. Amer. Math. Soc. **66** (1949), 202–252.
11. O. Ore, *Theory of non-commutative polynomials*, Ann. of Math. **34** (1933), 480–508.
12. G. Vincent, *Les groupes linéaires finis sans points fixes*, Comment. Math. Helv. **20** (1947), 117–171.
13. H. Zassenhaus, *The theory of groups*, Macmillan, New York, 1958.

UNIVERSITY OF CALIFORNIA,
BERKELEY, CALIFORNIA