RENDICONTI
del
SEMINARIO MATEMATICO
della
UNIVERSITÀ DI PADOVA

R. S. PIERCE
C. I. VINSONHALER

Carriers of torsion-free groups

Rendiconti del Seminario Matematico della Università di Padova, tome 84 (1990), p. 263-281

<http://www.numdam.org/item?id=RSMUP_1990__84__263_0>

REND. SEM. MAT. UNIV. PADOVA, Vol. 84 (1990)

Carriers of Torsion-Free Groups.

R. S. PIERCE - C. I. VINSONHALER (*)

1. Introduction.

Our objective in this paper is to determine the possible carriers of some special classes of torsion-free abelian groups and rings. Here we define the *carrier* $c(A)$ of a torsion-free (abelian) group A to be the set of all rational primes p such that $pA \neq A$. The classes of groups and rings that concern us are described in terms of an algebraic number field F and the ring 0_F of algebraic integers in F. We denote by $\boldsymbol{I}(F)$ the set of 0_F-submodules A of F such that $1 \in A$, and the quasi-endomorphism ring $QE(A)$ coincides with the set $\{\lambda_r\colon r \in F\}$ of left translation mappings $\lambda_r\colon a \mapsto ra$ by elements of F. Let $\boldsymbol{E}(F)$ be the set of subrings of F that are members of $\boldsymbol{I}(F)$. For example, $\boldsymbol{I}(\mathbb{Q})$ consists of all subgroups of $\mathbb{Q}$ that include 1 (hence, up to isomorphism, all rank one groups) and $\boldsymbol{E}(\mathbb{Q})$ is the set of all subrings of $\mathbb{Q}$. In general, for $R \in \boldsymbol{E}(F)$, the hypothesis $0_F \subseteq R$ implies (for example, by 3.1 below) that R is integrally closed in F, hence a Dedekind domain. The problem that interests us is: which subsets Ξ of the set Π of all rational primes can be realized as $c(A)$ for some $A \in \boldsymbol{I}(F)$, and which Ξ have the form $c(S)$ for some $S \in \boldsymbol{E}(F)$? Our main results are that $\{c(A)\colon A \in \boldsymbol{I}(F)\} = \{c(S)\colon S \in \boldsymbol{E}(F)\}$, and, in the case that F is a normal extension of $\mathbb{Q}$, the family $\{c(S)\colon S \in \boldsymbol{E}(F)\}$ is determined modulo a finite set of primes by the structure of the Galois group $\mathrm{Gal}(F/\mathbb{Q})$.

(*) Indirizzo degli AA.: Dept. of Mathematics, University of Arizona, Tucson, AZ 85721, U.S.A.

Research supported, in part, by NSF Grant DMS-8802062.

Our motivation for studying this question comes from several sources. In [Re], Reid introduced the class of irreducible groups. A torsion-free group B is irreducible if the only pure, fully invariant subgroups of B are 0 and B. If the rank of the torsion-free group B is finite, then B is irreducible if and only if B is quasi-isomorphic to a finite direct sum of copies of a group A such that the quasi-endomorphism ring $QE(A)$ of A is a division algebra with $\operatorname{rk} A = \dim_{\mathbb{Q}} QE(A)$. The groups of $\boldsymbol{I}(F)$ constitute a set of isomorphism representatives of those strongly indecomposable, irreducible groups A such that $QE(A) \cong F$. In earlier papers [P-V1] and [P-V2] the authors examined the question: for which division algebras D and $p \in \Pi$ is there a finite rank, irreducible group A such that $QE(A) \cong D$ and $c(A) = \{p\}$? We found that if D is not a field, then almost all p have this property, but when D is a field, then the situation is still not well understood,

Another source of interest in the carriers of the $R \in \boldsymbol{E}(F)$ comes from the study of E-rings. An E-ring is a ring R such that

$$\operatorname{Hom}_{\mathbb{Z}}(R, R) = \operatorname{Hom}_{R}(R, R) .$$

This concept was introduced by Schultz [S] in 1975. Although, they seem to be very special, E-rings arise naturally in many contexts. (See [A-P-R-V-W], [B-S], [D-M-V], and [P1].) The rings belonging to $\boldsymbol{E}(F)$ are E-rings, and every strongly indecomposable E-ring of finite rank is quasi-isomorphic to a member of $\boldsymbol{E}(F)$ for some algebraic number field F. The carriers of E-rings arise naturally in the effort to classify these rings up to quasi-isomorphism, as is seen in [P-V3].

Finally, our results in this paper shed light on a question that arises from the results of Zassenhaus and Butler on realizing rings as endomorphism rings of abelian groups. By the theorem of Zassenhaus [Z] (improved by Butler in [B1]), any ring R that is finitely generated as an abelian group is isomorphic to the endomorphism ring $\operatorname{End} A$, where A is a torsion-free group with $\operatorname{rk} A = \operatorname{rk} R$. If R is the ring of integers in the algebraic number field F, then the group A is isomorphic to a group in $\boldsymbol{I}(F)$, as is easily seen. It is natural to ask if the hypothesis that R is a finitely generated $\mathbb{Z}$ module can be weakened to the requirement that R is a finitely generated S module, where S is the localization of $\mathbb{Z}$ at some set $\Xi \subseteq \Pi$. In this case, Ξ would have to be the carrier of R and hence also the carrier of the realizing group A. An example in Corner's paper [C] shows that such a generalization is not always possible if $\Xi = \{p\}$. Our results in

Section 5 below show there is no such generalization even in cases that Ξ is infinite.

The terminology and notational conventions in this paper are standard in the literature of abelian groups. All of the groups and rings that we consider in this paper are assumed to be additive subgroups of a finite dimensional $\mathbb{Q}$-space, so that they are torsion-free abelian groups of finite rank. To simplify our statements, the term « group » will mean a torsion-free abelian group of finite rank, and « ring » will designate an associative ring with unity whose additive group is torsion-free and has finite rank. If A is a group, then $\mathbb{Q}A$ denotes the rational hull of A, that is, $\mathbb{Q}A = \bigcup_{n\in\mathbb{N}} n^{-1}A$. Similar notation is used for rings. Note that if R is a ring, then so is $\mathbb{Q}R$. In fact, if R is an integral domain, then $\mathbb{Q}R$ is the fraction field of R, since a finite dimensional $\mathbb{Q}$-algebra which is an integral domain is a field. The letters F and K will denote fields. Except in Section 3, they will be algebraic number fields, in which case, their rings of integers will be denoted by 0_F and 0_K.

2. Reduction steps.

Our first observation makes it possible to work within the quasi-category of groups, and to limit our attention to strongly indecomposable groups.

2.1. Lemma. (*a*) If the groups A and B are quasi-isomorphic, then $c(A) = c(B)$.

(*b*) For groups A and B, $c(A \oplus B) = c(A) \cup c(B)$.

The statement (*a*) is clear from the observation that $p \in c(A)$ if and only if the p-rank of A is not zero, and p-rank is a quasi-isomorphism invariant. (See [A], Theorem 0.2.) The assertion (*b*) is obvious from the definition of carriers.

As we noted above, every irreducible group B is quasi-isomorphic to a direct sum of copies of a strongly indecomposable, irreducible group A, and by 2.1, $c(B) = c(A)$. Thus, to characterize the carriers of irreducible groups, it suffices to consider only those groups that are strongly indecomposable. A similar reduction exists in the case of E-rings. Indeed, by a result of Bowshell and Schultz ([B-S], The-

orem 3.12), every E-ring is quasi-isomorphic to a direct product of strongly indedomposable E-rings.

Recall the notation $\boldsymbol{I}(F)$ and $\boldsymbol{E}(F)$, where F is an algebraic number field. The elements of $\boldsymbol{I}(F)$ are those 0_F-submodules A of F with $1 \in A$, such that $QE(A)$ is the set of left translation maps λ_r of A by elements of F, and $\boldsymbol{E}(F)$ is the collection of all $R \in \boldsymbol{I}(F)$ such that R is a subring of F.

2.2. LEMMA. Let F be an algebraic number field. (*a*) If B is a strongly indecomposable, irreducible group such that $QE(A) \cong F$, then there exists $A \in \boldsymbol{I}(F)$ such that $c(A) = c(B)$. (*b*) If S is a strongly indecomposable E-ring such that $\mathbb{Q}S \cong F$, then there exists $R \in \boldsymbol{E}(F)$ such that $c(R) = c(S)$.

PROOF. Since B is irreducible and strongly indecomposable, it follows from [Re], Theorem 5.4 that $\mathbb{Q}B$ can be viewed as a one dimensional F-space. Thus, B can be identified with a subgroup of F such that $1 \in B$ and $L(B) = \{r \in F: rB \subseteq B\}$ is a full subring of B. Since 0_F is finitely generated, there exist $n \in \mathbb{N}$ such that $n0_F \subseteq L(B)$. Then $A = 0_F B$ satisfies $nA = n0_F B \subseteq L(B)B \subseteq B \subseteq A$, that is $A \doteq B$. Thus, $c(A) = c(B)$. The same proof applies to the E-ring case since $QE(S) \cong \mathbb{Q}S \cong F$. □

We conclude this section with a remark about characterizing the irreducible groups whose quasi-endomorphism rings are fields.

2.3. LEMMA. For an irreducible, strongly indecomposable group A of rank $n \geqslant 1$, the following conditions are equivalent:

(1) $QE(A)$ is a field;

(2) there is an endomorphism φ of A such that for all non-zero $x \in A$, the elements $x, \varphi x, \ldots, \varphi^{n-1}x$ are linearly independent in $\mathbb{Q}A$;

(3) there is an endomorphism φ of A and $x \in A$ such that the elements $x, \varphi x, \ldots, \varphi^{n-1}x$ are linearly independent in $\mathbb{Q}A$.

PROOF. If (1) holds, then by the primitive element theorem, there exists $\varphi \in QE(A)$ such that $QE(A) = \mathbb{Q}[\varphi]$. Thus, $1, \varphi, \varphi^2, \ldots, \varphi^{n-1}$ are linearly independent over $\mathbb{Q}$ because $\dim QE(A) = \operatorname{rk} A = n$ by the irreducibility of A. If $x \in A$ and $\sum_{i<n} a_i \varphi^i x = 0$ with $a_i \in \mathbb{Q}$, not all 0, then $\psi x = 0$, where $\psi = \sum_{i<n} a_i \varphi^i \neq 0$. Since $QE(A)$ is a field, it follows

that $x = \varphi^{-1}\varphi x = 0$. Thus, (1) implies (2); and (3) is a weakening of (2). If (3) holds, then $1, \varphi, \varphi^2, \ldots, \varphi^{n-1}$ is a linearly independent subset of $QE(A)$. Hence, $\dim QE(A) = \operatorname{rk} A = n \leqslant \dim \mathbb{Q}[\varphi]$, because A is strongly indecomposable and irreducible. Thus, $QE(A) = \mathbb{Q}[\varphi]$ is commutative. □

3. Characteristics.

We will need to develop a characterization of the groups in $\boldsymbol{I}(F)$ and the rings in $\boldsymbol{E}(F)$. The framework for these descriptions is a representation of rank one modules over a Dedekind domain D in terms of characteristics, due originally to Ribenboim [Ri]. (See also the paper [K] by Kolettis.) The purpose of this section is to describe Ribenboim's results. We may just as well do so in the context of an arbitrary Dedekind domain D with fraction field F.

Denote by $\boldsymbol{J}(D)$ the family of all D-submodules A of F such that $1 \in A$. If F is an algebraic number field, we will write $\boldsymbol{J}(F)$ instead of $\boldsymbol{J}(0_F)$; in this case, $\boldsymbol{I}(F) \subseteq \boldsymbol{J}(F)$. For $A \in \boldsymbol{J}(D)$ and $P \in \max D$, the set of all maximal ideals in D, denote

$$\chi_A(P) = \sup \{n < \omega : 1 \in P^n A\} .$$

(As is customary, we will write $\chi_A(P) = \infty$ if this supremum is ω, that is, if $1 \in P^n A$ for all $n < \omega$.) The product $P^n A$ is to be interpreted as the usual product of D-submodules of F. Note that $1 \in A = P^0 A$, so that this definition yields a well defined mapping χ_A: $\max D \to \omega \cup \{\infty\}$. A mapping from $\max D$ to $\omega \cup \{\infty\}$ is called a *characteristic* over D. Thus, $A \mapsto \chi_A$ is a mapping from $\boldsymbol{J}(D)$ to the set $X(D)$ of all characteristics over D. The ordering of $\omega \cup \{\infty\}$ (in which $n < \infty$ for all $n \in \omega$) induces a partial ordering of $X(D)$ by the condition $\chi \leqslant \theta$ if $\chi(P) \leqslant \theta(P)$ for all $P \in \max D$. As an ordered set, $X(D)$ is a product of copies of the complete chain $\omega \cup \{\infty\}$, so that $X(D)$ is a complete, distributive lattice. It is clear from our definitions that if $A \subseteq B$ in $\boldsymbol{J}(D)$, then $\chi_A \leqslant \chi_B$ in $X(D)$.

For $\chi \in X(D)$, denote

$$A_\chi = \{x \in F : \text{for all } P \in \max D,$$
$$\text{there exists } n < \omega \text{ with } n \leqslant \chi(P) \text{ and } xP^n \subseteq D_P\} .$$

Here, D_P denotes the localization of D at P. Clearly, A_χ is a D-submodule of F, and $1 \in A_\chi$.

3.1. PROPOSITION. The mappings $A \mapsto \chi_A$, $\chi \mapsto A_\chi$ are mutually inverse, order isomorphisms between $\boldsymbol{J}(D)$ and $X(D)$. Moreover, for $A, B \in \boldsymbol{J}(D)$, $A \dot{\subseteq} B$ (i.e., $nA \subseteq B$ for some $n \in \mathbb{N}$) if and only if $\chi_A(P) \leqslant \leqslant \chi_B(P)$ for almost all $P \in \max D$ including those primes such that $\chi_A(P) = \infty$. Finally $R \in \boldsymbol{J}(D)$ is a subring of F if and only if χ_R takes only the values 0 and ∞.

Proofs of the statements in this proposition can be found in the papers of Ribenboim [Ri] and Kolettis [K].

We need three more lemmas on how properties of the groups in $\boldsymbol{J}(D)$ are reflected in the characteristics associated with these groups, These results apply to the context in which $D = 0_F$ with F an algebraic number field. To simplify notation, write Π_F for $\max 0_F$ and $\Pi_F(p) = \{P \in \Pi_F \colon p \in P\}$ for $p \in \Pi$, the set of all rational primes.

3.2. LEMMA. If $A \in \boldsymbol{J}(F)$, then

$$c(A) = \{p \in \Pi \colon \chi_A(P) < \infty \text{ for some } P \in \Pi_F(p)\} .$$

PROOF. By definition, $p \notin c(A)$ if and only if $pA = A$. The condition $pA = A$ is equivalent to $PA = A$ for all $P \in \Pi_F(p)$. Clearly $PA = A$ if and only if $P^n A = A$ for all $n \in \mathbb{N}$. The lemma therefore follows from the definition of $\chi_A(P)$. □

3.3. LEMMA. Assume that the algebraic number field F is normal over $\mathbb{Q}$. If $A \in \boldsymbol{J}(F)$ and $\beta \in \mathrm{Gal}\,(F/\mathbb{Q})$, then

(*a*) $\beta A \subseteq A$ if and only if $\chi_A(P) \leqslant \chi_A(\beta P)$ for all $P \in \Pi_F$;

(*b*) $\beta A \dot{\subseteq} A$ if and only if $\chi_A(P) \leqslant \chi_A(\beta P)$ for almost all $P \in \Pi_F$, including all P such that $\chi_A(P) = \infty$.

PROOF. Since $1 \in P^n A$ if and only if $1 \in (\beta P)^n \beta A$, it follows that $\chi_A(P) = \chi_{\beta A}(\beta P)$. The lemma follows from 3.1. □

3.4. LEMMA. Let F and K be algebraic number fields with $F \subseteq K$. For $A \in \boldsymbol{J}(F)$, denote $\overline{A} = 0_K A$. Then $\overline{A} \in \boldsymbol{J}(K)$ and for all $Q \in \Pi_K$,

$$\chi_{\overline{A}}(Q) = e(Q)\, \chi_A(Q \cap F) ,$$

where $e(Q)$ is the ramification index of Q over F. In particular, $\chi_{\bar{A}}(Q) = 0$ if and only if $\chi_A(Q \cap F) = 0$ and $\chi_{\bar{A}}(Q) = \infty$ if and only if $\chi_A(Q \cap F) = \infty$.

PROOF. Let θ be the characteristic over 0_K defined by $\theta(Q) = e(Q)\chi_A(Q \cap F)$. If $P = Q \cap F$, then the highest power of Q that divides $0_K P$ is Q^e, where $e = e(Q)$. Thus, if $1 \in P^n A$, then $1 \in Q^{en}\bar{A}$. Consequently $\theta \leqslant \chi_{\bar{A}}$. On the other hand, since $A = A_{\chi_A}$ by 3.1, if $x = \sum a_i y_i$ $(a_i \in 0_K,\ y_i \in A)$ is an element of $\bar{A}$, then there exists $n \in \omega$ with $n \leqslant \chi_A(P)$ such that $P^n y_i \in (0_F)_P$ for all i, and therefore $Q^{en}x \subseteq (0_K)_Q$. It follows that $x \in A_Q$. Consequently, $\bar{A} \subseteq A_Q$, so that $\chi_{\bar{A}} \leqslant \theta$. □

The results in 3.1 and 3.2 have an interesting consequence.

3.5. COROLLARY. If $A \in \boldsymbol{I}(F)$ is such that $c(A)$ is finite, then there exists $R \in \boldsymbol{E}(F)$ such that $A \doteq R$.

In particular, $c(R) = c(A)$; we will see later that this equality can be obtained without the assumption that $c(A)$ is finite.

We conclude this section with an application of 3.5 to the subject of local rings. Recall that a ring R is *local* if $\max R$ is a single ideal. Also, if $p \in \Pi$, then the algebraic number field F is said to be p-realizable if there is an irreducible group A such that A is p-local and $QE(A) \cong F$. Equivalently, there exists $A \in \boldsymbol{I}(F)$ such that $c(A) = \{p\}$. This terminology was introduced in [P-V1].

3.6. PROPOSITION. Let S be a local E-ring such that $\mathbb{Q}S = F$, an algebraic number field. Then $c(S) = \{p\}$ for some $p \in \Pi$ and F is p-realizable. Conversely, if F is p-realizable, then there is a local E-ring S such that $\mathbb{Q}S = F$ and $c(S) = \{p\}$.

PROOF. Assume that S is a local ring such that $\mathbb{Q}S = F$. Then $R = 0_F S \in \boldsymbol{J}(F)$, and $R \doteq S$ as we noted in the proof of 2.2. Also, by 3.1, R is a localization of 0_F at the multiplicative set consisting of the complement of $\cup \{P \in \Pi_F\colon \chi_R(P) = 0\}$. Thus, if $\max S = \{Q\}$ and $P \in \max R$ satisfies $Q = S \cap P$, then R/P is a finite field; and there exists a unique $p \in \Pi$ such that $p \in P$. Such an ideal P exists by [A-M], Theorem 5.10. It follows that $pS \subseteq Q \subset S$. If $q \in \Pi$ and $qS \neq S$, then $q \in qS \subseteq Q \subseteq P$. Therefore, $q = p$. This argument shows that $c(S) = \{p\}$ without the hypothesis that S is an E-ring. The latter assumption implies that F is p-realizable because $QE(S) =$

$= \mathbb{Q}S = F$. Conversely, assume that F is p-realizable, that is, there exists $A \in \boldsymbol{I}(F)$ such that $c(A) = \{p\}$. By 3.5, there exists $R \in \boldsymbol{E}(F)$ such that $c(R) = \{p\}$. Then $pR \neq R$ and $qR = R$ for all $q \neq p$ in Π. Let $S = \mathbb{Z} + pR$. Then $\mathbb{Q}S = F$ and $S \doteq R$; hence S is an E-ring. Moreover, $pR \lhd S$ and $S/pR \cong \mathbb{Z}/p\mathbb{Z}$ so that $pR \in \max S$. If $P \in \max R$, then $pR \subseteq P$ because $c(R) = \{p\}$. Therefore, $S \cap P = (\mathbb{Z} + pR) \cap P = (\mathbb{Z} \cap P) + pR = p\mathbb{Z} + pR = pR$. Since R is integrally closed (by 3.1 for example), the mapping $P \mapsto S \cap P$ is surjective from $\max R$ to $\max S$ ([A-M], Theorem 5.10). Thus, $\max S = \{pR\}$. □

4. Carriers of $\boldsymbol{I}(F)$.

In this section, F and K denote algebraic number fields with $F \subseteq K$. Moreover it is assumed that K is a normal extension of $\mathbb{Q}$. The Galois group $\mathrm{Gal}\,(K/\mathbb{Q})$ of K is denoted by G, and we write $H = \mathrm{Gal}\,(K/F)$. We identify F with a subring of $\mathrm{End}\,F$ via the translation mappings $x \mapsto \lambda_x$, where $\lambda_x y = xy$. Similarly, $K \subseteq \mathrm{End}\,K$.

For $A \in \boldsymbol{J}(F)$, denote $\overline{A} = 0_K A$. Thus, $\overline{A} \in \boldsymbol{J}(K)$.

4.1. Lemma. If $A \in \boldsymbol{J}(F)$, then $F \subseteq QE(A)$, $K \subseteq QE(\overline{A})$, and $H \subseteq QE(\overline{A})$.

Proof. If $x \in F$, then $nx \in 0_F$ for some $n \in \mathbb{N}$; and $n\lambda_x A \subseteq 0_F A = A$. Thus, $\lambda_x \in QE(A)$. Similarly, $K \subseteq QE(\overline{A})$. Finally, $\beta \in H$ implies

$$\beta\overline{A} = \beta(0_K A) = (\beta 0_K)(\beta A) = 0_K A = \overline{A}\,,$$

since 0_K is a G-module and $A \subseteq F$. □

If $A \in \boldsymbol{J}(F)$, then the condition for $A \in \boldsymbol{I}(F)$ is $QE(A) = F$. The next lemma shifts that condition to a property of $QE(\overline{A})$. We denote $KH = \left\{\sum_{\beta \in H} y_\beta \beta \colon y_\beta \in K\right\}$. By 4.1, KH is a $\mathbb{Q}$-subalgebra of $QE(\overline{A})$.

4.2. Lemma. If $A \in \boldsymbol{J}(F)$, then

$$QE(A) = F \quad \text{if and only if} \quad QE(\overline{A}) = KH\,.$$

A proof of this lemma can be found on pages 22-29 of Jacobson's book [J].

4.3. LEMMA. If $B \in \boldsymbol{J}(K)$, then

$$QE(B) = KN\,, \qquad \text{where } N = G \cap QE(B)\,.$$

PROOF. Plainly, $KN \subseteq QE(B)$. Since $\operatorname{End} K = KG$ (by 4.2 with $F = A = \mathbb{Q}$), it suffices to show that if $\sum_{\alpha \in G} x_\alpha \alpha \in QE(B)$, $x_\alpha \in K$, then $\alpha \in QE(B)$ for all $\alpha \in G$ such that $x_\alpha \neq 0$. This fact was established in the proof of Lemma 2.5 in [M-V]. □

4.4. THEOREM. Let $A \in \boldsymbol{I}(F)$. Then there is a finite set $\Xi_0 \subseteq c(A)$ with $|\Xi_0| < [F:\mathbb{Q}]$ such that if $\Xi_0 \subseteq \Xi \subseteq \Pi$, then $R \in \boldsymbol{E}(F)$ exists satisfying $c(R) = \Xi$.

PROOF. The hypothesis $A \in \boldsymbol{I}(F)$ implies $QE(A) = F$, so that $QE(\bar{A}) = KH$ by 4.2. It follows from 4.3 that $H = G \cap QE(\bar{A})$. Thus, if $\beta \in G \setminus H$, then $\beta\bar{A}$ is not quasi-contained in $\bar{A}$. It follows from 3.1 that either

(*a*) $\chi_{\bar{A}}(\beta Q) < \infty = \chi_{\bar{A}}(Q)$ for some $Q \in \Pi_K$, or

(*b*) $\chi_{\bar{A}}(\beta Q) < \chi_{\bar{A}}(Q)$ for infinitely many $Q \in \Pi_K$.

Let $\{\beta_0, \ldots, \beta_{s-1}, \beta_s, \ldots, \beta_{t-1}\}$, $0 \leqslant s \leqslant t = [G:H] - 1 = [F:\mathbb{Q}] - 1$ be representatives of all left cosets of H in G, excluding H, listed so that

(*a'*) for $i < s$, $\chi_{\bar{A}}(\beta_i Q_i) < \infty = \chi_{\bar{A}}(Q_i)$ for some $Q_i \in \Pi_K$; and

(*b'*) for $s \leqslant j < t$, if $Q \in \Pi_K$ and $\chi_{\bar{A}}(Q) = \infty$, then $\chi_{\bar{A}}(\beta_j Q) = \infty$.

Consequently,

(*b''*) for $s \leqslant j < t$, $\chi_{\bar{A}}(\beta_j Q) < \chi_{\bar{A}}(Q)$ for infinitely many $Q \in \Pi_K$.

For $i < s$, fix $Q_i \in \Pi_K$ satisfying (*a'*). Let $p_i \in \Pi$ be the unique rational prime in Q_i. Using (*b''*) and induction on j ($s \leqslant j < t$), choose a sequence of pairs (p_j, Q_j) such that $p_j \in Q_j$,

(*c*) $p_j \neq p_i$ for all $i < s$,

(*c'*) $\chi_{\bar{A}}(\beta_j Q_j) < \chi_{\bar{A}}(Q_j)$, and

(*c''*) if $s \leqslant j < j' < t$, then $p_j \neq p_{j'}$.

Such a choice is possible by (*b''*). The set $\Xi_0 = \{p_k : k < t\}$ is finite, and by 3.2, 3.4, (*a'*), (*b'*), and (*c'*), $\Xi_0 \subseteq c(A)$. We will prove that Ξ_0 fulfills the claims of the theorem. Let $\Xi_0 \subseteq \Xi \subseteq \Pi$. Define the characteristic χ on Π_F by $\chi(Q_k \cap F) = \infty$ for $k < t$, $\chi(P) = \infty$ if P lies

over a prime $p \in \Pi \setminus \Xi$, and $\chi(P) = 0$ for all other prime ideals P in Π_F. By 3.1, there is a subring $R \in \boldsymbol{J}(F)$ such that $\chi = \chi_R$. Then for $Q \in \Pi_K$, it follows from 3.4 that

(d) $\chi_{\bar{R}}(Q) = \infty$ if Q lies over a prime $p \in \Pi \setminus \Xi$,

(d') $\chi_{\bar{R}}(Q) = 0$ if Q lies over a prime $p \in \Xi \setminus \Xi_0$,

(d'') $\chi_{\bar{R}}(Q_k) = \infty$ for all $k < t$,

(d''') $\chi_{\bar{R}}(\beta_k Q_k) = 0$ for all $k < t$.

Indeed, (d), (d') and (d'') are clear from the definition of χ. To verify (d'''), note that if $k < t$, then $\beta_k Q_k$ lies over p_k. On the other hand, $\beta_k Q_k \cap F \neq Q_l \cap F$ for all $l < t$ by (a'), (c), (c'), and (c''). Hence, (d''') holds. It follows, from (d), (d'), (d''), (d''') and 3.2 that $c(R) = c(\bar{R}) = \Xi$. Moreover, by (d''), (d''') and 3.1, $\beta_k \notin QE(\bar{R})$ for all $k < t$. Since these automorphisms represent all left cosets of H in G except H, it follows from 4.1 and 4.3 that $QE(\bar{R}) = KH$; and $QE(R) = F$ by 4.2. Thus, $R \in \boldsymbol{E}(F)$. □

4.5. Corollary. If $A \in \boldsymbol{I}(F)$, then there exists $R \in \boldsymbol{E}(F)$ such that $c(R) = c(A)$.

4.6. Corollary. If $R \in \boldsymbol{E}(F)$ and $\Xi \supseteq c(R)$, then there exsits $S \in \boldsymbol{E}(F)$ such that $c(S) = \Xi$.

4.7. Corollary. If $R \in \boldsymbol{E}(F)$, then there is a semi-local E-ring $S \in \boldsymbol{E}(F)$ such that $c(S) \subseteq c(R)$ and $|c(S)| < [F:\mathbb{Q}]$.

Proof. Since $\Pi_F(p)$ is finite, it follows that $S \in \boldsymbol{E}(F)$ is semi-local (i.e., $\max S$ is finite) if and only if $c(S)$ is finite. The corollary therefore follows from 4.4. □

For each algebraic number field F, let $\mathfrak{C}(F)$ denote the set of all carriers of rings in the set $\boldsymbol{E}(F)$. By the remarks in Section 2, $\mathfrak{C}(F)$ consists of the carriers of E-rings R such that $\mathbb{Q}R \cong F$. Also, by 4.5, $\mathfrak{C}(F)$ can be characterized as the set of carriers of irreducible groups A such that $QE(A) \cong F$. The rest of this paper is concerned with the nature of $\mathfrak{C}(F)$.

5. Characterizing $\mathfrak{C}(F)$.

As usual, F denotes an algebraic number field. By 3.1, the rings in $\boldsymbol{J}(F)$ are of the form A_χ, where χ is a characteristic over 0_F that

takes its values in $\{0, \infty\}$. It is convenient to modify our notation. For $\Delta \subseteq \Pi_F$, denote $R_\Delta = A_\chi$, where χ is the characteristic over 0_F that is defined by $\chi(P) = 0$ if $P \in \Delta$ and $\chi(P) = \infty$ if $P \notin \Delta$. For $p \in \Pi$ and $\Delta \subseteq \Pi_F$, let

$$\Delta(p) = \Delta \cap \Pi_F(p) .$$

Since $\Pi_F(p)$ is a finite subset of Π_F, so is $\Delta(p)$. Then Lemma 3.2 takes the following form.

5.1. LEMMA. If $\Delta \subseteq \Pi_F$, then $c(R_\Delta) = \{p \in \Pi\colon \Delta(p) \neq \emptyset\}$.

As before, let K be an algebraic number field that includes F, such that K is normal over $\mathbb{Q}$. Denote

$$G = \mathrm{Gal}\,(K/\mathbb{Q}) \quad \text{and} \quad H = \mathrm{Gal}\,(K/F) .$$

For $\Delta \subseteq \Pi_F$, denote $\overline{\Delta} = \{Q \in \Pi_K\colon F \cap Q \in \Delta\}$. It follows from 3.4 that $\bar{R}_\Delta = R_{\overline{\Delta}}$. Define

$$G(\Delta) = \{\alpha \in G\colon \alpha\overline{\Delta} = \overline{\Delta}\} .$$

The result of 3.3 yields $G \cap QE(R_{\overline{\Delta}}) = G(\Delta)$. These comments and the results of Section 4 provide a characterization of the rings in $\boldsymbol{E}(F)$. Our result is a minor generalization of Theorem 2.13 in [P-V2] and of work of Butler in Section 4 of [B2].

5.2. PROPOSITION. If $\Delta \subseteq \Pi_F$, then $R_\Delta \in \boldsymbol{E}(F)$ if and only if $G(\Delta) = H$.

PROOF. Since $R_\Delta \in \boldsymbol{J}(F)$, it is a consequence of the definition of $\boldsymbol{E}(F)$ that $R_\Delta \in \boldsymbol{E}(F)$ if and only if $QE(R_\Delta) = F$. Using 4.2, it follows that $R_\Delta \in \boldsymbol{E}(F)$ is equivalent to $QE(R_{\overline{\Delta}}) = QE(\bar{R}_\Delta) = KH$ which, by 4.3, holds if and only if $G(\Delta) = G \cap QE(R_{\overline{\Delta}}) = H$. □

The computation of $G(\Delta)$ is a local matter in view of the fact that G acts transitively on the finite sets $\Pi_K(p)$. Indeed, we clearly have the following result.

5.3. LEMMA. For each $\Delta \subseteq \Pi_F$, $G(\Delta) = \bigcap_{p \in \Pi} G(\Delta(p))$.

For each prime $p \in \Pi$, the action of G on $\Pi_K(p)$ can be described in terms of the decomposition group of one of the ideals $Q \in \Pi_K(p)$. This fact enables us to translate the computation of $G(\Delta(p))$ into a group-theoretic problem. For $Q \in \Pi_K(p)$, denote the decomposition group of Q by

$$C(Q) = \{\alpha \in G\colon\ \alpha Q = Q\}\ .$$

The left cosets of $C(Q)$ are in one-to-one correspondence with the ideals in $\Pi_K(p)$ by $\alpha C(Q) \leftrightarrow \alpha Q$; and of course the action of G on the coset space is equivalent to the action of G on $\Pi_K(p)$. If $\Delta \subseteq \Pi_F$ and X_p is the union of all left cosets of $C(Q)$ corresponding to ideals in $\overline{\Delta}$, then it is easy to see that $HX_p\ C(Q) = X_p$ and $G(\Delta(p)) = G_{X_p}$, where G_{X_p} denotes $\{\alpha \in G\colon\ \alpha X_p = X_p\}$. By 5.3 and 5.2, $R_\Delta \in \boldsymbol{E}(F)$ if and only if $\bigcap_{p \in \Pi} G_{X_p} = H$. Thus, a subset Ξ of Π belongs to $\mathfrak{S}(F)$ if and only if there exist sets $X_p \subseteq G$ for each $p \in \Xi$ such that $HX_p C(Q) = X_p$ $(Q \in \Pi_k(p))$ and $\bigcap_{p \in \Xi} G_{X_p} = H$. This condition does not depend on the choices of $Q \in \Pi_K(p)$; if $\alpha \in G$, then $C(\alpha Q) = \alpha C(Q)\alpha^{-1}$, $HX_p C(Q) = X_p$ implies $HX_p\alpha^{-1}(\alpha C(Q)\,\alpha^{-1}) = X_p\alpha^{-1}$, and $G_{X_p\alpha^{-1}} = G_{X_p}$.

Henceforth, we assume that F is a normal extension of $\mathbb{Q}$ and $K = F$. In this case, $R_\Delta \in \boldsymbol{E}(F)$ if and only if $G(\Delta) = 1$, the one element subgroup of G. Moreover, $\Xi \in \mathfrak{S}(F)$ if and only if there exist sets $X_p \subseteq G$ for each $p \in \Xi$ such that $X_p C(Q) = X_p$ $(Q \in \Pi_F(p))$ and $\bigcap_{p \in \Xi} G_{X_p} = 1$. Following the terminology of [P-V2], a subgroup C of G is *abnormal* if there is a set $X \subseteq G$ such that $XC = X$ and $G_X = 1$.

Recall that the *core* of a subgroup C of a group G is defined by

$$\text{core } C = \bigcap_{\alpha \in G} \alpha C \alpha^{-1}\ .$$

Thus, the core of C is the largest normal subgroup of G that is contained in C. Moreover, core $(G/\text{core } C) = 1$.

5.4. LEMMA. Let C be a subgroup of the finite group G.

(1) If K is a cyclic, normal subgroup of G, then $K \cap C = K \cap \text{core } C$.

(2) If the set $X \subseteq G$ satisfies $XC = X$, then core $C \subseteq G_X$.

(3) If $C/\text{core } C$ is an abnormal subgroup of $G/\text{core } (C)$, then there exists $X \subseteq G$ such that $XC = X$ and $G_X = \text{core } C$.

PROOF. (1) Since K is cyclic, $K \cap C$ is a characteristic subgroup of K; hence $K \cap C \lhd G$ and $K \cap C \subseteq \text{core } C$. (2) The facts that core C is a subgroup of C and core $C \lhd G$ imply $(\text{core } C)X = X(\text{core } C) = X$. That is, core $C \subseteq G_X$. (3) Since $\bar{C} = C/\text{core } C$ is abnormal in $\bar{G} = G/\text{core } C$, there exists $\bar{X} \subseteq \bar{G}$ such that $\bar{X}\bar{C} = \bar{X}$ and $\bar{G}_{\bar{X}} = \bar{1}$. The preimage X of $\bar{X}$ in G satisfies $XC = X$ and $G_X = \text{core } C$. □

It is convenient to introduce some notation and terminology. For $p \in \Pi$, denote $K(p) = \text{core } C(P)$, where $C(P)$ is the decomposition group of any $P \in \Pi_F$ such that $p \in P$. We will say that p is of *cyclic type* if $C(P)$ is a cyclic group, and that p is *standard* if $C(P)/K(p)$ is an abnormal subgroup of $G/K(p)$. If p is not standard, then it is called *exceptional*. Since the decomposition groups of the various prime ideals over p are conjugate, this notation and terminology does not depend on the choice of P.

If the prime p is not of cyclic type, then p ramifies in F ([W], 4-10 11), so that p divides the discriminant of $F/\mathbb{Q}$ ([W], 4-8-14). In particular, almost all $p \in \Pi$ are of cyclic type.

For a prime p of cyclic type, it can be decided whether or not p is standard from the knowledge of the pair $(G/K(p), C(P)/K(p))$. Indeed, the main theorem of [P2] (and its proof) shows that if $\bar{C}$ is a cyclic subgroup of the finite group $\bar{G}$ such that core $\bar{C} = 1$, then $\bar{C}$ is not abnormal in $\bar{G}$ if and only if $(\bar{G}, \bar{C})$ has one of the following forms:

(1a) $\bar{G} \simeq S_4$, $|\bar{C}| = 4$;
(1b) $\bar{G} \simeq A_4$, $|\bar{C}| = 3$;
(1c) $\bar{G} \simeq F_{42}$, $|\bar{C}| = 6$;
(1d) $\bar{G} \simeq F_{20}$, $|\bar{C}| = 4$;
(1e) $G \simeq D_5$, $|\bar{C}| = 2$;
(1f) $\bar{G} \simeq D_3$, $|\bar{C}| = 2$;
(2) $\bar{G} \simeq D_4$, $|\bar{C}| = 2$, $\bar{C}$ not contained in the center of $\bar{G}$.

In all of the cases (1a)-(1f), the group $\bar{C}$ is determined up to conjugation by its order and the assumption that it is cyclic. In case (2), there are two conjugate classes of non-central cyclic subgroups of order two, but they are equivalent under an automorphism of $\bar{G}$.

If C is a cyclic subgroup of the finite group G, we will say that the pair (G, C) is of class 1 (or more specifically 1a, 1b, 1c, 1d, 1e, 1f) if $(G/\text{core } C, C/\text{core } C)$ has the corresponding form listed above, and

(G, C) is of class (2) if (G/core C, C/core C) has the form (2) above. If (G/core C, C/core C) has none of these forms, then (G, C) will be assigned the designation of class 0. A finite group G will be said to belong to the class 0, 1 (more precisely 1a, 1b, 1c, 1d, 1e, 1f), or 2 if there is a cyclic subgroup C of G such that (G, C) is in the corresponding class. As we will see, this classification is unambiguous.

5.5. THEOREM. Let F be an algebraic number field that is normal over $\mathbf{Q}$. Denote $G = \mathrm{Gal}(F/\mathbf{Q})$. Assume that $\Xi \subseteq \Pi$, the set of all rational primes. If there is an E-ring R such that $\mathbf{Q}R \cong F$ and $c(R) = \Xi$, then

$$(*) \qquad \bigcap_{p \in \Xi} K(p) = 1 .$$

Conversely, if $(*)$ is satisfied, together with any one of the following conditions (a), (b), or (c), then there is an E-ring R such that $0_F \subseteq R$, $\mathbf{Q}R = F$, and $c(R) = \Xi$.

- (a) G is of class 0, and Ξ includes at least one prime of cyclic type.
- (b) G is of class 1, and Ξ includes at least two primes of cyclic type.
- (c) G is of class 2, and Ξ includes at least three primes of cyclic type.

PROOF. Assume that there is an E-ring R satisfying $\mathbf{Q}R \cong F$ and $c(R) = \Xi$. It can be assumed that $R \in \boldsymbol{E}(F)$ since these properties hold for rings in the quasi-equality class of R. Thus, $R = R_\Delta$ for some $\Delta \subseteq \Pi_F$, where $G(\Delta) = 1$ by 5.2. Since $G(\Delta) = \bigcap_{p \in \Pi} G(\Delta(p)) = \bigcap_{p \in \Xi} G(\Delta(p))$ by 5.3, the equation $(*)$ follows from the fact that $K(p) \subseteq G(\Delta(p))$. Most of the remainder of this section is devoted to the proof of the converse statement. Therefore, suppose that $(*)$ holds. Let $p_0 \in \Xi$ be a standard prime of cyclic type. Thus, if $P \in \Pi_F(p_0)$, then $C(P)/K(p_0)$ is an abnormal subgroup of $G/K(p_0)$. By 5.4 (3), there is a non-empty subset X of G such that $XC(P) = X$ and $G_X = K(p_0)$. Thus, by the correspondence that was described after 5.3, there exists $\Delta(p_0) \subseteq \Pi_F(p_0)$ such that $\Delta(p_0) \neq \emptyset$ and $G(\Delta(p_0)) = K(p_0)$. For each $q \in \Xi \setminus \{p_0\}$, choose $Q_q \in \Pi_F(q)$ and define

$$\Delta = \Delta(p_0) \cup \{Q_q : q \in \Xi \setminus \{p_0\}\} .$$

By 5.1, $C(R_\Delta) = \Xi$. Moreover,

$$G(\Delta) = G(\Delta(p_0)) \cap \bigcap_{q \in \Xi \setminus \{p_0\}} C(Q_q) = \bigcap_{q \in \Xi \setminus \{p_0\}} K(p_0) \cap C(Q_q) =$$

$$= \bigcap_{q \in \Xi \setminus \{p_0\}} K(p_0) \cap \operatorname{core} C(Q_q) = \bigcap_{p \in \Xi} K(p) = 1$$

by 5.4 (1) and (*). By 5.2, R_Δ is an E-ring such that $0_F \subseteq R_\Delta$.

If G is in class 0, then every prime of cyclic type is standard. Thus (a) and (*) imply the existence of the required E-ring R. Moreover, for the rest of the proof, we can assume that either: G is in class 1 and p_1, p_2 are distinct, exceptional cyclic primes in Ξ; or G is of class 2 and p_1, p_2, p_3 are distinct, exceptional cyclic primes in Ξ.

5.6. LEMMA. If (G, C) is in the class 1, then core C is the center of G.

PROOF. Let H be the centralizer of core C in G. Since core C is a normal subgroup of G and C is cyclic, it follows that $C \subseteq H \lhd G$. Denote $\bar{G} = G/\operatorname{core} C$, $\bar{H} = H/\operatorname{core} C$, and $\bar{C} = C/\operatorname{core} C$. Then $\bar{C} \subseteq \bar{H} \lhd \bar{G}$. An examination of the forms (1a)-(1f) of $(\bar{G}, \bar{C})$ shows that $\bar{C}$ is not contained in a proper, normal subgroup of $\bar{G}$. Thus, $\bar{H} = \bar{G}$ and core C is contained in the center of G. In fact, core G is equal to the center of G because of all the groups $\bar{G}$ in (1a)-(1f) have trivial centers. □

At this point, we digress from the proof of 5.5 in order to exhibit an important consequence of 5.6.

5.7. PROPOSITION. Each finite group is a member of exactly one of the classes 0, 1a, 1b, 1c, 1d, 1e, 1f, or 2.

PROOF. By definition, every finite group G is in class 1 or 2, or in class 0 with no overlap. If G is in class 1, then there is a cyclic subgroup C of G such that (G, C) is of class 1. By 5.6, core C is the center Z of G, so that $G/Z \cong S_4$, A_4, F_{42}, F_{20}, D_5, or D_3. In particular, G is not in two different classes of type 1. If G also belongs to class 2, then there is a cyclic subgroup C' of G such that $G/\operatorname{core} C' \cong D_4$ by an isomorphism that carries $C'/\operatorname{core} C'$ to a non-central cyclic group of order 2. Since none of the groups S_4, A_4, F_{42}, F_{20}, D_5 or D_3 is a homomorphic image of D_4, it follows that core $C' \not\subseteq Z$. Thus, by 5.4 (1), $Z \cap C' = Z \cap \operatorname{core} C' \subset \operatorname{core} C' \subset C'$. In this case, ZC'/Z is a

cyclic subgroup of G/Z that properly contains the non-trivial, normal subgroup Z core C'/Z. However, none of the groups S_4, A_4, F_{42}, F_{20}, D_5 and D_3 contains such a chain of cyclic subgroups. Thus, the classes 1 and 2 are disjoint. □

To complete the proof of 5.5, another lemma is needed.

5.8. LEMMA. Let G be a group of class 2. Assume that for $1 \leqslant i \leqslant 3$, C_i is a cyclic subgroup of G such that the pair (G/core C_i, C_i/core C_i) is of class 2. Then core C_i = core C_j for some $i \neq j$.

PROOF. Assume that core C_1, core C_2, and core C_3 are distinct. Then core $C_i \not\subseteq$ core C_j for $i \neq j$ because $|G/\text{core } C_i| = |G/\text{core } C_j|$. By 5.4 (1),

$$C_2 \cap \text{core } C_1 = \text{core } C_2 \cap \text{core } C_1 \subset \text{core } C_2 \subset C_2 .$$

Thus,

$$1 \subset (\text{core } C_2)(\text{core } C_1)/\text{core } C_1 \subset C_2(\text{core } C_1)/\text{core } C_1 ,$$

so that C_2(core C_1)/core C_1 is a cyclic group of order 4. Since the cyclic group of order 4 in D_4 is unique, it follows by symmetry that C_2(core C_1) = C_3(core C_1). Moreover,

$$[C_2\colon \text{core } C_2] = [\text{core } C_2\colon (\text{core } C_2) \cap (\text{core } C_1)] =$$

$$= [\text{core } C_1\colon (\text{core } C_1) \cap (\text{core } C_2)] = 2 .$$

Therefore,

$$\big(C_2(\text{core } C_1)\big)^2 = C_2^2(\text{core } C_1)^2 = (\text{core } C_2)\big((\text{core } C_1) \cap (\text{core } C_2)\big) = \text{core } C_2 ,$$

and

$$\text{core } C_2 = \big(C_2(\text{core } C_1)\big)^2 = \big(C_3(\text{core } C_1)\big)^2 = \text{core } C_3 ,$$

contrary to our hypothesis. □

We can now finish the proof of 5.5. For the remaining cases, it can be assumed by 5.6 and 5.8 that p_1 and p_2 are distinct, exceptional, cyclic primes such that $K(p_1) = K(p_2)$. For all of the pairs

$(\bar{G}, \bar{C})$ in the list (1*a*)-(1*f*) and (2), none of the cyclic groups $\bar{C}$ is normal, and the various conjugates of these groups either coincide with $\bar{C}$ or meet $\bar{C}$ trivially. Thus, it is possible to choose $P_1 \in \Pi_F(p_1)$ and $P_2 \in \Pi_F(p_2)$ such that $C(P_1) \cap C(P_2) = K(p_1) = K(p_2)$. For each $q \in \Xi$, let $\Delta(q) = \{Q_q\}$ with $Q_q = P_1$ if $q = p_1$, $Q_q = P_2$ if $q = p_2$, and otherwise $Q_q \in \Pi_F(q)$ can be chosen arbitrarily. Let $\Delta = \bigcup_{q \in \Xi} \Delta(q)$. Then $C(R_\Delta) = \Xi$ by 5.1. Moreover,

$$G(\Delta) = \bigcap_{q \in \Xi} G(\Delta(q)) = \bigcap_{q \in \Xi} C(Q_q) = C(P_1) \cap C(P_2) \cap \bigcap_{q \in \Xi \setminus \{p_1, p_2\}} C(Q_q) =$$

$$= K(p_1) \cap K(p_2) \cap \bigcap_{q \in \Xi \setminus \{p_1, p_2\}} C(Q_q) = \bigcap_{q \in \Xi} K(q) = 1$$

by 5.3, 5.4 (1), and (*). It follows from 5.4 that $R_\Delta \in \boldsymbol{E}(F)$, that is, R_Δ is an E-ring with $0_F \subseteq R_\Delta$. □

5.9. Corollary. Let m be the number of prime divisors of the discriminant of the normal extension $F/\mathbb{Q}$. Assume that $\mathrm{Gal}(F/\mathbb{Q})$ belongs to the class i $(0 \leqslant i \leqslant 2)$. If $\Xi \subseteq \Pi$ satisfies $|\Xi| > m + i$, then $\Xi \in \mathfrak{C}(F)$ if and only if $\bigcap_{p \in \Xi} K(p) = 1$.

Indeed, $|\Xi| > m + i$ implies Ξ includes at least $i + 1$ primes of cyclic type. Note that if Ξ is infinite, then 5.9 applies to any normal extension $F/\mathbb{Q}$.

5.10. Corollary. Let F be an algebraic number field such that $F/\mathbb{Q}$ is a cyclic extension of prime power degree. If $\Xi \subseteq \Pi$, then $\Xi \in \mathfrak{C}(F)$ if and only if Ξ includes a prime that splits completely in F.

Proof. Since $G = \mathrm{Gal}(F/\mathbb{Q})$ is cyclic of prime power order, every $p \in \Pi$ is of cyclic type, G is in the class 0, and the lattice of subgroups of G is a chain. Thus, $\Xi \in \mathfrak{C}(F)$ if and only if $K(p) = 1$ for some $p \in \Xi$. Since G is abelian, $K(p) = C(P)$ for an arbitrary $P \in \Pi_F(p)$; and $C(P) = 1$ if and only if p splits completely in F. □

The results of class field theory give a fairly satisfactory characterization of the primes that split completely is an abelian extension of $\mathbb{Q}$. (See [N], p. 135.) Thus, 5.10 provides an effective characterization of $\mathfrak{C}(F)$ for quadratic extensions of F. For example, if $F = \mathbb{Q}(i)$, then $\mathfrak{C}(F)$ consists of all sets Ξ that include an odd prime p such that $p \equiv 1 \pmod 4$.

5.11. COROLLARY. Let $k \in \mathbb{N}$. There is a cyclic extension $F/\mathbb{Q}$ and a set $\Xi \subseteq \Pi$ with $|\Xi| = k$ such that $\Xi \in \mathfrak{C}(F)$, but no proper subset of Ξ is in $\mathfrak{C}(F)$.

PROOF. Let $q_1, q_2, \ldots, q_k$ be distinct primes, $n = q_1 q_2 \ldots q_k$, and $H = \mathbb{Z}/n\mathbb{Z}$. Note that $\bigcap_{i=1}^{k} q_i H = 0$, and for $1 \leqslant j \leqslant k$, $\bigcap_{i \neq j} q_i H \neq 0$. Let $F/\mathbb{Q}$ be a normal extension with $G = \mathrm{Gal}(F/\mathbb{Q}) \cong H$. By the Tchebotarev density theorem ([N], Theorem 6.4), there exist primes $p_i \in \Pi$ such that $C(P_i) = q_i H$ (where $P_i \in \Pi_F(p_i)$). The set $\Xi = \{p_1, p_2, \ldots, p_k\}$ satisfies $|\Xi| = k$, $\bigcap_{p \in \Xi} K(p) = 1$, and for a proper subset Ξ' of Ξ, $\bigcap_{p \in \Xi'} K(p) \neq 1$. Since G is cyclic, it is of class zero and every $p \in \Pi$ is of cyclic type. It follows from 5.5 that $\Xi \in \mathfrak{C}(F)$ and $\Xi' \notin \mathfrak{C}(F)$ for all $\Xi' \subset \Xi$. □

Acknowledgement. Part of the research that is reported in this paper was done while the first author was visiting the University of Padova. Sincere thanks are given to the members of the Mathematics Department in Padova, particularly Adalberto Orsatti and Luigi Salce, for their generous hospitality.

REFERENCES

[A] D. M. ARNOLD, *Finite rank torsion free abelian groups and rings*, Lecture Notes in Mathematics, **931**, Springer-Verlag, Berlin, Heidelberg, New York, 1982.

[A-M] M. F. ATIYAH - I. G. MACDONALD, *Introduction to Commutative Algebra*, Addison-Wesley, Reading, 1969.

[A-P-R-V-W] D. M. ARNOLD - R. S. PIERCE - J. D. REID - C. I. VINSONHALER - W. J. WICKLESS, *Torsion free abelian groups of finite rank projective as modules over their endomorphism rings*, Jour. Alg., **71** (1981), pp. 1-10.

[B1] M. C. R. BUTLER, *On locally free torsion-free rings of finite rank*, J. Lond. Math. Soc., **43** (1968), pp. 297-300.

[B2] M. C. R. BUTLER, *A Galois-theoretic description of certain quasi-endomorphism rings*, Symposia Mathematica, **13** (1974), pp. 143-151.

[B-S] R. A. BOWSHELL - P. SCHULTZ, *Unital rings whose additive endomorphisms commute*, Math. Ann., **228** (1977), pp. 197-214.

[C] A. L. S. CORNER, *Every countable reduced torsion-free ring is an endomorphism ring*, Proc. Lond. Math. Soc., (3), **13** (1963), pp. 687-710.

[D-V-M] M. DUGAS - A. MADER - C. I. VINSONHALER, *Large E-rings exist*, J. Algebra, **108** (1987), pp. 88-101.

[J] N. JACOBSON, *Lectures in Abstract Algebra*, vol. III, Von Nostrand, Princeton, 1964.

[K] G. KOLETTIS Jr., *Homogeneously decomposable modules*, Studies on Abelian Groups, Paris (1968), pp. 223-238.

[M-V] A. MADER - C. I. VINSONHALER, *Torsion-free E-modules*, J. Alg., **115** (1988), pp. 401-411.

[N] J. NEUKIRCH, *Class Field Theory*, Springer-Verlag, Berlin, Heidelberg, New York, Tokyo, 1980.

[P1] R. S. PIERCE, *Subrings of simple algebras*, Mich. Math. J., **7** (1960), pp. 241-243.

[P2] R. S. PIERCE, *Permutation representations with trivial set stabilizers*, J. Alg., **95** (1985), pp. 88-95.

[P-V1] R. S. PIERCE - C. I. VINSONHALER, *Realizing central division algebras*, Pac. J. Math., **109** (1983), pp. 165-177; correction, **130** (1987), pp. 397-399.

[P-V2] R. S. PIERCE - C. I. VINSONHALER, *Realizing algebraic number fields*, Lecture Notes in Mathematics, **1006**, Springer-Verlag, New York (1982/83), pp. 49-96.

[P-V3] R. S. PIERCE - C. I. VINSONHALER, *Classifying E-rings* (manuscript).

[Re] J. D. REID, *On the ring of quasi-endomorphisms of a torsion-free group* Topics in Abelian Groups, Chicago (1963), pp. 51-68.

[Ri] P. RIBENBOIM, *Modules sur un anneau de Dedekind*, Summa Brasil Math., **3** (1952), pp. 21-36.

[S] P. SCHULTZ, *The endomorphism ring of the additive group of a ring*, J. Aust. Math. Soc., **15** (1973), pp. 60-69.

[W] E. WEISS, *Algebraic Number Theory*, McGraw-Hill, New York, 1963.

[Z] H. ZASSENHAUS, *Orders as endomorphism rings of modules of the same rank*, J. Lond. Math. Soc., **42** (1967), pp. 180-182.

Manoscritto pervenuto in redazione il 4 gennaio 1990.