TORSION-FREE RINGS

BY

R. A. Beaumont and R. S. Pierce[1]

1. Introduction

In the following we are concerned with associative rings which have a torsion-free abelian group as additive group. Such rings are called *torsion-free rings*. The rank of a torsion-free ring is the rank of its additive group, which is the cardinality of a maximal independent set of elements.

The tensor product $R \otimes A$ [6], where R is the field of rational numbers and A is a torsion-free ring, can be made into an associative algebra over R by defining $r(s \otimes a) = rs \otimes a$ for $r, s \in R$, $a \in A$. We will denote $R \otimes A$ by A^*. It can be readily verified that A^* has the following properties:

(1) Every element of A^* can be written in the form $r \otimes a$, $r \in R$, $a \in A$.

(2) A is imbedded as a subring in A^*. Since A is torsion-free, the mapping $a \to 1 \otimes a$ is an imbedding [6, p. 130].

(3) For every $\bar{a} \in A^*$, there exists an integer $n \geqq 1$ such that $n\bar{a} \in A$. This follows from (1) and (2).

(4) The dimension of A^* over R is equal to the rank of A.

(5) A^* is a unique smallest associative algebra over R containing A as a subring.

Because of (1), we simplify the notation by writing ra instead of $r \otimes a$ for the elements of A^*. It should be noted that as an additive group A^* is just the minimal divisible torsion-free group containing A [9, p. 66], and that when A^* is regarded as the set of formal products ra, $r \in R$, $a \in A$, certain identifications which we make in the sequel are clear. We introduce the following terminology.

Definition 1.1. *The algebra $A^* = R \otimes A$ is called the algebra type of the ring A, and torsion-free rings A_1 and A_2 are said to have the same algebra type if their algebra types A_1^* and A_2^* are isomorphic algebras.*

Definition 1.2. *Let G be a torsion-free abelian group, and let T be an associative algebra over R. Then G admits a multiplication of algebra type T if there exists a ring A with additive group A^+ isomorphic to G such that A^* and T are isomorphic algebras.*

Received November 23, 1959.

[1] The second author was supported by the National Science Foundation while working on this paper.

We pose the following problems:

I. Find all torsion-free rings with a given algebra type T.

II. Find all torsion-free groups which admit multiplication of a given algebra type T.

Section 2 is concerned with the elementary properties of quasi-isomorphism of groups and rings.

DEFINITION 1.3. *Let A and B be abelian groups (rings). Then A and B are quasi-isomorphic if there exist subgroups (subrings) $A' \subseteq A$ and $B' \subseteq B$ such that*

(i) *A' and B' are isomorphic groups (rings);*

(ii) *there are integers $m \geqq 1$ and $n \geqq 1$ such that $mA \subseteq A'$ and $nB \subseteq B'$.*

We write $A \sim B$ if A and B are quasi-isomorphic as groups and $A \approx B$ if A and B are quasi-isomorphic as rings.

It is shown that quasi-isomorphic rings have the same algebra type (Theorem 2.5) and that quasi-isomorphic groups admit multiplication of the same type (Corollary 2.7). The concept of quasi-isomorphism is basic for the remainder of the paper.

In Sections 3 and 4 the structure theorems of Wedderburn are generalized to torsion-free rings of finite rank. These classical theorems extend to torsion-free rings, provided isomorphisms are weakened to quasi-isomorphisms. The main result is a generalization of the Wedderburn principal theorem.

THEOREM 1.4. *Let A be a torsion-free ring of finite rank. Let $A^* = \bar{S} \oplus \bar{N}$, where $\bar{N}$ is the radical of A^* and $\bar{S}$ is a semisimple subring of A^*, and let $S = \bar{S} \cap A$, $N = \bar{N} \cap A$. Then S is a subring of A such that $S^* = \bar{S}$, N is the maximum nilpotent ideal of A, $N^* = \bar{N}$, and $S \oplus N$ is a subring of A such that $S \oplus N$ has finite index in A.*

A by-product of Section 4 (Corollary 4.9) is the fact that any torsion-free group of finite rank which admits a multiplication of semisimple algebra type is an extension of a free group by a divisible torsion group. This motivates the following definitions.

DEFINITION 1.5. *Let A be a torsion-free group. A subgroup B of A is called a full subgroup of A if A/B is a torsion group.*

DEFINITION 1.6. *Let A be a torsion-free group. Then A is called a quotient-divisible or q.d. group if A contains a full subgroup B such that B is free and A/B is a direct sum of a divisible group and a group of bounded order. A torsion-free ring A is called a q.d. ring if the additive group of A is a q.d. group.*

In Section 5, q.d. groups are analyzed, and a reasonably simple system of invariants is obtained for the quasi-isomorphism classes of q.d. groups of finite rank. These invariants are patterned after those of Kurosh, Malcev, and Derry for the isomorphism classes of arbitrary torsion-free groups of finite rank, and are based on the following considerations.

Since any torsion-free group A of finite rank is a full subgroup of the finite-dimensional vector space $R \otimes A$, we restrict our attention to full subgroups of a fixed rational vector space V of finite dimension. Denote by $Z^{(p)}$ and $R^{(p)}$ the p-adic completions of the rings of integers and rationals respectively. For every rational prime p, form the $R^{(p)}$-space $V^{(p)} = V \otimes R^{(p)}$, and regard $V^{(p)}$ as an extension of V. Now for a subgroup A of V, we consider the $Z^{(p)}$-module,

$$A^{(p)} = Z^{(p)}A = \left\{\sum z_i x_i \mid z_i \in Z^{(p)}, x_i \in A\right\},$$

and denote by $\delta_p(A)$, the maximal divisible subgroup of $A^{(p)}$. Then $\delta_p(A)$ is the maximal divisible submodule of $A^{(p)}$ regarded as a $Z^{(p)}$-module, and hence is an $R^{(p)}$-subspace of $V^{(p)}$.

Following Jónsson [11], we introduce an equivalence relation on the subgroups of V.

DEFINITION 1.7. *If A and B are subgroups of the R-space V, define $A \dot{\subseteq} B$ if $nA \subseteq A \cap B$ for some $n \geqq 1$. Define $A \doteq B$ if $A \dot{\subseteq} B$ and $B \dot{\subseteq} A$.*

It is clear that the equivalence $\doteq$ is a refinement of quasi-isomorphism, so that $A \doteq B$ implies $A \sim B$.

DEFINITION 1.8. *For each prime p, let $\mathfrak{L}_p$ be the lattice of subspaces of the $R^{(p)}$-space $V^{(p)}$. Let $\mathfrak{L} = \prod_p \mathfrak{L}_p$ be the direct product of these lattices. For any $\delta \in \mathfrak{L}$, denote by δ_p the p^{th} component of δ. The elements of $\mathfrak{L}$ are called the q.d. invariants associated with V. If A is a subgroup of V, define $\delta(A) \in \mathfrak{L}$ by the condition that the p^{th} component of $\delta(A)$ is $\delta_p(A)$. We call $\delta(A)$ the q.d. invariant of A.*

We are now able to state the main result of Section 5.

THEOREM 1.9. *Let A and B be full q.d. subgroups of V.*

(1) *$A \doteq B$ if and only if $\delta(A) = \delta(B)$;*

(2) *if $\delta \in \mathfrak{L}$, then there exists a full q.d. subgroup A of V such that $\delta = \delta(A)$;*

(3) *$A \sim B$ if and only if there is a nonsingular linear transformation ϕ of V such that $(\phi \otimes \mathrm{id}_{R^{(p)}})\, \delta_p(A) = \delta_p(B)$ for all p.*

In Section 6, the q.d. invariants are used to reduce the study of torsion-free rings of simple algebra type to rings of field type. These results are based on the correspondence given in the following theorem.

THEOREM 1.10. *Let T be a rational algebra of finite order, and let A be a full subring of T. Then for each prime p, $\delta_p(A)$ is a two-sided ideal of the $R^{(p)}$-algebra $T^{(p)} = T \otimes R^{(p)}$. Conversely, if δ is a q.d. invariant such that each δ_p is a two-sided ideal of $T^{(p)}$, then there is a full q.d. subring A of T such that $\delta = \delta(A)$. If A and B are full q.d. subrings of T, then $A \approx B$ if and only if there is an automorphism ϕ of T such that $(\phi \otimes \mathrm{id}_{R^{(p)}})\, \delta_p(A) = \delta_p(B)$ for all p.*

It is convenient to state the principal applications of this result in terms of the notation introduced in the following definition.

DEFINITION 1.11. *Let T be a rational algebra of finite order with an identity, and let K be a subfield of the center of T which contains the identity. If C is a subring of K and $X = \{x_1, \cdots, x_r\}$ is a basis of T relative to K such that*

$$x_i x_j = \sum_k a_{ijk} x_k \quad \textit{with} \quad a_{ijk} \in C,$$

we call X a C-basis of T over K. If C is a full subring of K, denote by $C[X]$ the subring of T consisting of all elements of the form $c_1 x_1 + \cdots + c_r x_r$ with $c_i \in C$, where $X = \{x_1, \cdots, x_r\}$ is any C-basis of T over K.

THEOREM 1.12. *Let T be a simple rational algebra of finite order with center F. Let A be a full subring of T, and let $C = A \cap F$. Then C is the center of A and if X is a C-basis of T over F with $X \subseteq A$, the subring $C[X]$ has finite index in A.*

THEOREM 1.13. *Let T be a simple rational algebra of finite order with center F. Suppose T is r-dimensional over F. Then a torsion-free group A admits a multiplication of algebra type T if and only if A is quasi-isomorphic to a direct sum $\sum \oplus_{i=1}^{r} C_i$, where $C_i \cong C$ for all i and C admits a multiplication of algebra type F.*

In Section 7, the automorphisms of rings of field type are considered. In Section 8 some examples of rings of field type are constructed. In particular, the groups which admit multiplication of quadratic field type are characterized. Section 9 is in the form of an appendix. It is shown here that under very special conditions, quasi-isomorphisms can be replaced by isomorphisms. These conditions are satisfied, however, by rings of certain algebra types.

Notation. By a group we always mean an abelian group. Generally, A, B, C, and D stand for torsion-free groups or rings. The rings of integers and rationals are denoted by Z and R respectively; the p-adic completions of these rings are represented by $Z^{(p)}$ and $R^{(p)}$ (a slight departure from standard notation). If G is a group and H a subgroup, the factor group of G by H is G/H. The standard isomorphism theorems will be used repeatedly and without mention. Certain notation of the theory of abelian groups will be convenient. If G is a group, then: $d(G)$ is the maximal divisible subgroup of G; $G[m]$ is the m-layer of G, that is, $\{x \in G \mid mx = 0\}$; $G_p = \bigcup_{k=1}^{\infty} G[p^k]$ is the p-primary component of G; $d_p(G) = (d(G))_p$; rk G is the rank of G as a Z-module. If M is a $Z^{(p)}$-module, its $Z^{(p)}$-rank is denoted $\mathrm{rk}_{Z^{(p)}} M$. Similarly dim V is the R-dimension of the rational space V and $\dim_{R^{(p)}} V$ is the dimension over $R^{(p)}$ when V is an $R^{(p)}$-space. Isomorphisms, either in the ring or group sense, are symbolized by $\cong$. The distinction between ring and group isomorphisms will either be clear from context or will be explicitly noted. We will distinguish between group direct sums and ring direct sums by use of the symbols

$\oplus$ and $\dot{+}$ respectively. For addition and multiplication of complexes in a group the usual $+$ and juxtaposition notation is used. The symbol $\otimes$ stands for tensor product which in all applications will be taken over the ring of integers. We use A^+ to denote the additive group of the ring A, when this distinction has to be made explicit. The symbols of set theory $\subseteq$, $\subset$, $\supseteq$, $\supset$, $\cap$, $\cup$, $\{\cdot|\cdot\}$ and of number theory $m \mid n$, (m, n), mod n, etc., have their usual meanings.

We wish to extend our thanks to our algebraic colleagues at the University of Washington and elsewhere for valuable suggestions and for the encouragement derived from their interest. Particular thanks are due to Professor J. P. Jans whose ideas and suggestions guided and improved our work in many places.

2. Quasi-isomorphism of groups and rings

In this section we study the relations introduced in Definition 1.3. It is shown that quasi-isomorphic rings have the same algebra type and that quasi-isomorphic groups admit multiplication of the same type.

LEMMA 2.1. *The relations $\sim$ and $\approx$ are equivalences.*

Proof. These relations are clearly symmetric and reflexive. Let $A' \subseteq A$, $B' \subseteq B, B'' \subseteq B, C' \subseteq C, A' \cong B', B'' \cong C', nA \subseteq A', mB \subseteq B', n'B' \subseteq B''$, $m'C \subseteq C'$. Suppose $\phi: A' \to B'$, $\psi: B'' \to C'$ are the given isomorphisms. Let

$$A'' = \phi^{-1}(B' \cap B''), \qquad C'' = \psi(B' \cap B'').$$

Then A'' and C'' are subgroups (subrings) of A and C respectively. Also $\psi\phi$ maps A'' isomorphically on C''. Finally (as groups)

$$A'/A'' \cong B'/(B' \cap B'') \cong (B' + B'')/B'' \subseteq B/B'',$$

so $n'A' \subseteq A''$ and $n'nA \subseteq n'A' \subseteq A''$. Similarly, $m'mC \subseteq C''$.

It is evident that if A and B are rings such that $A \approx B$, then as groups, $A \sim B$.

The following lemma is an easy consequence of Definition 1.3.

LEMMA 2.2 *If $A \sim B$ and $C \sim D$, then $A \oplus C \sim B \oplus D$. If $A \approx B$ and $C \approx D$, then $A \dot{+} C \approx B \dot{+} D$.*

We now specialize our considerations to torsion-free groups. Henceforth, A, B, C, and D are torsion-free abelian groups or torsion-free rings.

LEMMA 2.3. *The following conditions are equivalent for torsion-free groups:*

(i) *there exist subgroups $A' \subseteq A$ and $B' \subseteq B$ and an integer $n \geqq 1$ such that $A \cong B'$, $B \cong A'$, $nA \subseteq A'$, and $nB \subseteq B'$;*

(ii) *there exist a subgroup $A' \subseteq A$ and an integer $n \geqq 1$ such that $A' \cong B$ and $nA \subseteq A'$;*

(iii) $A \sim B$.

Proof. It is clear that (i) implies (ii), and we see that (ii) implies (iii) by choosing $B' = B$. To show (iii) implies (i), let $A' \subseteq A$, $B' \subseteq B$ be subgroups, λ an isomorphism of A' onto B', and $m \geqq 1$, $n \geqq 1$ integers such that $mA \subseteq A'$, $nB \subseteq B'$. Then $\phi: a \to ma \to \lambda(ma)$ is an isomorphism of A into B', and $\psi: b \to nb \to \lambda^{-1}(nb)$ is an isomorphism of B into A'. Moreover, $mnB \subseteq mB' = m\lambda(A') = \lambda(mA') \subseteq \lambda(mA) = \phi(A)$. Similarly, $mnA \subseteq \psi(B)$.

The analogous properties (i), (ii), and (iii) for torsion-free rings are not equivalent. Evidently (i) implies (ii), and (ii) implies (iii). However, the ring Z of integers is quasi-isomorphic to the ring $2Z$ of even integers, but clearly Z is not isomorphic to any subring of $2Z$.

LEMMA 2.4. *Let A and B be torsion-free groups (rings), and let ϕ be a homomorphism of A into B. Then ϕ has a unique extension ϕ^* to a linear mapping (algebra homomorphism) of A^* into B^* considered as R-spaces (R-algebras). If ϕ is one-to-one, then so is ϕ^*. If $\phi(A)$ is a full subgroup (see Definition 1.5) of B, then ϕ^* is onto. Finally, if $\psi: B \to C$ is another homomorphism, then $(\psi\phi)^* = \psi^*\phi^*$.*

Proof. If $x \in A^*$, then there exist $a \in A$ and $r \in R$ such that $x = ra$. Define $\phi^*(x) = r\phi(a)$. A routine check shows that ϕ^* is well defined and has the stated properties.

Remark. Two consequences of 2.4 are worth noting. First, if ϕ maps A onto B, then $\phi(A) = B$ is full in B, so that ϕ^* maps A^* onto B^*. Second, if $A \sim B$, then $\operatorname{rk} A = \operatorname{rk} B = \dim A^* = \dim B^*$. These facts will be used in Section 5.

The motive for introducing the concepts of quasi-isomorphism for torsion-free groups and rings is provided by the next two theorems.

THEOREM 2.5. *If $A \approx B$, then A and B have the same algebra type.*

Proof. Let $mA \subseteq A' \subseteq A$, $nB \subseteq B' \subseteq B$, where A' and B' are isomorphic, $m \geqq 1$ and $n \geqq 1$. Then

$$A \otimes R \supseteq A' \otimes R \supseteq (mA) \otimes R = A \otimes R,$$

so $(A')^* = A^*$. Similarly $(B')^* = B^*$. By 2.4, $(A')^* \cong (B')^*$, that is, A and B have the same algebra type.

THEOREM 2.6. *Let $A \sim B$, and let A be a ring. Then there exists a ring multiplication on B such that B is isomorphic to a subring A' of A and $mA \subseteq A'$ for some $m \geqq 1$.*

Proof. By 2.3 there are an isomorphism $\phi: B \to A$ and an integer $n \geqq 1$ such that $nA \subseteq \phi(B)$. Define the multiplication in B by

$$x \cdot y = \phi^{-1}(n[\phi(x) \cdot \phi(y)]), \qquad x, y \in B,$$

where $\cdot$ denotes the multiplication in A. The mapping $\lambda: B \to A$ defined by $\lambda(x) = n\phi(x)$ is then a ring isomorphism, and since $\lambda(B) = n\phi(B)$, we have $n^2 A \subseteq n\phi(B) = \lambda(B)$.

COROLLARY 2.7. *If A admits a multiplication of algebra type T and $A \sim B$, then B admits a multiplication of algebra type T.*

Proof. By Theorem 2.6, B admits a multiplication such that $B \approx A$ and consequently, by 2.5, of algebra type T.

This corollary shows that the problem of determining the groups which admit multiplication of given algebra type T can be separated into the problem of finding representatives of the quasi-isomorphism classes of groups admitting multiplication of type T and the problem of finding all groups which are quasi-isomorphic to a given group. When the quasi-isomorphism classes are studied rather than the isomorphism classes, many of the subtle difficulties connected with torsion-free groups disappear. The results of Jónsson [11] on the decomposition arithmetic of groups of finite rank is evidence of this fact.[2] If A is a torsion-free group of finite rank, then it is clear that $A \sim B_1 \oplus \cdots \oplus B_n$, where the B_i are "strongly indecomposable" torsion-free groups, that is, if $B_i \sim C \oplus D$, where C and D are torsion-free, then $C = 0$ or $D = 0$. Jónsson shows that this decomposition is unique. Although we will not make essential use of Jónsson's theorem, it is an important foundation for our work, since it adds stature to the decomposition theorems of Sections 3 to 6 below.

3. Reduction theorems

In this section we will use the classical reduction theorems for rational algebras to reduce the question of classifying groups which admit multiplication of certain algebra types T to that of classifying groups which admit multiplication of more special types.

LEMMA 3.1. *Let A be a torsion-free ring such that*

$$A^* = \bar{A}_1 \oplus \bar{A}_2 \oplus \cdots \oplus \bar{A}_m$$

is a vector space decomposition, where $\bar{A}_i$, $i = 1, 2, \cdots, m$, are subrings of A^*. Then the $A_i = \bar{A}_i \cap A$ are independent subrings of A, and

(i) $A_i^* = \bar{A}_i$ *(making the usual identifications);*

(ii) *$A/(A_1 \oplus A_2 \oplus \cdots \oplus A_m)$ is a torsion group. If A^* contains elements e_i, $i = 1, 2, \cdots, m$, such that e_i acts as a right (left) identity on $\bar{A}_i$ and as a right (left) annihilator on $\bar{A}_j$, $j \neq i$, then $A/(A_1 \oplus A_2 \oplus \cdots \oplus A_m)$ has bounded order.*

Proof. It is clear that the A_i are independent subrings of A. Also $A_i \subseteq \bar{A}_i$, and for $\bar{a}_i \in \bar{A}_i$, $i = 1, 2, \cdots, m$, there exists an integer $n \geqq 1$

[2] We are grateful to Professor Jónsson for pointing out his results and for sending us a preliminary version of the manuscript of [11].

such that $n\bar{a}_i \in A_i$. Thus $\bar{A}_i$ is isomorphic to a subalgebra of A_i^*, and since A_i^* is a minimal subalgebra containing A_i, $\bar{A}_i = A_i^*$, proving (i). For $a \in A$, $a = \bar{a}_1 + \bar{a}_2 + \cdots + \bar{a}_m$, where $\bar{a}_i \in \bar{A}_i$. Choose $n \geqq 1$ such that $n\bar{a}_i \in A_i$, $i = 1, 2, \cdots, m$. Then

$$na = n\bar{a}_1 + n\bar{a}_2 + \cdots + n\bar{a}_m \in A_1 \oplus A_2 \oplus \cdots \oplus A_m,$$

and this proves (ii). Finally, suppose A^* contains elements e_i, $i = 1, 2, \cdots, m$, such that e_i acts as a right identity on $\bar{A}_i$ and a right annihilator on $\bar{A}_j$, $j \neq i$. Choose $n \geqq 1$ such that $ne_i \in A$, $i = 1, 2, \cdots, m$. For $a \in A$, $a = \bar{a}_1 + \bar{a}_2 + \cdots + \bar{a}_m$ with $\bar{a}_i \in \bar{A}_i$. Then A contains

$$a(ne_i) = (\bar{a}_1 + \bar{a}_2 + \cdots + \bar{a}_m)(ne_i) = n\bar{a}_i.$$

Thus $n\bar{a}_i \in \bar{A}_i \cap A = A_i$ for $i = 1, 2, \cdots, m$. Hence

$$na = n\bar{a}_1 + n\bar{a}_2 + \cdots + n\bar{a}_m \in A_1 \oplus A_2 \oplus \cdots \oplus A_m.$$

Since a was an arbitrary element of A, this proves the final statement of the lemma.

COROLLARY 3.2. *Let A be a torsion-free ring such that A^* has an identity e which is the sum of m mutually orthogonal idempotents, $e = e_1 + e_2 + \cdots + e_m$. Let $A_{ij} = e_i A^* e_j \cap A$. Then the A_{ij} are independent subrings of A, $A_{ij}^* = e_i A^* e_j$, and $A/\sum \oplus_{i,j} A_{ij}$ has bounded order.*

Proof. The decomposition

$$A^* = A^*e_1 \oplus A^*e_2 \oplus \cdots \oplus A^*e_m$$

satisfies the conditions of Lemma 3.1. Hence $A/(A_1 \oplus A_2 \oplus \cdots \oplus A_m)$ has bounded order, where $A_j = A^*e_j \cap A$ and $A_j^* = A^*e_j$. Now apply 3.1 to the decompositions

$$A^*e_j = e_1 A^*e_j \oplus e_2 A^*e_j \oplus \cdots \oplus e_m A^*e_j,$$

$j = 1, 2, \cdots, m$. Then $A_j/(A_{1j} \oplus A_{2j} \oplus \cdots \oplus A_{mj})$ has bounded order, where $A_{ij} = e_i A^*e_j \cap A$ and $A_{ij}^* = e_i A^*e_j$. Combining these results, we conclude that $A/\sum \oplus_{i,j} A_{ij}$ has bounded order.

THEOREM 3.3. *Let T be an algebra over R with an identity such that*

$$T = T_1 \dotplus T_2 \dotplus \cdots \dotplus T_m \qquad (\textit{ring direct sum}).$$

Let A be a torsion-free ring of algebra type T. Then there exists a subring C of A such that

$$C = A_1 \dotplus A_2 \dotplus \cdots \dotplus A_m,$$

where A_i is a ring of algebra type T_i, and A/C has bounded order.

Proof. The decomposition $T = T_1 \dotplus T_2 \dotplus \cdots \dotplus T_m$ yields a decomposition $e = e_1 + e_2 + \cdots + e_m$ of the identity e of T into mutually orthogonal central idempotents. By hypothesis, $A^* = T$, and by applying 3.2, $A_{ij} = e_i T e_j \cap A = 0$ if $i \neq j$, $A_{ii} = e_i T e_i \cap A = T_i \cap A$, and $A_{ii}^* = T_i$. The A_{ii}, $i = 1, 2, \cdots, m$, are independent subrings of A. Let

$$C = A_{11} \oplus A_{22} \oplus \cdots \oplus A_{mm} \qquad \text{(group direct sum).}$$

Since $A_{ii} A_{jj} = 0$ if $i \neq j$, it follows that C is a subring of A and

$$C = A_{11} \dotplus A_{22} \dotplus \cdots \dotplus A_{mm}.$$

By 3.2,

$$A/\textstyle\sum \oplus_{i,j} A_{ij} = A/(A_{11} \oplus A_{22} \oplus \cdots \oplus A_{mm}) = A/C$$

has bounded order.

THEOREM 3.4. *Let T be an algebra over R with an identity such that*

$$T = T_1 \dotplus T_2 \dotplus \cdots \dotplus T_m.$$

Then a torsion-free group A admits multiplication of algebra type T if and only if

$$A \sim A_1 \oplus A_2 \oplus \cdots \oplus A_m,$$

where A_i admits multiplication of algebra type T_i.

Proof. If A admits multiplication of algebra type T, then A is a torsion-free ring satisfying the hypotheses of Theorem 3.3. Hence by 3.3,

$$A/(A_1 \oplus A_2 \oplus \cdots \oplus A_m)$$

has bounded order, where $A_i^* = T_i$. Thus $A \sim A_1 \oplus A_2 \oplus \cdots \oplus A_m$ where A_i admits multiplication of algebra type T_i. Conversely, if

$$A \sim A_1 \oplus A_2 \oplus \cdots \oplus A_m,$$

where A_i admits multiplication of algebra type T_i, then

$$(A_1 \dotplus A_2 \dotplus \cdots \dotplus A_m)^* = A_1^* \dotplus A_2^* \dotplus \cdots \dotplus A_m^* = T_1 \dotplus T_2 \dotplus \cdots \dotplus T_m.$$

Thus $A_1 \oplus A_2 \oplus \cdots \oplus A_m$ admits multiplication of algebra type T. By Corollary 2.7, A admits multiplication of type T.

COROLLARY 3.5. *Let A be a torsion-free ring of finite rank with semisimple algebra type S. Then A contains a subring C of finite index such that*

$$C = S_1 \dotplus S_2 \dotplus \cdots \dotplus S_m,$$

where each S_i is a ring of simple algebra type.

Proof. This is an immediate consequence of Theorem 3.3, the decomposition of the semisimple algebra S into its simple constituents, and the observation that if A has finite rank, then A/C has finite rank and bounded order, and hence A/C is finite.

COROLLARY 3.6. *A torsion-free group A of finite rank admits multiplication of semisimple algebra type if and only if*

$$A \sim A_1 \oplus A_2 \oplus \cdots \oplus A_m,$$

where each A_i admits multiplication of simple algebra type.

Proof. This is an immediate consequence of Theorem 3.4.

THEOREM 3.7. *Let $T = B_m$ be a full m by m matrix ring over an R-algebra B with an identity. Let A be a torsion-free ring of algebra type T. Then there exists a subring C of A such that $C = D_m$, a full m by m matrix ring over a torsion-free ring D, where D has algebra type B, and A/C has bounded order.*

Proof. Let e_{ij}, $i, j = 1, 2, \cdots, m$, be the matrix units in $T = A^*$. Let $\bar{B} = e_{11} T e_{11}$. Then $\bar{B}$ is a subalgebra of T and is algebra-isomorphic to B. Further $\bar{B} \cap A$ is a subring of A such that $(\bar{B} \cap A)^* = \bar{B}$. Choose $n \geqq 1$ such that $ne_{ij} \in A$ for all i, j, and consider the subset of A,

$$D_{ij} = (ne_{1i})A(ne_{j1}) = n^2 e_{1i} A e_{j1}.$$

Since $D_{ij} = e_{11} D_{ij} e_{11}$, $D_{ij} \subseteq \bar{B} \cap A$. Also, D_{ij} is a subring of $\bar{B} \cap A$ because

$$(n^2 e_{1i} a_1 e_{j1})(n^2 e_{1i} a_2 e_{j1}) = n^2 e_{1i}(a_1 n^2 e_{ji} a_2) e_{j1},$$

for a_1 and a_2 in A.

Let $D = \bigcap_{i,j} D_{ij}$, and let $x \in \bar{B} \cap A$. Then

$$x = e_{11} x e_{11} = e_{1i} e_{i1} x e_{1j} e_{j1},$$

and

$$n^4 x = n^2 e_{1i}[(ne_{i1}) x (ne_{1j})] e_{j1}.$$

Since $x \in A$, $(ne_{i1})x(ne_{1j}) \in A$, so that $n^4 x \in D_{ij}$ for all i, j. Hence

$$n^4(\bar{B} \cap A) \subseteq D,$$

and $D^* = (\bar{B} \cap A)^* = \bar{B} \cong B$.

Now let $d_{ij} \in D$, $i, j = 1, \cdots, m$. Then $d_{ij} \in D_{ij}$, so $d_{ij} = (ne_{1i}) a_{ij} (ne_{j1})$ for some $a_{ij} \in A$. Hence

$$e_{i1} d_{ij} e_{1j} = (ne_{ii}) a_{ij} (ne_{jj}) \in A.$$

Therefore $\sum_{i,j} e_{i1} d_{ij} e_{1j} \in A$. By definition of the matrix units, the mapping

$$[d_{ij}] \rightarrow \textstyle\sum_{i,j} e_{i1} d_{ij} e_{1j}$$

is an isomorphism of D_m onto a subring $C \subseteq A$. If $x \in A$, then

$$n^6 x = n^6 \textstyle\sum_{i,j} e_{ii} x e_{jj} = \sum_{i,j} e_{i1}(n^4(ne_{1i}) x (ne_{j1})) e_{1j} \in C,$$

since $n^4(ne_{1i})x(ne_{j1}) \in n^4 D_{ij} \subseteq n^4(\bar{B} \cap A) \subseteq D$. Thus, A/C has bounded order.

THEOREM 3.8 *Let $T = B_m$ be a full m by m matrix ring over a rational algebra B with an identity. Then a torsion-free group A admits a multiplication* *of algebra type* T *if and only if* $A \sim \sum \oplus_{i,j=1}^{m} D_{ij}$ *where for all* i, j, $D_{ij} \cong D$ *and* D *admits multiplication of algebra type* B.

The proof is similar to 3.4, and we omit it.

COROLLARY 3.9. *Let* A *be a torsion-free ring of finite rank whose algebra type is simple. Then* A *contains a subring* C *of finite index such that* $C \cong D_m$, *where* D *is a torsion-free ring whose algebra type is a rational division algebra.*

COROLLARY 3.10. *A torsion-free group* A *of finite rank admits a multiplication of simple algebra type if and only if* $A \sim \sum \oplus_{i,j=1}^{m} D_{ij}$, *where* $D_{ij} \cong D$ *for all* i, j *and* D *admits a multiplication whose algebra type is a rational division algebra.*

These corollaries are consequences of 3.7 and 3.8 and the Wedderburn structure theorem for simple algebras of finite order. They can also be obtained from Theorems 6.9 and 1.12.

4. The principal decomposition

This section is devoted to the proof of Theorem 1.4. This result implies that a torsion-free group A of finite rank is a finite extension of a subgroup $S \oplus N$, where S admits a multiplication of semisimple type and N admits a multiplication of nilpotent type.

Let A be a torsion-free ring of finite rank. Then A^* is a finite-dimensional algebra over R, and by the Wedderburn principal theorem, $A^* = \bar{S} \oplus \bar{N}$, where $\bar{N}$ is the radical of A^* and $\bar{S}$ is a semisimple subring of A^*. Let $S = \bar{S} \cap A$ and $N = \bar{N} \cap A$. Then S and N are subrings of A, and, since $\bar{N}$ is an ideal, $S \oplus N$ is also a subring of A. In this section we show that as groups, $S \oplus N$ has finite index in A, and consequently $A \approx S \oplus N$. By making the obvious identifications, $S^* = \bar{S}$, $N^* = \bar{N}$, so that

$$A^* = \bar{S} \oplus \bar{N} = S^* \oplus N^* = (S \oplus N)^*.$$

Thus A has the same algebra type as the subring $S \oplus N$. It should be noted that N is the maximum nilpotent ideal in A [9, p. 271].

LEMMA 4.1. *Let* $S_1 = \{x \in \bar{S} \mid x + y \in A \text{ for some } y \in \bar{N}\}$. *Then* S_1 *is a subring of* $\bar{S}$ *and* $S_1^* = \bar{S}$.

Proof. It follows from the fact that $\bar{N}$ is an ideal in A^* that S_1 is a subring of $\bar{S}$. Clearly $S \subseteq S_1 \subseteq \bar{S}$. Hence $\bar{S} = S^* \subseteq S_1^* \subseteq \bar{S}$.

LEMMA 4.2. $A/(S \oplus N) \cong S_1/S$ (*as additive groups*).

Proof. Let $z \in A$. Then $z = x + y$, $x \in \bar{S}$, $y \in \bar{N}$, uniquely. The mapping defined by $z \rightarrow x + S$ is clearly a homomorphism of A onto S_1/S. The kernel of the mapping consists of all $z \in A$ such that $z = x + y$ with $x \in S$. But then $y = z - x \in A \cap \bar{N} = N$, so that $z \in S \oplus N$.

Since A has finite rank, A^*, and consequently $\bar{S}$, are finite-dimensional algebras.

LEMMA 4.3. *There exists a basis* $\{x_1, x_2, \cdots, x_m\}$ *of* $\bar{S}$ *such that the subgroup* B *of* $\bar{S}$ *generated by* $\{x_1, x_2, \cdots, x_m\}$ *is a subring of* S.

Proof. Since $S^* = \bar{S}$, a maximal independent set $z_1, z_2, \cdots, z_m$ in S is a basis of $\bar{S}$. We have $z_i z_j = \sum_k \gamma_{ijk} z_k$, where $\gamma_{ijk} \in R$. Choose $n \geqq 1$ so that $n\gamma_{ijk} = \gamma^*_{ijk}$ is an integer for all i, j, k. Set $x_i = nz_i$, $i = 1, 2, \cdots, m$. Then the subgroup B generated by $x_1, x_2, \cdots, x_m$ is a subring of S.

Let p be a fixed rational prime. We define for $k \geqq 0$

$$I_k = \{x \in B \mid (1/p^k)x \in S\}, \qquad J_k = \{x \in B \mid (1/p^k)x \in S_1\}.$$

LEMMA 4.4 *We have* $B = I_0 \supseteq I_1 \supseteq I_2 \supseteq \cdots$; $B = J_0 \supseteq J_1 \supseteq J_2 \supseteq \cdots$; $I_k \subseteq J_k$; I_k *and* J_k *are two-sided ideals in* B; $I_k^2 \subseteq I_{2k}$; $J_k^2 \subseteq J_{2k}$; $J_k^t \subseteq I_k$, *where* $\bar{N}^t = 0$.

Proof. The first four of these assertions follow at once from the definitions of I_k and J_k. If $x, y \in I_k$, then $(1/p^k)x \in S$, $(1/p^k)y \in S$, so that $(1/p^{2k})xy \in S$. Hence $xy \in I_{2k}$ and $I_k^2 \subseteq I_{2k}$. Similarly, $J_k^2 \subseteq J_{2k}$. To prove the last assertion, note that if $x_1, x_2 \in J_k$, then there exist $y_1, y_2 \in \bar{N}$ such that

$$(1/p^k)x_1 - y_1 \in A, \qquad (1/p^k)x_2 - y_2 \in A$$

and

$$\begin{aligned}(1/p^k)x_1 x_2 - p^k y_1 y_2 &= x_1((1/p^k)x_2 - y_2) \\ &\quad + ((1/p^k)x_1 - y_1)x_2 - p^k((1/p^k)x_1 - y_1)((1/p^k)x_2 - y_2)\end{aligned}$$

is in A. Thus, if $x_1, x_2, \cdots, x_t \in J_k$, there exist $y_i \in \bar{N}$ such that

$$(1/p^k)x_i - y_i \in A, \qquad i = 1, 2, \cdots, t,$$

and by induction we have

$$(1/p^k)x_1 x_2 \cdots x_t - p^{(t-1)k} y_1 y_2 \cdots y_t \in A.$$

Since $\bar{N}^t = 0$, $(1/p^k)x_1 x_2 \cdots x_t \in S_1 \cap A \subseteq \bar{S} \cap A$. Hence

$$x_1 x_2 \cdots x_t \in I_k,$$

and $J_k^t \subseteq I_k$.

LEMMA 4.5. If $k \geqq 0, l \geqq 0$, *then* $I_{k+l} \cap p^l B = p^l I_k$, *and* $J_{k+l} \cap p^l B = p^l J_k$.

Proof. If $x \in p^l I_k$, then $x = p^l y$, where $y \in I_k$. Thus, $(1/p^k)y \in S$ and $(1/p^{k+l})x = (1/p^k)y \in S$. Hence $x \in I_{k+l}$. Since $x \in p^l B$,

$$p^l I_k \subseteq I_{k+l} \cap p^l B.$$

On the other hand, if $x \in I_{k+l} \cap p^l B$, $x = p^l y$ with $y \in B$ and $(1/p^{k+l})x \in S$. Hence $(1/p^k)y \in S$, and $y \in I_k$. Therefore $x \in p^l I_k$. The proof of the second assertion is similar.

Since rank B = rank S = rank S_1, S/B and S_1/B are torsion groups. Let $T = T_p$ and $T_1 = T_{1p}$ be the p-primary components of S/B and S_1/B respectively.

LEMMA 4.6. *If* $k \geqq 0$, $l \geqq 0$, *then*

$$(p^kT)[p^l] \cong I_{k+l}/p^lB \cap I_{k+l},$$

and

$$(p^kT_1)[p^l] \cong J_{k+l}/p^lB \cap J_{k+l}.$$

Proof. Let $x \in I_{k+l}$. Then $x \in B$ and $(1/p^{k+l})x \in S$. Define $\phi: I_{k+l} \to S/B$ by $\phi(x) = (1/p^l)x + B$. Since $p^l\phi(x) = 0$ and

$$\phi(x) = p^k((1/p^{k+l})x + B) \in p^kT,$$

we have $\phi(x) \in (p^kT)[p^l]$. Thus $\phi(I_{k+l}) \subseteq (p^kT)[p^l]$. If $\bar{x} \in (p^kT)[p^l]$, then $\bar{x} = p^ky + B$, $y \in S$, where $p^{l+k}y \in B$. Then

$$x = p^{k+l}y \in p^{k+l}S \cap B = I_{k+l},$$

and $\phi(x) = \bar{x}$. Thus $\phi(I_{k+l}) = (p^kT)[p^l]$. Finally $x \in \ker \phi$ if and only if $(1/p^l)x \in B$, and this is so if and only if $x \in p^lB \cap I_{k+l}$.

A similar argument gives the second isomorphism.

LEMMA 4.7. *If the ring B/pB is semisimple, then $T_1 = T$, and T is a divisible p-primary group of rank $m_1 \leqq m$ = rank S.*

Proof. Since T and T_1 are homomorphic images of the rank-m groups S and S_1 respectively, they are groups of rank $\leqq m$ [15]. By the definitions of T and T_1, $T \subseteq T_1$. Let ψ be the natural ring homomorphism of B onto B/pB. Then since B/pB is semisimple and I_k, J_k are ideals in B, Lemma 4.4 yields

$$\psi(I_k) \subseteq \psi(J_k) = [\psi(J_k)]^t = \psi(J_k^t) \subseteq \psi(I_k),$$

and

$$\psi(I_k) = [\psi(I_k)]^2 = \psi(I_k^2) \subseteq \psi(I_{2k}) \subseteq \psi(I_k),$$

for all $k \geqq 0$.

Thus we have by Lemma 4.6

$$(p^kT)[p] \cong I_{k+1}/pB \cap I_{k+1} \cong \psi(I_{k+1}) = \psi(J_{k+1})$$
$$\cong J_{k+1}/pB \cap J_{k+1} \cong (p^kT_1)[p],$$

for all $k \geqq 0$. In particular, $T[p] = T_1[p]$, so that T and T_1 have the same finite rank. By a similar argument, $\psi(I_k) = \psi(I_{2k})$ for all $k \geqq 0$ implies that

$$T[p] = (pT)[p] = (p^2T)[p] = \cdots,$$

so that T is a divisible p-primary group. Since rank T = rank T_1, we have $T = T_1$, which completes the proof.

LEMMA 4.8. *$T_p = T_{1p}$ is divisible for almost all primes p.*

Proof. By Lemma 4.7, it is sufficient to show that B/pB is semisimple for almost all primes p. Let $\tilde{B}$ be a maximal order of $\bar{S}$ containing B. (The subring of $\bar{S}$ generated by B and the identity $e \in \bar{S}$ is an order of $\bar{S}$, and this subring is contained in a maximal order [8, p. 70].) Then $\tilde{B}/p\tilde{B}$ is semisimple if and only if p does not divide the discriminant d of $\bar{S}$ [8, p. 88]. Since $\bar{S}$ is separable over R, $d \neq 0$ [10, p. 116], so that $\tilde{B}/p\tilde{B}$ is semisimple for almost all primes p. The proof is completed by showing that $B/pB \cong \tilde{B}/p\tilde{B}$ for almost all primes p. Consider the natural homomorphism of $\tilde{B}$ onto $\tilde{B}/p\tilde{B}$. The induced homomorphism of B into $\tilde{B}/p\tilde{B}$ is onto for almost all p. For there exists an $n \geqq 1$ such that $n\tilde{B} \subseteq B \subseteq \tilde{B}$, which implies that

$$\tilde{B} + p\tilde{B} = n\tilde{B} + p\tilde{B} \subseteq B + p\tilde{B} \subseteq \tilde{B} + p\tilde{B}$$

for those primes p which do not divide n. Moreover, for such primes p, $pB = p\tilde{B} \cap B$, the kernel of the induced homomorphism.

COROLLARY 4.9. *Let A be a torsion-free group of finite rank which admits a multiplication of semisimple algebra type. Then A is a q.d. group (see Definition 1.6).*

Proof. Let A have rank n. Since A admits a multiplication of semisimple type, as a ring, the algebra type A^* of A is semisimple. As in Lemma 4.3, select a basis $x_1, x_2, \cdots, x_n$ of A^* such that the subgroup B generated by $x_1, x_2, \cdots, x_n$ is a subring of A. Then B is finitely generated, and B is a full subgroup of A. Now it follows from Lemmas 4.7 and 4.8 that the p-primary component of A/B is divisible for almost all primes p. Since A/B has finite rank, the p-primary component of A/B is a direct sum of a divisible group and a finite group for all primes p. Hence A/B is a direct sum of a divisible group and a finite group. Thus A is a q.d. group.

In case the algebra type of A is a quadratic field, Corollary 4.9 can be proved by direct computation. The result is obtained by such a procedure in [4].

To complete the proof of Theorem 1.4, it remains to examine the finite number of exceptional primes p which are not covered by Lemma 4.8. The result which we need is Lemma 4.13 which states that T_p has finite index in T_{1p} for all primes p.

Let $\tilde{B}$ be a maximal order of $\bar{S}$ containing B, and let $n \geqq 1$ be such that $n\tilde{B} \subseteq B$. We define

$$\tilde{I}_k = \tilde{B}I_k\tilde{B}, \qquad \tilde{J}_k = \tilde{B}J_k\tilde{B}.$$

LEMMA 4.10. $n^2\tilde{I}_k \subseteq I_k$; $n^2\tilde{J}_k \subseteq J_k$; $\tilde{I}_{k+1} \subseteq \tilde{I}_k$; $\tilde{J}_{k+1} \subseteq \tilde{J}_k$; $\tilde{I}_k \subseteq \tilde{J}_k$; $n\tilde{I}_k^2 \subseteq \tilde{I}_{2k}$; $n\tilde{J}_k^2 \subseteq \tilde{J}_{2k}$; $n^{t-1}\tilde{J}_k^t \subseteq \tilde{I}_k$, *where* $\bar{N}^t = 0$; $n^2(\tilde{I}_{k+l} \cap p^lB) \subseteq p^l\tilde{I}_k$.

Proof. These relations follow from Lemmas 4.4 and 4.5 and the fact that $n\tilde{B} \subseteq B$.

Since $\tilde{B}$ is a maximal order in the semisimple algebra $\bar{S}$, we can use the well-developed arithmetic of ideals in $\tilde{B}$ [8, pp. 72–78].

Let $P_1, P_2, \cdots, P_u$ be all prime ideals in $\tilde{B}$ which are factors of $p\tilde{B}$, $n\tilde{B}$,

$\tilde{I}_1$, or $\tilde{J}_1$. It follows from the relations $n\tilde{I}_k^2 \subseteq \tilde{I}_{2k}$ and $n\tilde{J}_k^2 \subseteq \tilde{J}_{2k}$ of Lemma 4.10 that these prime ideals are all of the prime factors of any of the ideals $\tilde{I}_k$ of $\tilde{J}_k$. Hence we can write

$$\begin{aligned} p\tilde{B} &= P_1^{\alpha_1} P_2^{\alpha_2} \cdots P_u^{\alpha_u}, \\ n\tilde{B} &= P_1^{\beta_1} P_2^{\beta_2} \cdots P_u^{\beta_u}, \\ \tilde{I}_k &= P_1^{\gamma_{k1}} P_2^{\gamma_{k2}} \cdots P_u^{\gamma_{ku}}, \\ \tilde{J}_k &= P_1^{\delta_{k1}} P_2^{\delta_{k2}} \cdots P_u^{\delta_{ku}}. \end{aligned}$$

LEMMA 4.11. *For $i = 1, 2, \cdots, u$ we have*

(i) $(t-1)\beta_i + t\delta_{ki} \geqq \gamma_{ki}$;

(ii) $2\beta_i + \max\{l\alpha_i, \gamma_{k+l,i}\} \geqq l\alpha_i + \gamma_{ki}$;

(iii) *there exists an integer $K(l)$ such that if $k \geqq K(l)$,*

$$\min\{\gamma_{ki}, l\alpha_i\} \leqq 2\beta_i + \delta_{ki}.$$

Proof. The inequalities (i) and (ii) follow from the last two inclusions of Lemma 4.10. We note first that (iii) holds if $\alpha_i = 0$ or if $\gamma_{ki} \leqq 2\beta_i$ for all k. Hence assume that $\alpha_i \neq 0$ and that for some k_0, $\gamma_{k_0 i} > 2\beta_i$. Since $\tilde{I}_{k+1} \subseteq \tilde{I}_k$, γ_{ki} does not decrease as k increases, so that $\gamma_{ki} > 2\beta_i$ for $k \geqq k_0$. Thus, (ii) must have the form

$$2\beta_i + \gamma_{k+l,i} \geqq l\alpha_i + \gamma_{ki}, \qquad \text{for } k \geqq k_0.$$

Since $\alpha_i \neq 0$, this implies that $\gamma_{ki} \to \infty$ as $k \to \infty$. Then by (i), $\delta_{ki} \to \infty$ as $k \to \infty$. Thus for sufficiently large k (depending on l), we have $l\alpha_i \leqq \delta_{ki}$. This inequality implies (iii).

LEMMA 4.12. *For any l there exists an integer $K(l)$ such that if $k \geqq K(l)$, then*

$$\tilde{I}_k + p^l\tilde{B} \supseteq n^2\tilde{J}_k.$$

Proof. This statement is equivalent to (iii), Lemma 4.11.

LEMMA 4.13. *For every prime p, T_p has finite index in T_{1p}.*

Proof. Since T_p and T_{1p} are p-primary groups of finite rank, it is sufficient to prove that these groups have the same maximal divisible subgroup.

From Lemma 4.12 and Lemma 4.10 we obtain

$$n^4J_k \subseteq n^4\tilde{J}_k \subseteq n^2\tilde{I}_k + p^l n^2\tilde{B} \subseteq I_k + p^lB, \quad \text{for } k \geqq K(l).$$

Let ψ_l be the natural homomorphism of B onto B/p^lB. Then

$$n^4\psi_l(J_k) \subseteq \psi_l(I_k), \qquad \text{for } k \geqq K(l).$$

Since

$$\psi_l(J_k) \cong J_k/p^lB \cap J_k \quad \text{and} \quad \psi_l(I_k) \cong I_k/p^lB \cap I_k,$$

we have for $k \geqq l$ by Lemma 4.6,

$$\psi_l(J_k) \cong (p^{k-l}T_1)[p^l] \quad \text{and} \quad \psi_l(I_k) \cong (p^{k-l}T)[p^l].$$

If j is the highest power of p dividing n^4, then

$$n^4(p^{k-l}T_1)[p^l] = (p^{k+j-l}T_1)[p^{l-j}]$$

is isomorphic to a subgroup of $(p^{k-l}T)[p^l]$. Let $l = j + 1$. Then for $k \geqq \max\{K(l), j + 1\}$, $(p^{k-1}T_1)[p]$ is isomorphic to a subgroup of $(p^{k-j-1}T)[p^{j+1}]$, which implies that the rank of $p^{k-1}T_1$ does not exceed the rank of $p^{k-j-1}T$. By taking k so large that p^{k-1} and p^{k-j-1} exceed the orders of the finite cyclic summands of T_1 and T respectively, we conclude that the rank of the maximal divisible subgroup of T_1 does not exceed the rank of the maximal divisible subgroup of T. On the other hand, $T \subseteq T_1$, and hence these maximal divisible subgroups coincide.

Proof of Theorem 1.4. The only statement left to prove is that $S \oplus N$ has finite index in A. By Lemma 4.2,

$$A/(S \oplus N) \cong S_1/S \cong (S_1/B)/(S/B) = \sum \oplus_p T_{1p}/T_p .$$

By Lemma 4.8, $T_{1p}/T_p = 0$ for almost all p, and by Lemma 4.13, T_{1p}/T_p is finite for all p. Hence $A/(S \oplus N)$ is finite.

5. Quotient-divisible groups

In this section we study quotient-divisible, or q.d., groups (see Definition 1.6).

Denote by $\mathfrak{D}$ the class of all torsion groups T such that $T = U \oplus V$, where U is of bounded order and V is divisible. It is not hard to show that a torsion group T belongs to $\mathfrak{D}$ if and only if T is quasi-isomorphic to a divisible group. We collect a few useful properties of the groups T in $\mathfrak{D}$.

LEMMA 5.1. *A torsion group T is in $\mathfrak{D}$ if and only if there is an integer $n \geqq 1$ such that nT is divisible.*

Proof. Assume nT is divisible. Then $T = nT \oplus T'$, and

$$nT = n^2T \oplus nT' = nT \oplus nT'.$$

Hence $nT' = 0$. The converse is clear.

LEMMA 5.2. *Let S and T be in $\mathfrak{D}$. Suppose W is an extension of S by T. Then W is in $\mathfrak{D}$.*

Proof. Choose m and $n \geqq 1$ so that mS and nT are divisible. We show mnW is divisible. Let $x \in W$, and suppose $k \geqq 1$ is arbitrary. Then $nx + S \in n(W/S) \cong nT$ is divisible, so $y \in nW$ exists such that $nx - ky \in S$. Then $nmx - mky \in mS$. Since mS is divisible, there exists $z \in mS = nmS \subseteq nmW$ such that $nmx - mky = kz$. Thus, $nmx = k(z + my)$, where $z \in mnW$ and $my \in mnW$. Since x and k are arbitrary, mnW is divisible.

LEMMA 5.3. *If T is a homomorphic image of a group S in $\mathfrak{D}$, then T is in $\mathfrak{D}$.*

Proof. If ϕ is a homomorphism of S on T and nS is divisible, then $nT = n\phi(S) = \phi(nS)$ is the homomorphic image of a divisible group, and hence is divisible.

We turn now to q.d. groups. Unless the contrary is stated, all groups considered are torsion-free.

LEMMA 5.4. *If the torsion-free group A is an extension of a q.d. group B by a torsion group T in $\mathfrak{D}$, then A is a q.d. group.*

Proof. Let C be a full subgroup of B such that C is free and B/C is in $\mathfrak{D}$. Then A/C is an extension of B/C by T, and hence, by 5.2, belongs to $\mathfrak{D}$. Thus, A is a q.d. group.

COROLLARY 5.5. *If $A \sim B$ and B is a q.d. group, then A is a q.d. group.*

Proof. By definition of $\sim$, B is isomorphic to a subgroup B' of A such that A/B' has bounded order.

LEMMA 5.6. *Suppose A is a q.d. group. Then A contains a full subgroup B which is free and such that A/B is divisible.*

Proof. Let $F \subseteq A$ be free and such that $A/F = C \oplus D$, with C bounded and D divisible. Let $B = \{x \in A \mid x + F \in C\}$. Then B is a subgroup of A containing F, $A/B \cong D$ is divisible, and $B/F \cong C$ satisfies $n(B/F) = 0$ for some $n \geqq 1$. Consequently $B \cong nB \subseteq F$, so B is free.

It is clear that any free group is a q.d. group, and so is any divisible group. Among the groups of rank one, the q.d. groups are precisely those of non-nil type, that is, of type $(a_1, a_2, \cdots)$ with all a_i either 0 or ∞ (see [13]). It follows from 5.6 that an arbitrary direct sum of q.d. groups is a q.d. group. The class of q.d. groups is not closed under homomorphisms since every group is the homomorphic image of a free group. However, a torsion-free homomorphic image of a q.d. group of finite rank is a q.d. group, a fact which can easily be deduced from the next lemma.

LEMMA 5.7. *Suppose A is a q.d. group of finite rank and B is any full subgroup of A. Then A/B is in $\mathfrak{D}$.*

Proof. Let F be a full subgroup of A such that F is free and A/F is in $\mathfrak{D}$. Since F is finitely generated and B is full, there is an $n \geqq 1$ such that $nF \subseteq B$. Since $n(F/nF) = 0$, F/nF is in $\mathfrak{D}$. By 5.2, A/nF is in $\mathfrak{D}$. But $nF \subseteq B$ implies A/B is a homomorphic image of A/nF. Therefore, A/B is in $\mathfrak{D}$ by 5.3.

COROLLARY 5.8. *A torsion-free homomorphic image of a q.d. group A of finite rank is a q.d. group.*

Proof. We prove an equivalent statement, namely, if B is a pure subgroup of a q.d. group A of finite rank, then A/B is a q.d. group. Let C/B be a full free subgroup of the torsion-free group A/B. Then C is a full subgroup of A. By Lemma 5.7, $A/C = (A/B)/(C/B)$ is in $\mathfrak{D}$. Hence A/B is a q.d. group.

LEMMA 5.9. *Let A be a torsion-free group of finite rank, and suppose B and C are full subgroups of A which are free. Then $d(A/B) \cong d(A/C)$.*

Proof. Suppose first that $B \subseteq C$. Since B is full and C is finitely generated, there is an $n \geqq 1$ such that $nC \subseteq B$. Because A is torsion-free, $A/C \cong nA/nC = n(A/nC)$, so that $d(A/C) \cong d(A/nC)$. Since the rank of A is finite, the homomorphisms $A/nC \to A/B \to A/C$ induce homomorphisms $d(A/nC) \to d(A/B) \to d(A/C)$. Thus, $\text{rk } d_p(A/C) = \text{rk } d_p(A/nC) \geqq \text{rk } d_p(A/B) \geqq \text{rk } d_p(A/C)$ for all p. Therefore, $d(A/B) \cong d(A/C)$. To remove the restriction $B \subseteq C$, note that $B \cap C$ is full and free and $d(A/B) \cong d(A/B \cap C) \cong d(A/C)$.

Our next objective is to construct a system of invariants for the quasi-isomorphism classes of finite-rank q.d. groups.

It is important to establish our notation carefully. Let R_p be the subring of R consisting of all m/n with $(n, p) = 1$. We have the inclusions

$$Z \subseteq R_p \subseteq R \subseteq R^{(p)}, \qquad R_p \subseteq Z^{(p)} \subseteq R^{(p)},$$

provided the obvious identifications are made.

As mentioned in the Introduction, we may restrict our attention to groups which are full subgroups of a fixed rational vector space V of finite dimension. For every rational prime p, form the $R^{(p)}$-space $V^{(p)} = V \otimes R^{(p)}$. We consider $V^{(p)}$ as an extension of V and assume that if $p \neq q$, the spaces $V^{(p)}$ and $V^{(q)}$ have only V in common. Since $R^{(p)}$ contains Z, R_p, R, and $Z^{(p)}$ as subrings, $V^{(p)}$ can be regarded as a module over each of these rings. From the inclusions $Z \subseteq R_p \subseteq R \subseteq R^{(p)}$ we get, for any subgroup A of V,

$$A \subseteq R_p A \subseteq RA \subseteq V,$$

where, for any ring $S \subseteq R^{(p)}$, SA is $\{\sum s_i x_i \mid s_i \in S,\ x_i \in A\}$ (which in fact reduces to $\{sx \mid s \in S,\ x \in A\}$ if $S \subseteq R$). Also, if we denote $A^{(p)} = Z^{(p)}A$, then the inclusions $R_p \subseteq Z^{(p)} \subseteq R^{(p)}$ yield $R_p A \subseteq A^{(p)} \subseteq V^{(p)}$. Note that $Z^{(p)}V = V^{(p)}$, since V is divisible. Also, $V^{(p)} = R^{(p)}V = R^{(p)}RA = R^{(p)}A$ if A is full in V. Moreover in this case

$$\text{rk } A = \dim V = \dim_{R^{(p)}} V^{(p)} = \text{rk}_{Z^{(p)}} A^{(p)}.$$

LEMMA 5.10. $A = \bigcap_p R_p A$.

Proof. (See [12].) Let $J_x = \{n \in Z \mid nx \in A \text{ for a fixed } x \in V\}$. Then J_x is an ideal in Z which, if $x \in R_p A$, contains an integer prime to p. Thus, if $x \in \bigcap_p R_p A$, then $J_x = (1)$ and $x \in A$.

If $X = \{x_1, \cdots, x_n\}$ is a subset of V, denote by $Z[X]$ the subgroup of V generated by X. Let $Z^{(p)}[X]$ be the $Z^{(p)}$-module in $V^{(p)}$ generated by X. Clearly $Z^{(p)}[X] = Z^{(p)}Z[X]$. Since $Z[X]$ is finitely generated, it is free. If also X spans V (over R), then $Z[X]$ is a full subgroup of V. Conversely, any free full subgroup A of V is of the form $Z[X]$, where X can be taken as a maximal independent subset of A.

LEMMA 5.11. *Let A and B be subgroups of V. Suppose B is a full subgroup of A. Then $(A/B)_p \cong R_p A/R_p B$.*

Proof. Consider the commutative diagram

$$\begin{array}{ccccccccc} 0 \to B & \longrightarrow & A & \xrightarrow{\phi} & A/B \to 0 \\ \downarrow i & & \downarrow i & & \downarrow \psi \\ 0 \to R_p B & \to & R_p A & \xrightarrow{\phi'} & R_p A/R_p B \to 0 \end{array}$$

where i and the unlabeled maps are inclusions, ϕ and ϕ' are the natural projections making the rows exact, and ψ is defined uniquely by the requirement of commutativity. First note that $\ker \psi = \sum_{q \neq p} (A/B)_q$. Indeed, if $x \in A$, then $\psi\phi x = 0$ if and only if $\phi' i x = 0$, or, by exactness, if and only if $ix \in R_p B$. Hence $\phi x \in \ker \psi$ if and only if $x = (1/m)y$, where $y \in B$ and $(m, p) = 1$. This is clearly equivalent to $m\phi x = 0$, or $\phi x \in \sum_{q \neq p} (A/B)_q$. We next prove that ψ is onto. For this, it suffices to show $\phi' i$ is onto, or, equivalently, $R_p A = A + R_p B$. Let $r = m/n \in R_p$, $(n, p) = 1$, and $x \in A$. Since B is full in A, there is an integer $k \geqq 1$ such that $kx \in B$. Let $k = p^t l$, where $(l, p) = 1$. Choose u and v in Z to satisfy $un + vp^t = 1$. Then

$$rx = (m/n)x = mux + (mv/nl)(kx) \in A + R_p B.$$

It follows that ψ induces an isomorphism of $(A/B)/(\sum_{q \neq p} (A/B)_q)$ (which is isomorphic to $(A/B)_p$) onto $R_p A/R_p B$.

LEMMA 5.12. *Let $X = \{x_1, \cdots, x_n\}$ be a maximal independent subset of A. Let $B = Z[X]$ and $B^{(p)} = Z^{(p)}[X]$. Then*

$$A + B^{(p)} = R_p A + B^{(p)} = A^{(p)},$$

and

$$B^{(p)} \cap V = B^{(p)} \cap R_p A = R_p B.$$

Hence,

$$A^{(p)}/B^{(p)} \cong R_p A/R_p B \cong (A/B)_p.$$

Proof. Clearly $A + B^{(p)} \subseteq R_p A + B^{(p)} \subseteq A^{(p)}$. Suppose $x \in A^{(p)}$. Then $x = \alpha_1 y_1 + \cdots + \alpha_m y_m$, where $y_i \in A$ and $\alpha_i \in Z^{(p)}$. Choose t so that $p^t y_i \in R_p B$ for $i = 1, \cdots, m$. This is possible since B is full in A. Select $k_1, \cdots, k_m$ in Z and $\beta_1, \cdots, \beta_m$ in $Z^{(p)}$ so that $\alpha_i = k_i + p^t \beta_i$. Then $x = \sum k_i y_i + \sum \beta_i (p^t y_i) \in A + B^{(p)}$. Clearly $R_p B \subseteq B^{(p)} \cap R_p A \subseteq B^{(p)} \cap V$. If $x \in B^{(p)} \cap V$, then $x = \sum \alpha_i x_i = \sum r_i x_i$, where $\alpha_i \in Z^{(p)}$, $r_i \in R$. Since X is independent, $\alpha_i = r_i \in R \cap Z^{(p)} = R_p$. Therefore $x \in R_p B$.

DEFINITION 5.13. *Let A be a subgroup of V. Define $\delta_p(A)$ to be the maximal divisible subgroup of $A^{(p)}$.*

Since $R_p \subseteq Z^{(p)}$, it follows that $\delta_p(A) = \bigcap_{k=1}^{\infty} p^{k+1} A^{(p)}$, and since the quotient field of $Z^{(p)}$ is $R^{(p)} = RZ^{(p)}$, $\delta_p(A)$ is the maximal divisible submodule of $A^{(p)}$ regarded as a $Z^{(p)}$-module. Thus $\delta_p(A)$ is an $R^{(p)}$-subspace of $V^{(p)}$, and it will always be so considered.

LEMMA 5.14. *Suppose A is a q.d. group in V. Let $X = \{x_1, \cdots, x_n\}$ be a maximal independent subset of A such that $A/Z[X]$ is divisible. Then*

$$A^{(p)} = \delta_p(A) + Z^{(p)}[X].$$

Proof. Let $y \in A$. Since $A/Z[X]$ is divisible, we can find $y_1, y_2, \cdots$ in A and $z_0, z_1, \cdots$ in $Z[X]$ such that $y = py_1 + z_0$, $y_1 = py_2 + z_1, \cdots$. Let $z_i = \sum_{j=1}^{n} m_{ij} x_j$. Put $a_{kj} = \sum_{i=0}^{k} m_{ij} p^i$. Then

$$a_{kj} \equiv a_{k+l,j} \mod p^{k+1},$$

so $\lim_k a_{kj} = \alpha_j$ exists in $Z^{(p)}$. Moreover, p^{k+1} divides $\alpha_j - a_{kj}$, say

$$\alpha_j = a_{kj} + p^{k+1}\beta_{kj},$$

where $\beta_{kj} \in Z^{(p)}$. Define $w = \sum_{j=1}^{n} \alpha_j x_j \in Z^{(p)}[X]$. Then we have

$$\begin{aligned} y &= z_0 + pz_1 + \cdots + p^k z_k + p^{k+1} y_{k+1} \\ &= \sum_{j=1}^{n} a_{kj} x_j + p^{k+1} y_{k+1} = w + p^{k+1}\left(y_{k+1} - \sum_{j=1}^{n} \beta_{kj} x_j\right). \end{aligned}$$

Thus $y - w \in \bigcap_{k=1}^{\infty} p^{k+1} A^{(p)} = \delta_p(A)$ and $y \in \delta_p(A) + Z^{(p)}[X]$. This shows that $A \subseteq \delta_p(A) + Z^{(p)}[X]$, and hence

$$A^{(p)} = Z^{(p)}A \subseteq \delta_p(A) + Z^{(p)}[X].$$

The opposite inclusion is obvious.

COROLLARY 5.15. *If A is a q.d. group in V and B is any free full subgroup of A, then* $\dim_{R^{(p)}} \delta_p(A) = \operatorname{rk} (d(A/B))_p$.

Proof. By 5.6 and 5.9, we can assume that A/B is divisible. By 5.12 and 5.14.

$$(A/B)_p \cong A^{(p)}/B^{(p)} = (\delta_p(A) + B^{(p)})/B^{(p)} \cong \delta_p(A)/\delta_p(A) \cap B^{(p)}.$$

Let $\dim_{R^{(p)}} \delta_p(A) = r$. Then $\delta_p(A) \cap B^{(p)}$, being full in $\delta_p(A)$ and a submodule of $B^{(p)}$, is a free $Z^{(p)}$-module of $Z^{(p)}$-rank r. Let $\{y_1, \cdots, y_r\}$ be a $Z^{(p)}$-basis of $\delta_p(A) \cap B^{(p)}$. Then $\{y_1, \cdots, y_r\}$ is an $R^{(p)}$-basis of $\delta_p(A)$. That is,

$$\delta_p(A) = R^{(p)}y_1 \oplus \cdots \oplus R^{(p)}y_r, \qquad \delta_p(A) \cap B^{(p)} = Z^{(p)}y_1 \oplus \cdots \oplus Z^{(p)}y_r,$$

and $\delta_p(A)/\delta_p(A) \cap B^{(p)}$ is a direct sum of r copies of $R^{(p)}/Z^{(p)}$. By 5.12, $R^{(p)}/Z^{(p)} \cong (R/Z)_p = Z(p^\infty)$. Hence

$$\operatorname{rk} (A/B)_p = \operatorname{rk} (\delta_p(A)/\delta_p(A) \cap B^{(p)}) = r = \dim_{R^{(p)}} \delta_p(A).$$

The integer $\dim_{R^{(p)}} \delta_p(A)$ is what Kurosh [12] calls the reduced p rank of A.

Recall that if A and B are subgroups of the R-space V, we have defined (see Definition 1.7) $A \mathrel{\dot\subseteq} B$ if $nA \subseteq A \cap B$ for some $n \geqq 1$, and $A \doteq B$ if $A \mathrel{\dot\subseteq} B$ and $B \mathrel{\dot\subseteq} A$. Evidently $A \doteq B$ if and only if $nA \subseteq B$ and $nB \subseteq A$ for some $n \geqq 1$. The relation $\doteq$ is clearly an equivalence and $\mathrel{\dot\subseteq}$ defines a partial ordering $\leqq$ of the set $\mathcal{G}$ of $\doteq$ equivalence classes. Since $A \doteq B$ obviously implies $A \sim B$, if $\sigma, \bar{\sigma} \in \mathcal{G}$, we can define $\sigma \sim \bar{\sigma}$ if $A \sim B$ for all $A \in \sigma$ and $B \in \bar{\sigma}$.

LEMMA 5.16. *If $A \doteq B$, then $\delta_p(A) = \delta_p(B)$ for all primes p.*

Proof. Let $nA \subseteq B$ and $nB \subseteq A$ with $n \geqq 1$. Then $nA^{(p)} = Z^{(p)}(nA) \subseteq Z^{(p)}B = B^{(p)}$. Thus

$$\delta_p(B) = d(B^{(p)}) \supseteq d(nA^{(p)}) = d(A^{(p)}) = \delta_p(A).$$

Similarly, $\delta_p(A) \supseteq \delta_p(B)$.

If ϕ is a linear transformation of V, then $\phi \otimes \mathrm{id}\colon V \otimes R^{(p)} \to V \otimes R^{(p)}$ is an $R^{(p)}$-linear transformation of $V^{(p)}$. We denote this mapping by $\phi^{(p)}$ and call it the transformation induced by ϕ.

COROLLARY 5.17. *If A and B are quasi-isomorphic, full subgroups of V, then there is a nonsingular linear transformation ϕ of V such that $\phi^{(p)}\delta_p(A) = \delta_p(B)$ for all primes p.*

Proof. Let ϕ be a monomorphism of A into B such that $nB \subseteq \phi A \subseteq B$ for some $n \geqq 1$ (so that $\phi A \doteq B$). By 2.4, ϕ extends to an isomorphism of $A^* = V$ on $B^* = V$, and clearly $\phi^{(p)}(\delta_p(A)) = \delta_p(\phi A) = \delta_p(B)$ by 5.16.

We have defined $\delta(A)$, the q.d. invariant of A in Definition 1.8.

DEFINITION 5.18. *If σ is in the set $\mathcal{G}$ of $\doteq$ classes, define $\delta(\sigma) = \delta(A)$, where $A \in \sigma$. Two q.d. invariants δ and $\bar{\delta}$ are called similar if there is a nonsingular linear transformation ϕ of V such that $\phi^{(p)}\delta_p = \bar{\delta}_p$ for all p.*

By 5.16, the definition of $\delta(\sigma)$ is unambiguous. By 5.17, if A and B are quasi-isomorphic full subgroups of V, then $\delta(A)$ and $\delta(B)$ are similar. The relation of similarity is easily seen to be an equivalence. Indeed, this follows immediately from the observation that if ϕ and ψ are nonsingular linear transformations of V, then $(\phi\psi)^{(p)} = \phi^{(p)}\psi^{(p)}$ and $(\phi^{-1})^{(p)} = (\phi^{(p)})^{-1}$.

DEFINITION 5.19. *Let δ be a q.d. invariant (see Definition 1.8). Suppose X is any basis of V. Define*

(i) $N_p^X(\delta) = Z^{(p)}[X] + \delta_p$,

(ii) $M_p^X(\delta) = V \cap N_p^X(\delta)$,

(iii) $A^X(\delta) = \bigcap_p M_p^X(\delta)$.

Note that $X \subseteq A^X(\delta)$, so $Z[X] \subseteq A^X(\delta) \subseteq V$ and $A^X(\delta)$ is a full subgroup of V.

LEMMA 5.20. *If X and Y are any two bases of V, then $A^X(\delta) \doteq A^Y(\delta)$.*

Proof. Choose $n \geqq 1$ so that $nx_i \in Z[Y]$ for all $x_i \in X$. Then $nZ^{(p)}[X] \subseteq Z^{(p)}[Y]$ for all p, and consequently $nA^X(\delta) \subseteq A^Y(\delta)$. Similarly, $mA^Y(\delta) \subseteq A^X(\delta)$ for some $m \geqq 1$.

LEMMA 5.21. *If δ is similar to $\bar{\delta}$, and if X and Y are bases of V, then $A^X(\delta) \sim A^Y(\bar{\delta})$.*

Proof. Let ϕ be a nonsingular linear transformation of V such that $\phi^{(p)}\delta_p = \bar{\delta}_p$ for all p. Let $W = \phi(X)$. Then W is a basis of V, and

$$\phi^{(p)}Z^{(p)}[X] = Z^{(p)}[W].$$

Hence ϕ maps $A^X(\delta)$ isomorphically on $A^W(\bar{\delta})$. By 5.20, $A^X(\delta) \cong A^W(\bar{\delta}) \doteq A^Y(\bar{\delta})$. Thus, $A^X(\delta) \sim A^Y(\bar{\delta})$.

Definition 5.22. *Let $\delta \in \mathfrak{L}$. Define $\sigma(\delta)$ to be the $\doteq$ class containing the group $A^X(\delta)$, where X is any basis of V.*

By 5.20, $\sigma(\delta)$ depends only on δ, not on X. For the remainder of this section, we simplify our notation by writing N_p^X, M_p^X, and A^X instead of $N_p^X(\delta)$, $M_p^X(\delta)$, and $A^X(\delta)$ respectively.

Lemma 5.23. $(A^X)^{(p)} = N_p^X$.

Proof. By definition $N_p^X = Z^{(p)}[X] + \delta_p$, $A^X \subseteq N_p^X$, and N_p^X is a $Z^{(p)}$-module, so $Z^{(p)}A^X \subseteq N_p^X$. On the other hand, $Z[X] \subseteq A^X$, so $Z^{(p)}[X] \subseteq Z^{(p)}A^X$. It suffices to show $\delta_p \subseteq Z^{(p)}A^X$. If $y \in \delta_p$, we can write $y = p^{-t}(\alpha_1 x_1 + \cdots + \alpha_n x_n)$, where $X = \{x_1, \cdots, x_n\}$ and $\alpha_i \in Z^{(p)}$. Choose $a_i \in Z$ and $\beta_i \in Z^{(p)}$, so that $\alpha_i = a_i + p^t\beta_i$ for all i. Then

$$y = p^{-t}(\sum a_i x_i) + \sum \beta_i x_i .$$

Since $X \subseteq A^X$, it follows that $\sum \beta_i x_i \in Z^{(p)}A^X$. Also,

$$p^{-t}(\sum a_i x_i) = y - \sum \beta_i x_i \in (\delta_p + Z^{(p)}[X]) \cap V = M_p^X.$$

Moreover, if $q \neq p$, then $p^{-t}a_i \in Z^{(q)}$, so $p^{-t}(\sum a_i x_i) \in Z^{(q)}[X] \cap M_q^X$. Thus

$$p^{-t}(\sum a_i x_i) \in \bigcap_{q\neq p} M_q^X \cap M_p^X = A^X \subseteq Z^{(p)}A^X,$$

and finally $y \in Z^{(p)}A^X$.

Corollary 5.24. *A^X is a q.d. group.*

Proof. $Z[X]$ is a free full subgroup of A^X. By 5.12 and 5.23,

$$(A^X/Z[X])_p \cong (A^X)^{(p)}/Z^{(p)}[X] = (\delta_p + Z^{(p)}[X])/Z^{(p)}[X] \cong \delta_p/(\delta_p \cap Z^{(p)}[X]),$$

which is the homomorphic image of a divisible group and therefore divisible. Since this is true for all p, A^X is a q.d. group.

The correspondence established in the following theorem yields Theorem 1.9.

Theorem 5.25. *The mappings $\sigma \to \delta(\sigma)$ and $\delta \to \sigma(\delta)$ are inverse, order-preserving correspondences between the lattice $\mathfrak{L}$ of all q.d. invariants and the set $\mathcal{G}$ of all $\doteq$ equivalence classes of full, q.d. subgroups of V. Moreover $\sigma \sim \bar{\sigma}$ if and only if $\delta(\sigma)$ is similar to $\delta(\bar{\sigma})$.*

Proof. By 5.24 and 5.5, the $\doteq$ class $\sigma(\delta)$ consists of full q.d. groups. If $\sigma_1 \leqq \sigma_2$ in $\mathcal{G}$, and if $A \in \sigma_1$, $B \in \sigma_2$, then $A \cap B \in \sigma_1$. Consequently,

$$\delta_p(\sigma_1) = \delta_p(A \cap B) \subseteq \delta_p(B) = \delta_p(\sigma_2)$$

for all p. Thus $\delta(\sigma_1) \leqq \delta(\sigma_2)$. If $\delta_1 \leqq \delta_2$ in $\mathfrak{L}$, then clearly $A^X(\delta_1) \subseteq A^X(\delta_2)$ for any basis X of V. Thus $\sigma(\delta_1) \leqq \sigma(\delta_2)$. We show next that $\sigma(\delta(\sigma)) = \sigma$ when σ is a $\doteq$ class of a full q.d. subgroup A of V. By 5.6 ,there is a maximal independent set X in A such that $A/Z[X]$ is divisible. Since A is full, X is a basis of V. By 5.14,

$$A^{(p)} = \delta_p(A) + Z^{(p)}[X] = N_p^X(\delta(A)).$$

Hence

$$M_p^X(\delta(A)) = A^{(p)} \cap V = (R_p A + Z^{(p)}[X]) \cap V$$
$$= R_p A + (Z^{(p)}[X] \cap V) = R_p A + R_p Z[X] = R_p A$$

by 5.12. Finally, by using 5.10,

$$A^X(\delta(A)) = \bigcap_p R_p A = A.$$

Thus, $\sigma(\delta(\sigma)) = \sigma(\delta(A))$ is the $\doteq$ class of A, namely σ. Now suppose $\delta \in \mathfrak{L}$. Let X be any basis of V. Thus $\sigma(\delta)$ is the $\doteq$ class of $A^X(\delta)$. By 5.23,

$$(A^X)^{(p)} = N_p^X = \delta_p + Z^{(p)}[X].$$

Hence $(\delta(\sigma(\delta)))_p = d(Z^{(p)}[X] + \delta_p) = \delta_p$. Indeed, δ_p is a divisible subgroup of $Z^{(p)}[X] + \delta_p$, and

$$(Z^{(p)}[X] + \delta_p)/\delta_p \cong Z^{(p)}[X]/(Z^{(p)}[X] \cap \delta_p)$$

is a finitely generated $Z^{(p)}$-module, and hence reduced (since any factor module of $Z^{(p)}$ is either $Z^{(p)}$ or a finite cyclic group). Finally $\sigma \sim \bar{\sigma}$ if and only if $\delta(\sigma)$ is similar to $\delta(\bar{\sigma})$ by 5.17, 5.21, and what we have just shown.

Remark. The proof establishes somewhat more than is stated, namely, every full q.d. group in V is of the form $A^X(\delta(A))$ for a suitable choice of X.

To conclude this section, we interpret the decomposability of a full subgroup A of V in terms of the q.d. invariant $\delta(A)$. We will say that a group A is *quasi-decomposable* if $A \sim B \oplus C$, where B and C are groups, neither of which is quasi-isomorphic to the zero group (i.e., of bounded order). If A is not quasi-decomposable, then we say, following Jónsson [11], that A is *strongly indecomposable.*

LEMMA 5.26. *Let A be a full subgroup of V. Then A is quasi-decomposable if and only if nonzero subspaces U and W exist in V such that $V = U \oplus W$ and*

$$\delta_p(A) = \delta_p(A) \cap U^{(p)} \oplus \delta_p(A) \cap W^{(p)}$$

for all primes p.

Proof. Suppose A is quasi-decomposable. Then clearly A contains independent subgroups B and C such that $B \oplus C$ has finite index in A. Let $U = RB$, $W = RC$. Then $V = U \oplus W$. Moreover, if $n \geqq 1$ is such that $nA \subseteq B \oplus C$, then

$$nA^{(p)} \subseteq (B \oplus C)^{(p)} = B^{(p)} \oplus C^{(p)} \subseteq A^{(p)}.$$

Therefore

$$\delta_p(A) = d(A^{(p)}) \supseteq d(B^{(p)} \oplus C^{(p)}) = d(B^{(p)}) \oplus d(C^{(p)})$$
$$= \delta_p(B) \oplus \delta_p(C) \supseteq d(nA^{(p)}) = d(A^{(p)}) = \delta_p(A).$$

Since $U^{(p)} \supseteq \delta_p(B)$ and $U^{(p)} \cap \delta_p(C) = 0$, the modular law gives $\delta_p(B) = \delta_p(A) \cap U^{(p)}$. Similarly, $\delta_p(C) = \delta_p(A) \cap W^{(p)}$. To prove the converse, note that by Theorem 1.9, full q.d. subgroups $B \subseteq U$ and $C \subseteq W$ exist such that $\delta_p(B) = \delta_p(A) \cap U^{(p)}$ and $\delta_p(C) = \delta_p(A) \cap W^{(p)}$ for all p. By the first part of the argument and our hypothesis,

$$\delta_p(B \oplus C) = \delta_p(B) \oplus \delta_p(C) = \delta_p(A) \cap U^{(p)} \oplus \delta_p(A) \cap W^{(p)} = \delta_p(A)$$

for all p. Hence, by 1.9 again, $A \doteq B \oplus C$, and $A \sim B \oplus C$.

COROLLARY 5.27. *Let A be a full subgroup of V such that for some prime p, $\delta_p(A)$ is one-dimensional over $R^{(p)}$. Assume that for this p and for some basis $\{x_1, \cdots, x_n\}$ of V, $\delta_p(A)$ contains $\alpha_1 x_1 + \cdots + \alpha_n x_n$ where the p-adic numbers $\alpha_1, \cdots, \alpha_n$ are rationally independent. Then A is strongly indecomposable.*

Proof. Suppose otherwise. By 5.26, $V = U \oplus W$, where U and W are nonzero subspaces and

$$\delta_p(A) = \delta_p(A) \cap U^{(p)} \oplus \delta_p(A) \cap W^{(p)}.$$

Since $\delta_p(A)$ is one-dimensional, either $\delta_p(A) \subseteq U^{(p)}$, or $\delta_p(A) \subseteq W^{(p)}$. Thus there exist $y_1, \cdots, y_r$ in V, $\beta_1, \cdots, \beta_r$ in $R^{(p)}$ with $r < n$ such that

$$\alpha_1 x_1 + \cdots + \alpha_n x_n = \beta_1 y_1 + \cdots + \beta_r y_r .$$

Let $y_i = \sum_{j=1}^{n} c_{ij} x_j$. Then $\alpha_j = \sum_{i=1}^{r} c_{ij} \beta_i$. Since $r < n$, there is a non-trivial rational solution $(d_1, \cdots, d_n)$ of $\sum_{j=1}^{n} c_{ij} d_j = 0$. But then $\sum_{j=1}^{n} d_j \alpha_j = 0$, contrary to the assumed rational independence.

6. Quotient-divisible rings

Now we resume the study of torsion-free rings, making use of the results obtained in the last section. Our notation and viewpoint is a continuation of that introduced in Section 5. Thus we will be concerned with full subrings A of a rational algebra T. It follows that T is the algebra type of A.

Throughout this section, T is a rational algebra of finite order with an identity element. If K is a subfield of the center of T and C is a subring of K, we have defined a C-basis of T over K (Definition 1.11). Note that if C is a full subring of K, and if X is any basis of T relative to K, then there is an integer $n \geqq 1$ such that $nX = \{nx \mid x \in X\}$ is a C-basis of T over K. A basis of T relative to R will be called a basis of T.

LEMMA 6.1. *If K and F are subfields of the center of T with $F \subseteq K$, and if X is a basis of T relative to K and Y is a basis of K relative to F, then*

$$XY = \{x_i y_j \mid x_i \in X, y_j \in Y\}$$

is a basis of T relative to F.

Proof. If $\sum_{i,j} a_{ij}\, x_i\, y_j = 0$ with $a_{ij} \in F$, then since all y_i belong to the center of T and the set X is independent over K, all the sums $\sum_j a_{ij}\, y_j$ are zero. Therefore all a_{ij} are zero. Clearly XY spans T over F.

COROLLARY 6.2 *If $X = \{x_1, \cdots, x_n\}$ is a basis of T over K, then X is also a basis of $T^{(p)}$ over $K^{(p)} = K \otimes R^{(p)}$.*

Proof. If Y is a basis of K, then XY is a basis of T. By the definition of $T^{(p)}$, XY is also a basis of $T^{(p)}$ over $R^{(p)}$, and Y is a basis of $K^{(p)}$ over $R^{(p)}$. Thus X is a basis of $T^{(p)}$ over $K^{(p)}$.

Proof of Theorem 1.10. Clearly $A^{(p)} = Z^{(p)}A$ is a subring of $T^{(p)}$. Suppose $y \in \delta_p(A) = d(A^{(p)})$ and $z \in T^{(p)}$. Then $p^t z \in A^{(p)}$ for some t, since A is full in T and $R_p \subseteq Z^{(p)}$. Also, for any k, $p^{-(k+t)}y \in d(A^{(p)})$ by divisibility. Hence $p^{-k}zy \in A^{(p)}$ for arbitrary k. Thus $zy \in d(A^{(p)}) = \delta_p(A)$. Similarly, $yz \in \delta_p(A)$. Therefore $\delta_p(A)$ is an ideal. To prove the converse, we will show that for any Z-basis X of T, the group $A^X(\delta)$ is a subring of T. Note that since X is a Z-basis, $Z[X]$ is a subring of T, and $Z^{(p)}[X] = Z^{(p)}Z[X]$ is a subring of $T^{(p)}$. Since δ_p is an ideal by assumption,

$$\begin{aligned} N_p^X(\delta)N_p^X(\delta) &= (Z^{(p)}[X] + \delta_p)(Z^{(p)}[X] + \delta_p) \\ &= Z^{(p)}[X]Z^{(p)}[X] + \delta_p\, Z^{(p)}[X] + Z^{(p)}[X]\delta_p + \delta_p\, \delta_p \\ &\subseteq Z^{(p)}[X] + \delta_p = N_p^X(\delta). \end{aligned}$$

Hence, $N_p^X(\delta)$ is a subring of $T^{(p)}$. Consequently, $M_p^X(\delta) = N_p^X(\delta) \cap T$ is a subring of T, and finally $A^X(\delta) = \bigcap_p M_p^X(\delta)$ is also a subring of T. Suppose A and B are full q.d. subrings of T such that $A \approx B$. Then subrings of finite index $C \subseteq A$ and $D \subseteq B$ exist, together with a ring isomorphism ϕ of C on D. The extension ϕ^* of ϕ to T is an automorphism by 2.4. Moreover, by 5.16,

$$\phi^{*(p)}\delta_p(A) = \phi^{*(p)}\delta_p(C) = \delta_p(D) = \delta_p(B).$$

Conversely, let ϕ be an automorphism of T such that $\phi^{(p)}\delta_p(A) = \delta_p(B)$ for all p. Choose a Z-basis X of T and let $Y = \phi X$. Then Y is also a Z-basis of T. Thus, $A^X(\delta(A))$ and $A^Y(\delta(B))$ are subrings of T, and ϕ is an isomorphism of $A^X(\delta(A))$ on $A^Y(\delta(B))$. By Theorem 1.9, $A \doteq A^X(\delta(A))$, $B \doteq A^Y(\delta(B))$. Thus,

$$A \approx A^X(\delta(A)) \cong A^Y(\delta(B)) \approx B.$$

(Note that $C \doteq D$ implies $C \approx D$ for subrings of T, since $C \cap D$ has finite index in both C and D.)

COROLLARY 6.3. *There is a one-to-one correspondence between the $\doteq$ classes of full q.d. subrings of T and the q.d. invariants δ for which every δ_p is an ideal of $T^{(p)}$.*

Proof. We use Theorem 1.10 and Theorem 5.25.

In the remainder of this section we will use Theorem 1.10 to complete our reduction of rings of simple algebra type to rings of field type. Recall the definition of the subring $C[X]$ of T given in 1.11.

LEMMA 6.4. *Let K be a subfield of the center of the rational algebra T which contains the identity of T; let C and $\bar{C}$ be full subrings of K; let X be a C-basis and $\bar{X}$ a $\bar{C}$-basis of T over K; finally let A be a subring of T.*

(i) *If $C \doteq \bar{C}$, then $C[X] \doteq \bar{C}[\bar{X}]$.*

(ii) *If $A \doteq C[X]$, then $C \doteq A \cap K$.*

(iii) *If $A \approx C[X]$, then $A \doteq \bar{C}[\bar{X}]$ where $C \cong \bar{C}$.*

Proof. The verification of (i) is routine, and we omit it. To prove (ii), let $\bar{X}$ be a C-basis of T over K such that a multiple of the identity element of T is in $\bar{X}$, say $n \cdot 1 \in \bar{X}$. Then by (i), $A \doteq C[X] \doteq C[\bar{X}]$, and hence $A \cap K \doteq C[\bar{X}] \cap K = nC \doteq C$. To prove (iii), note that there is an isomorphism ϕ of a subring of finite index of $C[X]$ onto a subring of finite index of A. Thus for some $n \geqq 1$, $\phi nC[X]$ is a subring of finite index of A. By Lemma 2.4, ϕ extends to an automorphism ϕ^* of T, and $\phi nC[X] = \phi^* nC[X] = n(\phi^* C)[\phi^* X]$. Thus $A \doteq (\phi^* C)[\phi^* X]$ where $\phi^* C \cong C$.

It follows from 6.4 (ii) that if $A \doteq C[X]$, then C is uniquely determined up to $\doteq$ by A and K. By 6.4 (ii) and (iii), if $A \approx C[X]$, then $C \cong \bar{C} \doteq A \cap K$, so that $C \approx A \cap K$. In this case C is determined up to $\approx$ by A and K. This remark justifies the following terminology.

DEFINITION 6.5. *A full subring A of T is said to be induced from K, where K is a subfield of the center of T containing the identity of T, if $A \doteq (A \cap K)[X]$, where X is an $(A \cap K)$-basis of T over K.*

It follows from 6.4 that A is induced from K if and only if $A \approx C[X]$, where C is a full subring of K and X is a C-basis of T over K. When $A \doteq C[X]$, we say C *induces* A.

If A is induced by C, then A is determined up to quasi-isomorphism by C, and the structure of T, considered as an algebra over K. Because the theory of simple rational algebras has been so thoroughly worked out (see [1, Chapter XI] and [8, Teil VII]), the result contained in Theorem 1.12 represents a substantial simplication of the theory of torsion-free rings of simple algebra type.

LEMMA 6.6. *Let K be a subfield of the center of the rational algebra T which contains the identity of T, and let A be a full subring of T. Then there exists an $(A \cap K)$-basis X of T over K such that $X \subseteq A$ and $(A \cap K)[X]$ is a subring of A. If A is induced from K, then $(A \cap K)[X]$ has finite index in A.*

Proof. Since A is full in T, $A \cap K$ is full in K, and there is a basis X of T over K with the stated properties. Then since $A \cap K$ is contained in the center of T and X is an $(A \cap K)$-basis, $(A \cap K)[X]$ is a subring of A. If $A \doteq (A \cap K)[X]$, then $nA \subseteq (A \cap K)[X]$ for some $n \geqq 1$, and since A has finite rank, $A/(A \cap K)[X]$ is finite.

LEMMA 6.7. *Let K be a subfield of the center of the rational algebra T which contains the identity of T. Let A be a full q.d. subring of T, and B a full subring of K. Then B induces A if and only if $\delta_p(B)$ generates $\delta_p(A)$ for all p (that is, $\delta_p(A) = T^{(p)}\delta_p(B)$).*

Proof. Let $\bar{\delta}_p = T^{(p)}\delta_p(B)$ for all p. Let Y be a Z-basis of K, and let $X = \{x_1, \cdots, x_r\}$ be a $(B \cap Z[Y])$-basis of T over K. Then XY is a Z-basis of T by 6.1. Moreover, by 6.2 and 1.10

$$\bar{\delta}_p = \delta_p(B)x_1 + \cdots + \delta_p(B)x_r .$$

Again by 6.2 and 1.10,

$$\begin{aligned} A^{XY}(\bar{\delta}) &= \textstyle\bigcap_p [(\bar{\delta}_p + Z^{(p)}[XY]) \cap T] \\ &= (\textstyle\bigcap_p [(\delta_p(B) + Z^{(p)}[Y]) \cap K])x_1 \oplus \cdots \oplus (\textstyle\bigcap_p [(\delta_p(B) + Z^{(p)}[Y]) \cap K)x_r \\ &= (A^Y(\delta(B)))[X] \doteq B[X]. \end{aligned}$$

Assume $A \doteq B[X]$. Then $A \doteq A^{XY}(\bar{\delta})$, and therefore $\delta(A) = \delta(A^{XY}(\bar{\delta})) = \bar{\delta}$ by 1.9. Conversely, if $\delta(A) = \bar{\delta}$, then $B[X] \doteq A^{XY}(\delta(A)) \doteq A$. This proves the lemma.

COROLLARY 6.8. *Let A be a full q.d. subring of T. Then A is induced from K if and only if there is an ideal $\bar{\delta}_p$ of $K^{(p)}$ such that $\delta_p(A) = T^{(p)}\bar{\delta}_p$ for each p.*

Proof. If such an ideal exists, by 1.10, there is a full subring B of K such that $\delta_p(B) = \bar{\delta}_p$ for all primes p. By 6.7, B induces A. Conversely, if $A \doteq (A \cap K)[X]$, then $A \cap K$ induces A, and $\delta_p(A \cap K) = \delta_p$ by 6.7.

THEOREM 6.9. *Let A be a full subring of the simple rational algebra T with center F. Then for each prime p, there exists a unique idempotent e_p in $F^{(p)}$ such that $\delta_p(A) = e_p T^{(p)}$. Moreover, A is induced from a subfield K of F if and only if $e_p \in K^{(p)}$ for all p.*

Proof. By standard theorems on associative algebras (in particular [10, p. 115], [8, p. 7], and [2, p. 29]), $T^{(p)} = T \otimes R^{(p)}$ is a semisimple $R^{(p)}$-algebra with center $F^{(p)}$, and the two-sided ideal $\delta_p(A)$ has a unique idempotent generator e_p belonging to $F^{(p)}$. If $e_p \in K^{(p)}$ where K is a subfield of F, then

$$\delta_p(A) = T^{(p)}e_p = T^{(p)}(K^{(p)}e_p) = T^{(p)}\bar{\delta}_p ,$$

where $\bar{\delta}_p = K^{(p)}e_p$ is an ideal of $K^{(p)}$. Consequently A is induced from K by 6.8. Conversely, if A is induced from K, then by 6.8, $\delta_p(A) = T^{(p)}\bar{\delta}_p$, where $\bar{\delta}_p$ is an ideal of $K^{(p)}$. Hence, $\bar{\delta}_p = K^{(p)}\bar{e}_p$, where $\bar{e}_p$ is an idempotent of $K^{(p)}$. Therefore

$$\delta_p(A) = T^{(p)}K^{(p)}\bar{e}_p = T^{(p)}\bar{e}_p ,$$

and by uniqueness $e_p = \bar{e}_p \in K^{(p)}$.

The proof of Theorem 1.12 is now complete since by 6.9, A is induced from F, and the result follows from Lemma 6.6.

Proof of Theorem 1.13. Suppose A admits a multiplication of type T. We may assume that A is (the additive group of) a full subring of T. By Theorem 1.12, A contains a subring of finite index which is of the form $C_1 \oplus \cdots \oplus C_r$, where $C_i = Cx_i$ with C the center of A and $x_i \neq 0$ in A. Since T is simple and C is in the center, the mapping $c \to cx_i$ is an isomorphism of C on C_i. Moreover $C^* = RC = F$, so C is a ring of algebra type F. Conversely, if $A \sim C_1 \oplus \cdots \oplus C_r$, $C_i \cong C$, and C admits a multiplication of algebra type F, then A admits a multiplication of algebra type T. For if X is a C-basis of T over F, then $C[X]$ is a full subring of T which is isomorphic as a group to $C_1 \oplus \cdots \oplus C_r$. Thus by 2.7, A admits a multiplication of algebra type T.

COROLLARY 6.10. *If T is a central simple rational algebra of order r, then a torsion-free group A admits a multiplication of algebra type T if and only if A is quasi-isomorphic to a direct sum of r isomorphic non-nil groups of rank one.*

For if T is central simple, its center is R by definition, and a torsion-free group admits a multiplication of algebra type R if and only if it is rank one and non-nil [5]. We will show in Section 9 that "quasi-isomorphic" can be replaced by "isomorphic" in 6.10.

LEMMA 6.11. *If K and L are subfields of the center F of the simple rational algebra T, then $(K \cap L)^{(p)} = K^{(p)} \cap L^{(p)}$.*

Proof. Clearly $(K \cap L)^{(p)} \subseteq K^{(p)} \cap L^{(p)}$. Let $X = \{x_1, \cdots, x_r\}$ be a basis of K over $K \cap L$, and $Y = \{y_1, \cdots, y_s\}$ a basis of L over $K \cap L$, such that $x_1 = y_1 = 1$. Then $\{x_1, x_2, \cdots, x_r, y_2, \cdots, y_s\}$ is linearly independent over $K \cap L$. Hence, this set is also linearly independent over $(K \cap L)^{(p)}$ by 6.2. Now suppose $u \in K^{(p)} \cap L^{(p)}$. Then

$$u = \sum_{i=1}^{r} z_i x_i = \sum_{i=1}^{s} w_i y_i, \qquad z_i, w_i \in (K \cap L)^{(p)}.$$

By the independence, $z_i = w_i = 0$ if $i > 1$ and $z_1 = w_1 = u$. Hence

$$u \in (K \cap L)^{(p)}.$$

THEOREM 6.12. *Let A be a ring of algebra type T, where T is a simple rational algebra. Then there is a unique smallest subfield of the center of T from which A is induced.*

Proof. We use 6.9 and 6.11.

We shall call K the *smallest field of definition* of A if A is induced from K, but not from any proper subfield of K. Our results show that the search for rings of semisimple algebra type can be narrowed down to the rings A of field type K where K is the smallest field of definition of A.

7. The automorphisms of rings of field type

In keeping with our point of view we extend the notion of automorphism. The extension is based on the following.

LEMMA 7.1. *Let A be a full subring of the algebraic number field K. Let ϕ be an automorphism of K. Then the following conditions are equivalent.*

(i) $\phi A \doteq A$.

(ii) *A contains a subring B of finite index such that the restriction of ϕ to B is an automorphism.*

(iii) $\phi^{(p)}\delta_p(A) = \delta_p(A)$ *for all primes p.*

Proof. Suppose $\phi A \doteq A$. Then for some $n \geqq 1$, $nA \subseteq \phi A$, and by induction, $n^j A \subseteq \phi^j A$. Let k be the order of ϕ, that is, ϕ^k is the identity automorphism. Define

$$B = A \cap \phi A \cap \cdots \cap \phi^{k-1} A.$$

Then B is a subring of A, and $n^{k-1} A \subseteq B$. Moreover,

$$\phi B = \phi A \cap \phi^2 A \cap \cdots \cap \phi^k A = B.$$

Hence ϕ defines an automorphism of B. Thus (i) implies (ii). By 1.10, (ii) implies

$$\phi^{(p)}\delta_p(A) = \phi^{(p)}\delta_p(B) = \delta_p(B) = \delta_p(A).$$

Also by 1.10, (iii) implies (i).

DEFINITION 7.2. *Let A be a torsion-free ring of algebra type K, where K is an algebraic number field. Let B and B' be subrings of finite index in A, and let ϕ and ϕ' be automorphisms of B and B' respectively. Define $\phi \approx \phi'$ if $\phi \mid B \cap B' = \phi' \mid B \cap B'$. The equivalence classes of automorphisms under the equivalence relation $\approx$ are called quasi-automorphisms of A. The set of quasi-isomorphisms of A will be denoted $\mathfrak{G}_A$.*

This definition, while logically sound and intrinsic, is somewhat cumbersome. We can simplify the notion of quasi-automorphism by making the identification suggested by the next observation.

LEMMA 7.3. *If ϕ and ϕ' are respectively automorphisms of B and B', subgroups of finite index in A, then $\phi \approx \phi'$ if and only if $\phi^* = (\phi')^*$ on A^*. The mapping $\phi \rightarrow \phi^*$ induces a one-to-one correspondence between $\mathfrak{G}_A$ and a subgroup of the automorphism group $\mathfrak{G}$ of K. This subgroup consists of all $\phi \in \mathfrak{G}$ such that $\phi A \doteq A$.*

This lemma is a simple consequence of 2.4 and 7.1. Henceforth $\mathfrak{G}_A$ will be identified with a subgroup of $\mathfrak{G}$, and we will restrict our considerations to the full subrings of a fixed field K. By making this identification, it follows that if $A \doteq B$, then $\mathfrak{G}_A = \mathfrak{G}_B$, and if $A \approx B$, then $\mathfrak{G}_A$ and $\mathfrak{G}_B$ are conjugate subgroups of $\mathfrak{G}$ (by 7.1 and 1.10). This is the reason for considering quasi-automorphisms rather than automorphisms.

In general, $\mathfrak{G}_A$ is a proper subgroup of $\mathfrak{G}$. By 7.1, a necessary and sufficient condition for an automorphism ϕ to belong to $\mathfrak{G}_A$ is $\phi^{(p)}\delta_p(A) = \delta_p(A)$ for all primes p. If $\delta_p(A) = e_p K^{(p)}$ with e_p idempotent, then $\phi^{(p)}\delta_p(A) = \delta_p(A)$ is equivalent by the uniqueness of e_p to $\phi^{(p)} e_p = e_p$. Hence, by 6.8

COROLLARY 7.4. *If ϕ is an automorphism of K which leaves every element of the smallest field of definition of A fixed, then ϕ induces a quasi-automorphism of A.*

The converse of this corollary is true under the assumption that K is a normal field. To prove this fact requires a simple lemma.

LEMMA 7.5. *Let K be a normal algebraic number field, and let F be a subfield of K. Let $\mathfrak{G}_F$ be the group of automorphisms of K which leave all elements of F fixed. Suppose $z \in K^{(p)}$ satisfies $\phi^{(p)}z = z$ for all $\phi \in \mathfrak{G}_F$. Then $z \in F^{(p)}$.*

Proof. Let $\{x_1, \cdots, x_n\}$ be a basis of K, and write $z = \alpha_1 x_1 + \cdots + \alpha_n x_n$, $\alpha_i \in R^{(p)}$. Then for any $\phi \in \mathfrak{G}_F$,

$$z = \phi^{(p)}z = \alpha_1 \phi x_1 + \cdots + \alpha_n \phi x_n .$$

Summing over the r elements ϕ of $\mathfrak{G}_F$ and dividing by r gives

$$z = \alpha_1 w_1 + \cdots + \alpha_n w_n ,$$

where

$$w_i = (1/r)\textstyle\sum_{\phi\in\mathfrak{G}_F} \phi x_i .$$

Clearly, if $\phi \in \mathfrak{G}_F$, then $\phi w_i = w_i$. Hence $w_i \in F$ for all i, and $z \in F^{(p)}$.

THEOREM 7.6. *Let K be a normal algebraic number field. Let A be a full subring of K. Let F be the smallest field of definition of A. Then the group of quasi-automorphisms of A is precisely the group of F-automorphisms of K.*

Proof. Let $\mathfrak{G}_A$ be the group of all quasi-automorphisms of A, considered as a subgroup of the group of automorphisms of K. Let L be the fixed field of $\mathfrak{G}_A$. Then $L \subseteq F$ by 7.4. Suppose $\delta_p(A) = e_p K^{(p)}$, where e_p is idempotent. By 7.1 and the uniqueness of e_p, $\phi^{(p)}e_p = e_p$ for all $\phi \in \mathfrak{G}_A$. Hence, by 7.5, $e_p \in L^{(p)}$. By 6.9, this implies that A is induced from L. Consequently, $L = F$. Therefore $\mathfrak{G}_A$ is the group of F-automorphisms of K.

COROLLARY 7.7. *If A is a ring of algebra type K, where K is an algebraic number field, and if K is the smallest field of definition of A, then $\mathfrak{G}_A$ is the identity group. In particular, A has no nontrivial automorphisms.*

Proof. Let L be an extension of K which is normal. Let $B = A[X]$, where X is an A-basis of L over K. Then it is easy to show by using 6.9 that K is the smallest field of definition of B. If ϕ is an automorphism of K which belongs to $\mathfrak{G}_A$, then ϕ extends to an automorphism of L, and the extension belongs to $\mathfrak{G}_B$, since if e_p is the idempotent generator of $\delta_p(A)$, it is also the idempotent generator of $\delta_p(B) = \delta_p(A)L^{(p)}$, and $\phi^{(p)}e_p = e_p$. Hence, by 7.6, the extension of ϕ is a K-automorphism of L. Thus, ϕ is the identity.

8. Examples of rings of field type

If K is an algebraic number field, the structure of $K^{(p)} = K \otimes R^{(p)}$ can be determined in a variety of ways.

LEMMA 8.1. *Let $K = R(\theta)$, where θ is a root of the rational polynomial $f(X)$ which is irreducible over R. Let*

$$f(X) = f_1(X) \cdots f_g(X)$$

where the $f_i(X)$ are distinct polynomials with coefficients in $R^{(p)}$ which are irreducible over $R^{(p)}$. Then

$$K^{(p)} = K_1 \dotplus \cdots \dotplus K_g ,$$

where

$$K_i = R^{(p)}(\theta_i),$$

with θ_i a root of $f_i(X)$. If δ is an ideal of $K^{(p)}$, then $\delta = K_{i_1} \dotplus \cdots \dotplus K_{i_r}$, $i_1 < \cdots < i_r$. Let $h = f_{i_1} \cdots f_{i_r}$ and $k = f/h$. Let the degree of h be s. Then

$$k(\theta), \quad \theta k(\theta), \quad \cdots, \quad \theta^{s-1}k(\theta)$$

form a basis of δ.

Proof. Let $k_i = f_1 \cdots f_{i-1} f_{i+1} \cdots f_g$. Then the greatest common divisor of $k_1, \cdots, k_g$ is 1, so we can write

$$1 = l_1 k_1 + \cdots + l_g k_g .$$

Thus, for any $m(\theta) \in K^{(p)}$, we have

$$(*) \qquad m(\theta) = m(\theta)l_1(\theta)k_1(\theta) + \cdots + m(\theta)l_g(\theta)k_g(\theta).$$

Note that $k_i(\theta)k_j(\theta) = 0$ if $i \neq j$, since $k_i k_j$ is divisible by f. Thus, by $(*)$,

$$l_i(\theta)k_i(\theta) = (l_i(\theta)k_i(\theta))^2.$$

Hence, $K^{(p)}$ is the direct sum of the ideals K_i generated by the orthogonal idempotents $l_i(\theta)k_i(\theta)$. Let $\theta_i = \theta l_i(\theta)k_i(\theta)$. Then $\theta_i^t = \theta^t l_i(\theta)k_i(\theta)$, and $f_i(\theta_i) = f_i(\theta)l_i(\theta)k_i(\theta) = 0$. Hence $K_i = R^{(p)}(\theta_i)$. (Note that

$$l_i(\theta)k_i(\theta) \neq 0,$$

since $k_i(\theta) = l_i(\theta)[k_i(\theta)]^2$ and $1, \theta, \cdots, \theta^{n-1}$ are linearly independent over $R^{(p)}$.) To prove the last part of the lemma, note that k is the greatest common divisor of $\{k_{i_1}, \cdots, k_{i_r}\}$. Thus, $k = m_1 k_{i_1} + \cdots + m_r k_{i_r}$, and

$$k(\theta) = m_1(\theta)k_{i_1}(\theta)(l_{i_1}(\theta)k_{i_1}(\theta)) + \cdots$$
$$+ m_r(\theta)k_{i_r}(\theta)(l_{i_r}(\theta)k_{i_r}(\theta)) \in K_{i_1} \dotplus \cdots \dotplus K_{i_r} .$$

On the other hand, every k_{i_j} is a multiple of k, so δ is the principal ideal generated by $k(\theta)$. Since $h(\theta)k(\theta) = 0$ and $m(\theta)k(\theta) \neq 0$ if the degree of m is less than s, we conclude that $k(\theta), \theta k(\theta), \cdots, \theta^{s-1}k(\theta)$ is a basis of δ.

COROLLARY 8.2. *Let A be a torsion-free ring of algebra type K, where K is an algebraic number field. Suppose that for some prime p, $\delta_p(A)$ is one-dimensional over $R^{(p)}$. Then A^+ is strongly indecomposable.*

Proof. Let $K = R(\theta)$, where θ is a root of the irreducible rational polynomial $f(X)$. By 8.1 and the assumption that $\delta_p(A)$ is one-dimensional, there are an $\alpha \in R^{(p)}$ and an $R^{(p)}$-polynomial $k(X)$ such that

$$f(X) = (X - \alpha)k(X)$$

and $k(\theta)$ is a basis of $\delta_p(A)$. Let

$$f(X) = X^n + c_1 X^{n-1} + \cdots + c_n$$

and

$$k(X) = X^{n-1} + \gamma_1 X^{n-2} + \cdots + \gamma_{n-1}.$$

Then solving for $\gamma_1, \gamma_2, \cdots, \gamma_{n-1}$ gives

$$\gamma_1 = \alpha + c_1, \quad \gamma_2 = \alpha^2 + c_1 \alpha + c_2, \quad \cdots, \quad \gamma_{n-1} = \alpha^{n-1} + c_1 \alpha^{n-2} + \cdots + c_{n-1}.$$

It follows that $\{\gamma_1, \gamma_2, \cdots, \gamma_{n-1}, 1\}$ is a linearly independent set over R. For otherwise, α would be a root of a nonzero rational polynomial of degree less than n, and this polynomial would then divide $f(X)$, contradicting irreducibility. Consequently, by 5.27, A^+ is strongly indecomposable.

For the application of 8.1, it is useful to have a criterion for the factorization of a rational polynomial in $R^{(p)}$. Such criteria exist when $f(X)$ has integral coefficients. A fairly complete discussion of these can be found in [16, Chapter III]. For our purposes, the following very special result will suffice.

LEMMA 8.3. *Let $f(X)$ be a monic polynomial with coefficients in Z. Let p be a prime which does not divide the discriminant of $f(X)$. Suppose a is an integer such that $f(a) \equiv 0 \bmod p$. Then there exists $\alpha \in R^{(p)}$, congruent to a mod p, such that $f(\alpha) = 0$.*

Proof. Since p does not divide the discriminant of f, the roots of $f(X)$ modulo p are distinct. Thus, Hensel's lemma applies to the factorization $f(X) \equiv (X - a)h(X) \bmod p$ and gives the conclusion.

THEOREM 8.4. *If K is an algebraic number field, then there exists a ring A of algebra type K such that A^+ is strongly indecomposable. In fact there are $2^{\aleph_0}$ such rings, no two of which are quasi-isomorphic.*

Proof. Let $K = R(\theta)$, where θ is the root of the rational monic irreducible polynomial $f(X)$. We can suppose θ is an algebraic integer, so that the coefficients of $f(X)$ are integers. We can also assume $K \neq R$, so $f(X)$ is not a constant polynomial. Then the set of prime divisors of the integers of the form $f(a)$, $a \in Z$, is infinite [14, p. 82]. In particular, there are a prime p and an integer a such that $f(a) \equiv 0 \bmod p$ and p does not divide the discriminant of $f(X)$. If p is such a prime, then $f(X) = (X - \alpha)k(X)$ in $R^{(p)}$ by 8.3. Hence by 8.1, $K^{(p)}$ has a one-dimensional ideal J. For each q.d. invariant δ with the property $\delta_q = 0$ or $K^{(q)}$ if $q \neq p$ and $\delta_p = J$, there is a full subring A of K such that $\delta = \delta(A)$ by 1.10. By 8.2 such a ring is strongly indecomposable. Since there are $2^{\aleph_0}$ nonsimilar q.d. invariants satisfying these conditions, there are $2^{\aleph_0}$ non-quasi-isomorphic strongly indecomposable full subrings of K.

Lemma 8.1 gives some information on the problem of when a torsion-free group will admit a multiplication of field type.

COROLLARY 8.5. *Let $K = R(\theta)$, where θ is a root of the irreducible rational polynomial $f(X)$ of degree n. Then a torsion-free group A admits multiplication of algebra type K if and only if A is a q.d. group of rank n and there is a distinguished basis $x_0, x_1, \cdots, x_{n-1}$ of A^* such that for every prime p, either $\delta_p(A) = 0$, or $\delta_p(A) = A^{*(p)}$, or there is a basis $z_0, \cdots, z_{s-1}$ of $\delta_p(A)$ such that*

$$z_i = \gamma_0 x_i + \gamma_1 x_{i+1} + \cdots + \gamma_{n-s-1} x_{n-s+i-1} + x_{n-s+1}, \quad i = 0, \cdots, s-1,$$

where

$$k_p(X) = \gamma_0 + \gamma_1 X + \cdots + \gamma_{n-s-1} X^{n-s-1} + X^{n-s}$$

is a factor of $f(X)$ with coefficients in $R^{(p)}$.

Proof. The necessity follows from 4.9 and 8.1. Conversely, if such bases exist, then the mapping $x_0 \to 1, x_1 \to \theta, \cdots, x_{n-1} \to \theta^{n-1}$ induces a vector space isomorphism ϕ of A^* on K in such a way that each $\phi^{(p)}\delta_p(A)$ is an ideal of $K^{(p)}$. Consequently, by 1.10, A is quasi-isomorphic to a full subring of K.

In the case $n = 2$, the criterion of 8.5 can be simplified to a reasonably effective test for groups of rank two to admit a multiplication of quadratic field type.

THEOREM 8.6. *Let A be a torsion-free group of rank two. Let $\{x_0, x_1\}$ be an independent pair of elements in A. Let a be a square-free integer. Then A admits a multiplication of algebra type $R(\sqrt{a})$ if and only if A is a q.d. group and there exist rational numbers r and s with $s \neq 0$ such that for every p, either $\delta_p(A)$ is zero or $(A^*)^{(p)}$, or $\delta_p(A)$ is one-dimensional and if $\alpha x_0 + \beta x_1$ is in $\delta_p(A)$, then*

$$\alpha^2 - 2r\alpha\beta + (r^2 - s^2 a)\beta^2 = 0.$$

Proof. Suppose A admits a multiplication of algebra type $R(\sqrt{a})$. Then by 8.5, A is a q.d. group and there exists a basis $\{y_0, y_1\}$ of A^* such that for every prime p, either $\delta_p(A) = 0$ or $\delta_p(A) = (A^*)^{(p)}$, or $\delta_p(A)$ is one-dimensional and there is a $z \in \delta_p(A)$ with $z = \gamma y_0 + y_1$, where $\gamma + X$ is a factor of $X^2 - a$, that is, $\gamma^2 = a$. We can write $y_0 = r_0 x_0 + r_1 x_1$, $y_1 = s_0 x_0 + s_1 x_1$, where r_0, r_1, s_0, s_1 are rational and $r_0 s_1 - r_1 s_0 \neq 0$. Then if $\delta_p(A)$ is one-dimensional, its elements will be $\alpha x_0 + \beta x_1$, where $\alpha = \lambda(\gamma r_0 + s_0)$, $\beta = \lambda(\gamma r_1 + s_1)$ with $\lambda \in R^{(p)}$. A simple computation shows that

$$\alpha^2 - 2r\alpha\beta + (r^2 - s^2 a)\beta^2 = 0,$$

where

$$r = (s_0 s_1 - a r_0 r_1)/(s_1^2 - a r_1^2) \quad \text{and} \quad s = (r_0 s_1 - r_1 s_0)/(s_1^2 - a r_1^2) \neq 0.$$

Since this transformation of variables can be reversed, the argument can be turned around to obtain the converse result.

9. Direct decompositions

The problem considered in this section is that of determining when a quasi-decomposition of a group can be replaced by a direct sum decomposition. The chief tool in the investigation is 9.6 below, a generalization of a theorem due to Baer.

We introduce some standard notation [13; Section 30]. Let $h_p(x, A)$ denote the p-height of the element x in the group A. By definition $0 \leqq h_p(x, A) \leqq \infty$. A function χ on the set of all primes with values in the set $\{\infty, 0, 1, 2, \cdots\}$ is called a characteristic. The characteristic of the element x in A is the function $\chi_A(x)$ defined by $[\chi_A(x)](p) = h_p(x, A)$. Addition and ordering of characteristics is defined componentwise. An equivalence relation is defined on the set of all characteristics by the condition $\chi \approx \psi$ if χ and ψ differ on at most finitely many primes and these differences, if any, are all finite. The equivalence class of a characteristic χ is called its type and is denoted $\bar{\chi}$. In particular, we write $\tau_A(x)$ for $\overline{\chi_A(x)}$. When there is no danger of confusion, we omit reference to A in the notation and write $h_p(x)$, $\chi(x)$, $\tau(x)$ for $h_p(x, A)$, $\chi_A(x)$, and $\tau_A(x)$ respectively. If U is a torsion-free group of rank one, every nonzero element of U has the same type which is designated $\tau(U)$. It is clear that $\chi \approx \chi_1$, $\psi \approx \psi_1$ implies $\chi + \psi \approx \chi_1 + \psi_1$. This observation justifies the definition of sums of types: $\bar{\chi} + \bar{\psi} = \overline{(\chi + \psi)}$. Define $\bar{\chi} \leqq \bar{\psi}$ if there exists $\chi_1 \approx \chi$ and $\psi_1 \approx \psi$ with $\chi_1 \leqq \psi_1$. This relation is a partial ordering of the set of types, and it has the property that $\chi \leqq \psi$ implies $\bar{\chi} \leqq \bar{\psi}$. The following properties of the types of elements in a torsion-free group A are easily proved: $\tau(nx) = \tau(x)$ if n is a nonzero integer; $A \subseteq B$ implies $\tau_A(x) \leqq \tau_B(x)$, and equality holds if A is a pure subgroup of B. If A is a ring,

$$\tau(xy) \geqq \tau(x) + \tau(y);$$

in particular, $\tau(xy) \geqq \tau(x)$ and $\tau(xy) \geqq \tau(y)$.

LEMMA 9.1. *Let A be a torsion-free group, and let A' be a subgroup of A such that $nA \subseteq A'$ for some $n \geqq 1$. Then for any $x \in A'$, $\tau_{A'}(x) = \tau_A(x)$.*

Proof. Since A is torsion-free, $a \to na$ is an isomorphism of A onto nA Thus,

$$\tau_A(x) = \tau_{nA}(nx) \leqq \tau_{A'}(nx) = \tau_{A'}(x) \leqq \tau_A(x).$$

COROLLARY 9.2. *If U is a torsion-free group of rank one, then $A \sim U$ implies $A \cong U$. (See [3].)*

LEMMA 9.3. *Let A be a torsion-free group containing independent subgroups B and C such that $nA \subseteq B + C$ for some $n \geqq 1$. Assume that C is pure in A and that the rank of B is finite. Then $B + C$ has finite index in A.*

Proof. Since C is pure in A, $nA \cap C = nC$. Using this identity and the fact that A is torsion-free gives

$$A/(B + C) \cong nA/(nB + nC) = nA/(nB + nA \cap C)$$
$$= nA/nA \cap (nB + C) \cong (nA + nB + C)/nB + C$$
$$\subseteq (B + nB + C)/(nB + C) \cong B/B \cap (nB + C).$$

Thus, $A/(B + C)$ is a subgroup of a homomorphic image of a group of finite rank. Hence $A/(B + C)$ has finite rank. But it also has bounded order and is therefore finite.

LEMMA 9.4. *Let B and C be independent subgroups of a torsion-free group A. Suppose B' and C' are the smallest pure subgroups of A containing B and C respectively. Then B' and C' are independent. If $nA \subseteq B + C$ for some $n \geqq 1$, then $B \doteq B'$ and $C \doteq C'$.*

Proof. Let $x \in B' \cap C'$. Then for some $m \geqq 1$, $mx \in B$, $mx \in C$; hence $mx \in B \cap C = 0$, and $x = 0$ since A is torsion-free. Also, $nB' + nC' \subseteq nA \subseteq B + C$ implies

$$nB' = nB' + (nC' \cap B') = (nB' + nC') \cap B'$$
$$\subseteq (B + C) \cap B' = B + (C \cap B') = B.$$

Similarly, $nC' \subseteq C$.

THEOREM 9.5. *Let A be a torsion-free group. Let U and C be independent subgroups of A such that $A \doteq U + C$. Assume that* rk $U = 1$ *and that $\tau(U) \leqq \tau(y)$ for all $y \in C$. Then $A = U' \oplus C'$ where $C' \supseteq C$, $C' \doteq C$, and $U' \cong U$. Moreover, if C is pure in A, then $C = C'$.*

Proof. Lemmas 9.4 and 9.2 reduce the proof to the case that both C and U are pure subgroups of A. By 9.3, $A/(U + C)$ is finite. Thus, the theorem will follow by induction if we can prove it when $A/(U + C)$ is cyclic of prime order p. Henceforth assume that this is the case.

(1) If $z \in A$, $z \notin U + C$, and if $pz = x + y$ with $x \in U$, $y \in C$, then $h_p(x) = h_p(y) = 0$. This follows immediately from the purity of U and C.

(2) There is an element $w \in A$, $w \notin U + C$, such that $pw = b + c$, where $b \in U$, $c \in C$, and $h_q(b) \leqq h_q(c)$ for all primes q. To prove this, let $z \in A$, $z \notin U + C$ be arbitrary, and let $pz = x + y$ with $x \in U$, $y \in C$. Then $h_p(x) = h_p(y) = 0$ by (1). From the assumption that $\tau(U) \leqq \tau(y)$, it follows that there is some $b \in U$ such that $\chi(b) \leqq \chi(x)$ and $\chi(b) \leqq \chi(y)$. Since the rank of U is one, there is an integer m such that $x = mb$. Because $h_p(x) = 0$, p cannot divide m. Choose integers u and v so that $um + pv = 1$. Put $w = uz + vb$ and $c = uy \in C$. Since u is prime to p, $w \in A$ and $w \notin U + C$. Also $h_q(b) \leqq h_q(c)$ for all q. Finally, $pw = puz + pvb = u(mb + y) + pvb = b + c$.

(3) Let U' be the smallest pure subgroup of A containing w. Then $U' \cap C = 0$. In fact, $b \neq 0$, so the subgroup of A generated by w is independent of C, and therefore so is U' by 9.4.

(4) $U' + C = A$. To prove this, let $z \in A$. Then $z - kw \in U + C$ for some integer k. Hence, it suffices to prove $U \subseteq U' + C$. Suppose then that z is a nonzero element of U. Since rk $U = 1$, integers m and n exist satisfying $(m, n) = 1$ and $mz = nb$. Thus, m divides b, so, since $h_q(b) \leqq h_q(c)$ for all q, m also divides c in C. That is, there is an element $y \in C$ such that $c = my$. Thus, $mz = nb = n(pw - c) = npw - mny$, or $npw = m(z + ny)$. By the purity of U', it follows that $z + ny \in U'$, and consequently $z \in U' + C$.

(5) $U' \cong U$. For by (3) and (4), $A = U' \oplus C$, so $U' \cong A/C \supseteq (U \oplus C)/C \cong U$. Moreover $p(A/C) \subseteq (U \oplus C)/C$. Hence $U' \sim U$, which implies $U' \cong U$ by 9.2.

Corollary 9.6. *Let A be torsion-free and $U_1, \cdots, U_n, C$ an independent set of subgroups of A with each U_i of rank one and $A \doteq U_1 \oplus \cdots \oplus U_n \oplus C$. Assume that*

$$\tau(U_1) \leqq \tau(U_2) \leqq \cdots \leqq \tau(U_n) \leqq \tau(y)$$

for all $y \in C$. Then $A = U_1' \oplus \cdots \oplus U_n' \oplus C'$, where $U_i' \cong U_i, C' \doteq C$ (and $C' = C$ if C is pure in A).

The corollary is obtained from 9.5 by induction on n. In case $C = 0$, 9.6 follows from the results of Baer [3, Theorem 10.2 and Corollary 3.9]. Baer also shows that the restriction $\tau(U_1) \leqq \tau(U_2) \leqq \cdots \leqq \tau(U_n)$ is essential.

The application of 9.6 to torsion-free rings is based on two simple facts.

Lemma 9.7. *If A is a torsion-free ring of algebra type T, where T is simple, then $\tau(x) = \tau(y)$ for all nonzero x and y in A.*

Proof. Since T is simple, there exist z and w in T such that $zxw = y$. Choose positive integers m and n so that $mz \in A$, $nw \in A$. Then $\tau(y) = \tau(mny) = \tau(mzxnw) \geqq \tau(x)$. Similarly, $\tau(x) \geqq \tau(y)$.

Lemma 9.8. *Let T be a rational algebra of finite order with a left (right) identity and radical $\bar{N}$ such that $T/\bar{N}$ is simple. Let $T = \bar{S} \oplus \bar{N}$ be a Wedderburn decomposition of T with the identity of T in $\bar{S}$. Let A be a ring of algebra type T, and put $S = A \cap \bar{S}$, $N = A \cap \bar{N}$. Then for any nonzero $x \in S$ and any $y \in N$, $\tau(x) \leqq \tau(y)$.*

Proof. Note that S is pure in A. Choose $n \geqq 1$ so that $ne \in A$, where e is the identity of T. Then $ne \in S$, so by 9.7 and the purity of S, $\tau_A(x) = \tau_S(x) = \tau_S(ne) = \tau_A(ne) \leqq \tau_A((ne)y) = \tau_A(ny) = \tau_A(y)$.

Corollary 9.9. *If A is a finite-rank, torsion-free ring of simple algebra type T, whose smallest field of definition is R (in particular, if T is central simple over R), then A is isomorphic as a group to a direct sum of isomorphic non-nil rank-one groups.*

Proof. We use 9.7, 6.6, 6.10, and 9.6.

COROLLARY 9.10. *Let T be a rational algebra with a left (right) identity and radical $\bar{N}$ such that $T/\bar{N}$ is a central simple R-algebra. Let $N = \bar{N} \cap A$, where A is a ring of algebra type T. Then N is a group direct summand of A.*

Proof. If we note that N is a pure subgroup of A, the corollary follows from 9.8, 6.10, and 9.6.

Example 9.11. The study of torsion-free rings of rank two was initiated in [4]. We now consider these rings in the light of our preceding theory. Among the algebras of order two, the only simple ones are the quadratic fields. The groups admitting a multiplication of this algebra type were characterized in 8.6. The only nonsimple, semisimple rational algebra of order two is $R \dotplus R$. By 3.4, a group A admits of this algebra type if and only if $A \sim U_1 \oplus U_2$, where U_1 and U_2 are non-nil rank-one groups. There are four isomorphically distinct algebras of order two with one-dimensional radical [7]. They can be described in terms of a distinguished basis, z_1, z_2 with the following multiplication tables:

	z_1^2	$z_1 z_2$	$z_2 z_1$	z_2^2
I	z_1	0	0	0
II	z_1	z_2	0	0
III	z_1	0	z_2	0
IV	y_1	z_2	z_2	0

By 1.4, a rank-two torsion-free group A which admits any one of the multiplications is quasi-isomorphic to a direct sum $U_1 \oplus U_2$ of two rank-one groups. Moreover, one of these groups, say U_1, is of non-nil type. In cases II, III, and IV, the algebra has a left, right, and two-sided identity respectively. Therefore, by 9.8, $\tau(U_1) \leqq \tau(U_2)$, and $A \cong U_1 \oplus U_2$ by 9.6. Conversely' it is clear that if U_1 and U_2 are rank-one groups and U_1 is non-nil, then $U_1 \oplus U_2$ admits multiplication of the algebra type I. Hence, by 2.7, if $A \sim U_1 \oplus U_2$, then A admits multiplication of algebra type I. If also $\tau(U_1) \leqq \tau(U_2)$, $U_1 \oplus U_2$ admits multiplication of types II, III, and IV also. Thus we have a complete characterization of all rank-two groups which admit a multiplication of mixed algebra type. There are two isomorphically distinct nilpotent algebras of order two, the nil algebra (and every rank-two torsion-free group admits multiplication of this type) and the algebra with a basis z_1, z_2 satisfying the multiplication rules [7]

	z_1^2	$z_1 z_2$	$z_2 z_1$	z_2^2
V	z_2	0	0	0

We close this paper with a discussion of the groups admitting multiplication of algebra type V. Let T be this algebra. Then $T^{(p)}$ is an algebra with precisely three ideals: 0, $T^{(P)}$, $R^{(P)}z_2$. Thus, by 1.10, 5.26, and 9.6, any q.d. group which admits multiplication of algebra type T is a direct sum $U_1 z_1 \oplus U_2 z_2$, U_1, U_2 non-nil subgroups of R, such that $2\tau(U_1) \leqq \tau(U_2)$ (or, since U_1 and U_2 are non-nil, $\tau(U_1) \leqq \tau(U_2)$). Conversely, any such group admits multiplication of algebra type T. Thus, we can determine the q.d. rings of algebra type T. However, there are non-q.d. groups admitting multiplication of algebra type T. For example, let A be the subgroup of $Rz_1 \oplus Rz_2$ generated by z_1 and the set $\{(1/p)z_1 + (1/p^3)z_2 \mid p = 2, 3, 5, \cdots\}$. Then A is closed under the multiplication V. By direct calculation it can be shown that if w_1 and w_2 are any two independent elements in A, and if U_1 and U_2 are the smallest pure subgroups of A containing w_1 and w_2 respectively, then the p-primary component of $A/(U_1 + U_2)$ is not zero for almost all primes p. Hence, A is strongly indecomposable and in particular not a q.d. group.

BIBLIOGRAPHY

1. A. A. ALBERT, *Structure of algebras*, New York, 1939.
2. E. ARTIN, C. NESBITT, AND R. THRALL, *Rings with minimum condition*, Ann Arbor, University of Michigan Press, 1944.
3. R. BAER, *Abelian groups without elements of finite order*, Duke Math. J., vol. 3 (1937), pp. 68–122.
4. R. A. BEAUMONT AND R. J. WISNER, *Rings with additive group which is a torsion-free group of rank two*, Acta Sci. Math. Szeged, vol. 20 (1959), pp. 105–116.
5. R. A. BEAUMONT AND H. S. ZUCKERMAN, *A characterization of the subgroups of the additive rationals*, Pacific J. Math., vol. 1 (1951), pp. 169–177.
6. H. CARTAN AND S. EILENBERG, *Homological algebra*, Princeton, 1956.
7. A. CAYLEY, *On double algebra*, Proc. London Math. Soc., vol. 15 (1884), pp. 185–197.
8. M. DEURING, *Algebren*, Berlin, 1935.
9. L. FUCHS, *Abelian groups*, Budapest, Publishing House of the Hungarian Academy of Sciences, 1958.
10. N. JACOBSON, *The theory of rings*, Mathematical Surveys, no. II, New York, Amer. Math. Soc., 1943.
11. B. JÓNSSON, *On direct decompositions of torsion free Abelian groups*, Math. Scand., vol. 7 (1959), pp. 361–371.
12. A. G. KUROSCH, *Gruppentheorie*, Berlin, Akademie-Verlag, 1953.
13. A. G. KUROSH, *The theory of groups*, translated from the 2nd Russian ed. by K. A. Hirsch, New York, Chelsea, 1955.
14. T. NAGELL, *Introduction to number theory*, New York, 1951.
15. H. PRÜFER, *Untersuchungen über die Zerlegbarkeit der abzählbaren primären Abelschen Gruppen*, Math. Zeitschrift, vol. 17 (1923), pp. 35–61.
16. H. WEYL, *Algebraic theory of numbers*, Princeton, 1940.

UNIVERSITY OF WASHINGTON
SEATTLE, WASHINGTON