DIVISIBLE MODULES

EBEN MATLIS

Introduction. Let $R$ be an integral domain with quotient field $Q$, and let $A$ be a module over $R$. $A$ is said to be a divisible $R$-module, if $rA = A$ for every $r \neq 0 \in R$. An element $x \in A$ is said to be a torsion element of $A$, if there exists $r \neq 0 \in R$ such that $rx = 0$. The set of torsion elements of $A$ is a submodule of $A$ called the torsion submodule of $A$, and we will consistently denote it by $A_T$. We will let $E(A)$ denote the injective envelope of $A$ (see [3]); and $\text{hd}_R A$ will denote the homological dimension of $A$ as an $R$-module.

We will study conditions, some necessary, some sufficient, for the torsion submodule of a divisible module to be a direct summand. These will be related to the condition that $\text{hd}_R Q = 1$, where $Q$ is the quotient field of $R$. We will apply these conditions to show that, if $R$ is a Noetherian integral domain in which prime ideals different from zero are maximal, and if $D$ is a divisible module over $R$, then $D$ is a homomorphic image of an injective $R$-module and $D_T$ is a direct summand of $D$. The same conclusions hold, if we merely assume for an arbitrary integral domain that its quotient field is countably generated as a module over the ring.

1. The torsion submodule. It is easy to see that, if $C$ is an injective module over an integral domain $R$, then its torsion submodule $C_T$ is also an injective $R$-module, and therefore a direct summand. Namely, any homomorphism of an ideal of $R$ into $C_T$ can be extended to a homomorphism of $R$ into $C_T$; but this extension must in fact map $R$ into $C_T$. The following theorem is a generalization of this fact.

Theorem 1.1. Let $R$ be an integral domain and $H$ a homomorphic image of an injective $R$-module. Then $H_T$ is a direct summand of $H$.

Proof. The mapping of a free $R$-module $F$ onto an injective $R$-module $C$ can be extended to a mapping of $E(F)$ onto $C$. We can thus assume that there exists a torsion-free, divisible $R$-module $U$ and an epimorphism $f: U \to H$. Now $H/H_T$, being torsion-free and divisible, is a direct sum of $R$-modules $Q_i$, where $Q_i$ is isomorphic to $Q$ the quotient field of $R$. Let $S_i$ be the inverse image of $Q_i$ under the canonical map $H \to H/H_T$. We will prove that $H_T$ is a direct summand of each $S_i$, and by [2, Lemma 2] this will complete the proof of the theorem.

Presented to the Society, September 3, 1959; received by the editors May 23, 1959.
Let \( y \in S_j - H_T \); then \( R_y \) is a torsion-free submodule of \( S_j \). Choose \( x \in U \) such that \( f(x) = y \). Since \( U \) is a vector space over \( Q \), there exists an \( R \)-submodule \( T_j \) of \( U \) such that \( T_j \subseteq Q \) and \( x \in T_j \). If \( u \neq 0 \in T_j \), there exist \( r, s \in R \) such that \( ru = sx \neq 0 \). Since \( rf(u) = sf(x) = sy \neq 0 \), we have \( f(u) \neq 0 \), and thus \( f(T_j) \cong T_j \subseteq Q \).

Since \( H = \sum_i S_i f(u) = w + z \), where \( w \in \sum_i S_i \) and \( z \in S_j \). Hence \( rw + rz = rf(u) = sy \in S_j \). Thus \( rw \in \sum_i S_i \cap S_j = H_T \). Therefore, \( w \in H_T \subseteq S_j \), and so \( f(u) \in S_j \). This shows that \( f(T_j) \subseteq S_j \). Since \( f(T_j) \cong Q \), we have \( f(T_j) \cap H_T = 0 \) and \( f(T_j) \) maps onto \( Q_j \) under the canonical map \( H \to H/H_T \). Thus \( S_j = H_T \oplus f(T_j) \); and so \( H_T \) is a direct summand of \( H \).

**Theorem 1.2.** Let \( R \) be an integral domain with quotient field \( Q \neq R \). Suppose that \( D_T \) is a direct summand of \( D \) for every divisible \( R \)-module \( D \). Then \( \text{hd}_R Q = 1 \).

**Proof.** Let \( A \) be any \( R \)-module and let \( E = E(A) \). Since \( E \) is an essential extension of \( A \), \( E/A \) is a torsion \( R \)-module. Let \( G \) be any \( R \)-module extension of \( E/A \) by \( Q \). Since both \( Q \) and \( E/A \) are divisible, \( G \) is also divisible. Clearly \( E/A \) is the torsion submodule of \( G \); and thus by assumption \( E/A \) is a direct summand of \( G \). Thus \( \text{Ext}_R^1(Q, E/A) = 0 \) [1, Theorem 14.1.1]. We also have \( \text{Ext}_R^n(Q, E) = 0 \) for \( n > 0 \), since \( E \) is injective. Therefore, from the exact sequence:

\[
\text{Ext}_R^1(Q, E/A) \to \text{Ext}_R^2(Q, A) \to \text{Ext}_R^2(Q, E)
\]

we deduce that \( \text{Ext}_R^2(Q, A) = 0 \). Hence \( \text{hd}_R Q \leq 1 \). Since \( Q \) is not \( R \)-projective, \( \text{hd}_R Q = 1 \).

Over an arbitrary integral domain it is not true that \( D_T \) is a direct summand for every divisible module \( D \). For by the above theorem this would imply that \( \text{hd}_R Q = 1 \). However, I. Kaplansky has shown (unpublished) that \( \text{hd}_R Q = 1 \) for a valuation ring \( R \) if and only if \( Q \) is a countably generated \( R \)-module.

**Theorem 1.3.** Let \( R \) be an integral domain with quotient field \( Q \neq R \), and suppose that \( Q \) is countably generated as a \( R \)-module. Then every divisible \( R \)-module \( D \) is a homomorphic image of an injective \( R \)-module. Thus \( D_T \) is a direct summand of \( D \), and \( \text{hd}_R Q = 1 \).

**Proof.** There exists a countable set of generators \( \{q_n\} \) for \( Q \) over \( R \), and elements \( \{a_{n+1}\} \) of \( R \) such that \( q_1 = 1 \) and \( a_{n+1}q_{n+1} = q_n \). Let \( D \) be a divisible \( R \)-module, and let \( x \neq 0 \in D \). We define a mapping \( f \) from the generators \( \{q_n\} \) to \( D \). Let \( f(1) = x \); then there exists \( x_1 \in D \) such that \( a_{2}x_2 = x \), and we define \( f(q_2) = x_2 \). There exists \( x_3 \in D \) such that \( a_{3}x_3 = x_2 \), and we define \( f(q_3) = x_3 \). We continue in this way and
DIVISIBLE MODULES

define \( f \) on all the generators \( \{ q_n \} \). It is easily verified that \( f \) induces an \( R \)-homomorphism from \( Q \) into \( D \) such that the image contains \( x \). It is now clear that by taking a big enough direct sum \( G \) of copies of \( Q \) we can define an \( R \)-homomorphism of \( G \) onto \( D \).

It should be remarked that if \( R \) is any integral domain and \( S \) a countable, multiplicatively closed subset of \( R \), then it can be easily shown that if \( F \) is a countably generated free \( R \)-module and \( f \) a suitably chosen mapping of \( F \) onto \( RS \), then the kernel of \( f \) is free; and thus \( \text{hd}_R RS \leq 1 \).

2. \( \text{hd}_R Q = 1 \).

**Proposition 2.1.** Let \( R \) be an integral domain with quotient field \( Q \) such that \( \text{hd}_R Q = 1 \). Let \( H \) be an \( R \)-module. Then the following statements are equivalent:

1. \( \text{Ext}_R(Q/R, H) = 0 \).
2. Every \( R \)-homomorphism from \( R \) into \( H \) can be extended to an \( R \)-homomorphism from \( Q \) into \( H \).
3. \( H \) is a homomorphic image of an injective \( R \)-module.

**Proof.** That (1) implies (2) follows immediately from the exact sequence:

\[
\text{Hom}_R(Q, H) \to \text{Hom}_R(R, H) \to \text{Ext}_R^1(Q/R, H).
\]

That (2) implies (3) is trivial. That (3) implies (1) follows from the fact that \( \text{hd}_R Q/R = 1 \).

**Proposition 2.2.** Let \( R \) be an integral domain with quotient field \( Q \) such that \( \text{hd}_R Q = 1 \). Let \( H \) be an \( R \)-module. Then:

1. If \( H \) is a homomorphic image of an injective \( R \)-module, so is \( H_T \).
2. If \( B \) is a submodule of \( H \) and if \( B \) and \( H/B \) are homomorphic images of injective modules, then so is \( H \).

**Proof.**

1. If \( H \) is a homomorphic image of an injective \( R \)-module, then \( H_T \) is a direct summand of \( H \) by Theorem 1.1. Hence \( H_T \) is also a homomorph image of an injective \( R \)-module.

2. Suppose that \( B \) and \( H/B \) are homomorphic images of injective \( R \)-modules. We have an exact sequence:

\[
\text{Ext}_R^1(Q/R, B) \to \text{Ext}_R^1(Q/R, H) \to \text{Ext}_R^1(Q/R, H/B).
\]

By Proposition 2.1 the two end modules are zero, and thus \( \text{Ext}_R^1(Q/R, H) = 0 \). Hence by Proposition 2.1 again, \( H \) is a homomorphic image of an injective \( R \)-module.
DEFINITION. Let $B$ be a module over an integral domain. Then we will say that $B$ is $h$-reduced, if $B$ has no nonzero submodules which are homomorphic images of injective modules.

**Corollary 2.3.** Let $A$ be a module over an integral domain $R$ with quotient field $Q$ such that $\text{hd}_R Q = 1$. Then $A$ has a unique largest submodule $H$ which is a homomorphic image of an injective $R$-module, and $A/H$ is $h$-reduced.

**Proof.** Let $H$ be the sum of all submodules of $A$ which are homomorphic images of injective $R$-modules. It is clear that $H$ is the unique largest submodule of $A$ which is a homomorphic image of an injective $R$-module. Suppose that $B/H$ is a homomorphic image of an injective $R$-module, where $B$ is a submodule of $A$ containing $H$. Then by Proposition 2.2 $B$ is a homomorphic image of an injective $R$-module. Therefore, $B = H$ and $B/H = 0$.

**Proposition 2.4.** Let $R$ be an integral domain with quotient field $Q$ such that $\text{hd}_R Q = 1$. Let $D$ be a divisible module over $R$, and let $H$ be a submodule of $D$ such that $H$ is a homomorphic image of an injective $R$-module. Then $D/H$ is a direct summand of $D$ if and only if $D/T/H$ is a direct summand of $D/H$.

**Proof.** Suppose that $D/T$ is a direct summand of $D$, and let $S$ be a complementary summand of $D/T$ in $D$. Then $D/H \cong D/T/H \oplus S$, and since $D/T/H$ is the torsion submodule of $D/H$, $D/T/H$ is a direct summand of $D/H$. Conversely, suppose that $D/H = D/T/H \oplus G/H$, where $G$ is a submodule of $D$ containing $H$. Now $G/H$ is torsion-free and divisible, hence injective. Thus by Proposition 2.2 and Theorem 1.1 $H$ is a direct summand of $G$. Let $L$ be a complementary summand of $H$ in $G$. Then it is clear that $D = D/T \oplus L$.

**Proposition 2.5.** Let $R$ be an integral domain with quotient field $Q$, and let $T$ be an $h$-reduced torsion $R$-module. Then $\text{Ext}^1_R(Q, T) = 0$ if and only if $T \cong \text{Ext}^1_R(Q/R, T)$.

**Proof.** Since $\text{Hom}_R(Q, T) = 0$, we have an exact sequence:

$$0 \to \text{Hom}_R(R, T) \to \text{Ext}^1_R(Q/R, T) \to \text{Ext}^1_R(Q, T) \to 0.$$  

It follows that if $\text{Ext}^1_R(Q, T) = 0$, then $T \cong \text{Ext}^1_R(Q/R, T)$. Conversely, if $T \cong \text{Ext}^1_R(Q/R, T)$, then the above exact sequence shows that $\text{Ext}^1_R(Q, T)$ is a torsion module. However, $\text{Ext}^1_R(Q, T)$ is torsion-free, and thus $\text{Ext}^1_R(Q, T) = 0$.

**Corollary 2.6.** Let $R$ be an integral domain with quotient field $Q$. 

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
Then the torsion submodule of a divisible $R$-module is always a direct summand if and only if the following two conditions hold:

1. $\text{hd}_R Q = 1$.
2. $T \cong \text{Ext}_R^h(Q/R, T)$, whenever $T$ is an $h$-reduced, torsion, divisible $R$-module.

**Proof.** The necessity follows from Theorem 1.2 and Proposition 2.5; the sufficiency follows from Corollary 2.3 and Propositions 2.4 and 2.5.

**Proposition 2.7.** Let $R$ be an integral domain with quotient field $Q$ such that $\text{hd}_R Q = 1$ and $\text{gl. dim. } R \leq 2$. Let $S$ be any torsion-free $R$-module. Then $\text{hd}_R S \leq 1$. Thus if $A$ is an $R$-module such that $A_T$ is a homomorphic image of an injective $R$-module, then $A_T$ is a direct summand of $A$.

**Proof.** Let $B$ be any $R$-module. Then from the exact sequence:

$$0 \to S \to Q \otimes_R S \to Q/R \otimes_R S \to 0$$

we derive the exact sequence:

$$\text{Ext}_R^2(Q \otimes_R S, B) \to \text{Ext}_R^2(S, B) \to \text{Ext}_R^3(Q/R \otimes_R S, B).$$

Since $\text{hd}_R Q = 1$ and $\text{gl. dim. } R \leq 2$, the two end modules are zero. Thus $\text{hd}_R S \leq 1$, and the rest of the theorem follows immediately.

2. **Krull dimension = 1.**

Throughout this section $R$ will be a Noetherian integral domain with the property that nonzero prime ideals are maximal. We will let $Q$ be the quotient field of $R$ and $K = Q/R$.

**Definition.** Let $A$ be an $R$-module and $M$ a prime ideal of $R$. We will say that $A$ is $M$-primary, if for any $x \neq 0 \in A$, the order ideal of $x$ is an $M$-primary ideal. If $B$ is any $R$-module, and $A$ is the set of all elements of $B$ whose order ideal is $M$-primary (together with the element 0), then $A$ is an $M$-primary $R$-module which we will call the $M$-primary component of $B$.

**Lemma 3.1.** Let $B$ be any torsion $R$-module. Then $B$ is the direct sum of its $M$-primary components, $M$ ranging over the prime ideals of $R$. Furthermore, $B \otimes_R R_M$ is the $M$-primary component of $B$.

**Proof.** Let $\{ M_a \}$ be the collection of nonzero prime ideals of $R$. By [3, Theorem 3.3] $E(B) = \sum_a \oplus E_a$, where $E_a$ is the $M_a$-component of $E(B)$. Let $B_a = B \cap E_a$; then $B_a$ is the $M_a$-component of $B$. Let $x \neq 0 \in B$; then $x = x_1 + \cdots + x_n$, where $x_i \in E_i$. Now $\cap_{i=2}^n M_i \subseteq M_1$;
hence there exists \( s \in \cap M_i \) such that \( s \in M_i \). Then there exists an integer \( k > 0 \) such that \( s^k x_i = 0 \) for \( i = 2, \ldots, n \). Hence \( s^k x = s^k x_1 \).

There are elements \( m \in M \) and \( t \in R \) such that \( 1 = m + ts^k \). There is an integer \( q > 0 \) such that \( m^q x_1 = 0 \). Since \( 1 = m^q + rs^k \), \( r \in R \), we have \( x_1 = rs^k x_1 = rs^k x \in B_1 \). Similarly \( x_i \in B_i \) for \( i = 2, \ldots, n \). Thus \( B = \sum a_i \oplus B_a \).

Let \( M_e \) be a prime ideal of \( R \). Clearly \( B_a \otimes_R R_{M_e} = 0 \), if \( M_a \neq M_e \). Thus \( B \otimes_R R_{M_e} = B \otimes_R R_{M_a} \). It is easily seen that the canonical map \( B_a \to B \otimes_R R_{M_a} \) is an epimorphism. However, since \( B_a \) is \( M_e \)-primary, the kernel of this map is zero. Thus \( B_a = B_a \otimes_R R_{M_e} \), and so \( B \otimes_R R_{M_a} = B_a \).

**Lemma 3.2.** \( \text{hd}_R Q = 1 \).

**Proof.** It is sufficient to prove that \( \text{hd}_R K = 1 \). By Lemma 3.1 \( K = \sum a_i \oplus K_{M_a} \); thus it is sufficient to prove that \( \text{hd}_R K_{M_a} = 1 \). For this it is sufficient to prove that if \( D \) is any divisible \( R \)-module, then \( \text{Ext}_R(K_{M_a}, D) = 0 \). Let \( A \) be any extension of \( D \) by \( K_{M_a} \); then \( A \) is a divisible \( R \)-module. We have \( D = \sum a_i \oplus D_{M_a} \) and \( A = \sum a_i \oplus A_{M_a} \). Clearly \( D_{M_a} = D \cap A_{M_a} \). Hence for \( a \neq v \), we have \( D_{M_a} = A_{M_a} \). Thus we have an exact sequence:

\[
0 \to D_{M_a} \to A_{M_a} \to K_{M_a} \to 0,
\]

and all of the modules and mappings of this sequence are \( R_{M_a} \)-modules and mappings. Thus we can assume that \( R \) is a local ring with a single nonzero prime ideal \( M \).

Take \( s \neq 0 \in M \), and let \( S \) be the multiplicatively closed set consisting of the powers of \( s \). Now \( R_S \subset Q \); on the other hand, the prime ideals of \( R_S \) and the prime ideals of \( R \) not meeting \( S \) are in 1-1 correspondence. Thus \( R_S \) is a field, and \( R_S = Q \). Therefore, \( Q \) is a countably generated \( R \)-module; and thus \( \text{hd}_R Q = 1 \) by Theorem 1.3, or the remark following it.

**Theorem 3.3.** Every divisible \( R \)-module \( D \) is a homomorphic image of an injective \( R \)-module; and thus \( D_T \) is a direct summand of \( D \).

**Proof.** Since \( \text{hd}_R Q = 1 \) by Lemma 3.2, it follows from Proposition 2.2 that we only need to prove that \( D_T \) is a homomorphic image of an injective \( R \)-module. By Lemma 3.1 \( D_T = \sum a_i \oplus D_{T_a} \), where \( D_{T_a} = D_T \otimes_R R_{M_a} \) is a divisible \( R_{M_a} \)-module. As we have seen in Lemma 3.2, \( Q \) is a countably generated \( R_{M_a} \)-module; and thus by Theorem 1.3, \( D_{T_a} \) is a homomorphic image of an injective \( R_{M_a} \)-module. Thus \( D_{T_a} \) is a homomorphic image of an injective \( R \)-module; and therefore, the same is true of \( D_T \).
A CHARACTERIZATION OF ALGEBRAIC NUMBER FIELDS WITH CLASS NUMBER TWO

L. CARLITZ

Let \( Z = \mathbb{Q}(\theta) \) denote an algebraic number field over the rationals with class number \( h \). It is familiar that \( h = 1 \) if and only if unique factorization into prime holds for the integers of \( Z \). For fields with \( h \leq 2 \) we have the following criterion.

**Theorem.** The algebraic number field \( Z \) has class number \( h = 2 \) if and only if for every nonzero integer \( \alpha \in Z \) the number of primes \( \pi_j \) in every factorization

\[
\alpha = \pi_1 \pi_2 \cdots \pi_k
\]

depends only on \( \alpha \).

Suppose first that \( h = 2 \) and consider the factorization into prime ideals

\[
(\alpha) = \mathfrak{p}_1 \cdots \mathfrak{p}_s \mathfrak{r}_1 \cdots \mathfrak{r}_t,
\]

where the \( \mathfrak{p}_j \) are principal ideals while the \( \mathfrak{r}_j \) are not. Then

\[
\mathfrak{p}_j = (\pi_j) \quad (j = 1, \ldots, s).
\]

Since \( h = 2 \), it follows that

\[
\mathfrak{r}_i \mathfrak{r}_j = (\sigma_{ij}) \quad (i, j = 1, \ldots, t);
\]

moreover \( t \) must be even, \( t = 2u \), say. Thus every factorization into primes implied by \( (2) \), for example

Received by the editors August 3, 1959.

\(^1\) Research sponsored by National Science Foundation grant NSF G-9425.