MATH 725 NOTES
MODULES

MARIO L. GUTIERREZ ABED

Basic Properties of Modules

Definition. *Let $\mathcal{R}$ be a commutative ring with identity, whose elements are called scalars. An $\mathcal{R}$-**module** (or a **module** over $\mathcal{R}$) is a nonempty set M, together with two operations. The first operation, called addition and denoted by $+$, assigns to each pair $(u, v) \in M \times M$, an element $u + v \in M$. The second operation, denoted by juxtaposition, assigns to each pair $(r, u) \in \mathcal{R} \times M$, an element $ru \in M$. Furthermore, the following two properties must hold:*

1) *M is an abelian group under addition.*
2) *For all $r, s \in \mathcal{R}$ and $u, v \in M$, we have*

$$\begin{aligned} r(u+v) &= ru + rv \\ (r+s)u &= ru + su \\ (rs)u &= r(su) \\ 1u &= u. \end{aligned}$$

*The ring $\mathcal{R}$ is called the **base ring** of M.* ★

<u>Remark</u>: Note that vector spaces are just special types of modules: a vector space is a module over a field.

Definition. *A **submodule** of an $\mathcal{R}$-module M is a nonempty subset S of M that is an $\mathcal{R}$-module in its own right, under the operations obtained by restricting the operations of M to S.* ★

Theorem 1. *A nonempty subset S of an $\mathcal{R}$-module M is a submodule if and only if it is closed under linear combinations, that is, if*

$$r, s \in \mathcal{R}, \quad u, v \in S \quad \Longrightarrow \quad ru + sv \in S.$$

Theorem 2. *If S and T are submodules of M, then $S \cap T$ and $S + T$ are also submodules of M.*

<u>Remark</u>: When we think of a ring $\mathcal{R}$ as an $\mathcal{R}$-module rather than as a ring, multiplication is treated as scalar multiplication. This has some important implications. In particular, if S is a submodule of $\mathcal{R}$ then it is closed under scalar multiplication, which means that it is closed under multiplication by all elements of the ring $\mathcal{R}$. In other words, S is an ideal of the ring $\mathcal{R}$. Conversely, if $\mathcal{I}$ is an ideal of the ring $\mathcal{R}$, then $\mathcal{I}$ is also a submodule of the module $\mathcal{R}$. Hence, <u>the submodules of the $\mathcal{R}$-module $\mathcal{R}$ are precisely the ideals of the ring $\mathcal{R}$</u>.

Definition. *Let M be an $\mathcal{R}$-module. A submodule of the form*

$$\langle v \rangle = \mathcal{R}v = \{rv \mid r \in \mathcal{R}\}$$

for $v \in M$ is called the ***cyclic submodule*** *generated by v. (It is also the* ***principal ideal*** *generated by v.)* ★

Remark: Of course, any finite-dimensional vector space is the direct sum of cyclic submodules, that is, one-dimensional subspaces. One of our main goals is to show that a finitely generated module over a principal ideal domain has this property as well.

Note: In a vector space V over a field F, singletons $\{v\}$ where $v \neq 0$ are linearly independent. Put another way, $r \neq 0$ and $v \neq 0$ imply $rv \neq 0$. However, in a module, this need not be the case, as we show in the following example:

Example: The abelian group $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ is a $\mathbb{Z}$-module, with scalar multiplication defined by $za = (z \cdot a) \mod n$ for all $n \in \mathbb{Z}$ and $a \in \mathbb{Z}_n$. However, since $na = 0$ for all $a \in \mathbb{Z}_n$, no singleton $\{a\}$ is linearly independent. Indeed, $\mathbb{Z}_n$ has no linearly independent sets. ▲

This example motivates the following definition:

Definition. *Let M be an $\mathcal{R}$-module. A nonzero element $v \in M$ for which $rv = 0$ for some nonzero $r \in \mathcal{R}$ is called a* ***torsion element*** *of M. A module that has no nonzero torsion elements is said to be* ***torsion-free****. If all elements of M are torsion elements then M is a* ***torsion module****. The set of all torsion elements of M, together with the zero element, is denoted by M_{tor}.* ★

Remark: If M is a module over an integral domain, it is not hard to see that M_{tor} is a submodule of M and that M/M_{tor} is torsion-free.

Closely associated with the notion of a torsion element is that of an annihilator:

Definition. *Let M be an $\mathcal{R}$-module. The* ***annihilator*** *of an element $v \in M$ is*

$$\operatorname{ann}(v) = \{r \in \mathcal{R} \mid rv = 0\}$$

and the ***annihilator*** *of a submodule N of M is*

$$\operatorname{ann}(N) = \{r \in \mathcal{R} \mid rN = \{0\}\}$$

where $rN = \{rv \mid v \in N\}$. Annihilators are also called ***order ideals****.*[1] ★

Remark: It is easy to see that $\operatorname{ann}(v)$ and $\operatorname{ann}(N)$ are ideals of $\mathcal{R}$. Clearly, $v \in M$ is a torsion element if and only if $\operatorname{ann}(v) \neq \{0\}$.

Definition. *Let M be an $\mathcal{R}$-module. A subset $\mathcal{B}$ of M is a basis if $\mathcal{B}$ is linearly independent and spans M. An $\mathcal{R}$-module M is said to be* ***free*** *if $M = \{0\}$ or if M has a basis. If $\mathcal{B}$ is a basis for M, we say that M is* ***free on*** *$\mathcal{B}$.* ★

[1] See page 5 to see where the name *order ideal* comes from.

The next example shows that even free modules are not very much like vector spaces. It is an example of a free module that has a submodule that is not free:

Example: The set $\mathbb{Z} \times \mathbb{Z}$ is a free module over itself, using components-wise scalar multiplication

$$(n, m)(a, b) = (na, mb)$$

with basis $\{(1, 1)\}$. However the submodule $\mathbb{Z} \times \{0\}$ is not free since it has no linearly independent elements and hence no basis. ▲

Note: It is not hard to see that any free module over an integral domain is torsion-free. The converse however does not hold, unless we strengthen the hypotheses by requiring that the module be finitely generated:

Theorem 3. *Let M be a torsion-free finitely generated module over a principal ideal domain $\mathcal{R}$. Then M is free. Thus, a finitely generated module over a principal ideal domain is free if and only if it is torsion-free.*

Modules Are Not As Nice As Vector Spaces

Here is a list of some of the properties of modules (over commutative rings with identity) that emphasize the differences between modules and vector spaces:

- A submodule of a module need not have a complement.
- A submodule of a finitely generated module need not be finitely generated.
- There exist modules with no linearly independent elements and hence with no basis.
- A minimal spanning set or maximal linearly independent set is not necessarily a basis.
- There exist free modules with submodules that are not free.
- There exist free modules with linearly independent sets that are not contained in a basis and spanning sets that do not contain a basis.

Remark: Recall also that a module over a noncommutative ring may have bases of different sizes. However, all bases for a free module over a commutative ring with identity have the same size.

Free and Noetherian Modules

Since all bases for a vector space V have the same cardinality, the concept of vector space dimension is well-defined. A similar statement holds for free $\mathcal{R}$-modules when the base ring is commutative (but not otherwise).

Theorem 4. *Let M be a free module over a commutative ring $\mathcal{R}$ with identity. Then we have the following two results:*

i) Any two bases of M have the same cardinality.

ii) The cardinality of a spanning set is greater than or equal to that of a basis.

The previous theorem allows us to define the *rank* of a free module (the term *dimension* is not used for modules in general):

Definition. *Let $\mathcal{R}$ be a commutative ring with identity. The* ***rank*** *of a nonzero free $\mathcal{R}$-module M, denoted $\mathrm{rk}(M)$, is the cardinality of any basis for M. The rank of the trivial module $\{0\}$ is 0.* ★

Recall that if B is a basis for a vector space V over $\mathbb{F}$ then V is isomorphic to the vector space $(\mathbb{F}^B)_0$ of all functions from B to $\mathbb{F}$ that have finite support. A similar result holds for free $\mathcal{R}$-modules. We begin with the fact that $(\mathcal{R}^B)_0$ is a free $\mathcal{R}$-module:

Theorem 5. *Let B be any set and let $\mathcal{R}$ be a ring. The set $(\mathcal{R}^B)_0$ of all functions from B to $\mathcal{R}$ that have finite support is a free $\mathcal{R}$-module of rank $|B|$ with basis $\mathcal{B} = \{\delta_b\}$, where*

$$\delta_b(x) = \begin{cases} 1 & \text{if } x = b, \\ 0 & \text{if } x \neq b. \end{cases}$$

This basis is referred to as the ***standard basis*** *for $(\mathcal{R}^B)_0$.*

Theorem 6. *Let M be an $\mathcal{R}$-module. If B is a basis for M, then M is isomorphic to $(\mathcal{R}^B)_0$.*

Theorem 7. *Two free $\mathcal{R}$-modules (over a commutative ring) are isomorphic if and only if they have the same rank.*

Definition. *An $\mathcal{R}$-module M is said to satisfy the* ***ascending chain condition*** *on submodules if any ascending sequence of submodules*

$$S_1 \subseteq S_2 \subseteq S_3 \subseteq \dots$$

of M is eventually constant. That is, there exists an index k for which

$$S_k = S_{k+1} = S_{k+2} = \dots$$

Modules with the ascending chain condition on submodules are called ***noetherian modules***. ★

Theorem 8. *An $\mathcal{R}$-module M is noetherian if and only if every submodule of M is finitely generated.*

Since a ring $\mathcal{R}$ is a module over itself and since the submodules of the module $\mathcal{R}$ are precisely the ideals of the ring $\mathcal{R}$, the preceding discussion may be formulated for rings as follows:

Definition. *A ring $\mathcal{R}$ is said to satisfy the* ***ascending chain condition*** *on ideals if any ascending sequence*

$$\mathcal{I}_1 \subseteq \mathcal{I}_2 \subseteq \mathcal{I}_3 \subseteq \dots$$

of ideals of $\mathcal{R}$ is eventually constant. That is, there exists an index k for which

$$\mathcal{I}_k = \mathcal{I}_{k+1} = \mathcal{I}_{k+2} = \dots$$

A ring that satisfies the ascending chain condition on ideals is called a ***noetherian ring***. ★

Theorem 9. *A ring $\mathcal{R}$ is noetherian if and only if every ideal of $\mathcal{R}$ is finitely generated.*

Theorem 10. *Let $\mathcal{R}$ be a commutative ring with identity. Then,*

i) $\mathcal{R}$ is noetherian if and only if every finitely generated $\mathcal{R}$-module is noetherian.

ii) *If, in addition, $\mathcal{R}$ is a principal ideal domain then, if M is generated by n elements, any submodule of M is generated by at most n elements.*

Theorem 11 (Hilbert Basis Theorem). *If a ring $\mathcal{R}$ is noetherian, then so is the polynomial ring $\mathcal{R}[x]$.*

Modules Over a Principal Ideal Domain

Theorem 12. *Let $\mathcal{R}$ be a principal ideal domain. Then,*

i) *An element $r \in \mathcal{R}$ is irreducible if and only if the ideal $\langle r \rangle$ is maximal.*

ii) *An element in $\mathcal{R}$ is prime if and only if it is irreducible.*

iii) *$\mathcal{R}$ is a unique factorization domain.*

iv) *$\mathcal{R}$ satisfies the ascending chain condition on ideals. Hence, so does any finitely generated $\mathcal{R}$-module M. Moreover, if M is generated by n elements, any submodule of M is generated by at most n elements.*

Definition. *Let $\mathcal{R}$ be a principal ideal domain and let M be an $\mathcal{R}$-module, with submodule N. Any generator of $\operatorname{ann}(N)$ is called an **order** of N. Also, an order of an element $v \in M$ is an order of the submodule $\langle v \rangle$.* ★

Remark: Note that if $A \subseteq B \subseteq M$ are submodules of M, then $\operatorname{ann}(B) \subseteq \operatorname{ann}(A)$, and so any order of A divides any order of B. Thus, just as with finite groups, the order of an element/submodule divides the order of the module.

The simplest type of nonzero module is clearly a cyclic module. Despite their simplicity, cyclic modules are extremely important and so we want to explore some of their basic properties:

Theorem 13. *Let $\mathcal{R}$ be a principal ideal domain. Then we have the following:*

- *If $\langle v \rangle$ is a cyclic $\mathcal{R}$-module with $\operatorname{ann}(v) = \langle \alpha \rangle$, then the map $\tau \colon \mathcal{R} \longrightarrow \langle v \rangle$ defined by $\tau(r) = rv$ is a surjective $\mathcal{R}$-homomorphism with kernel $\langle \alpha \rangle$. Hence*
$$\langle v \rangle \cong \mathcal{R}/\langle \alpha \rangle.$$
In other words, cyclic $\mathcal{R}$-modules are isomorphic to quotient modules of the base ring $\mathcal{R}$. If α is a prime then $\langle \alpha \rangle$ is a maximal ideal in $\mathcal{R}$, and so $\mathcal{R}/\langle \alpha \rangle$ is a field.
- *Any submodule of a cyclic $\mathcal{R}$-module is cyclic.*
- *Let $\langle v \rangle$ be a cyclic submodule of M of order α. Then $\langle \beta v \rangle$ has order $\alpha / \gcd(\alpha, \beta)$. Hence, if β and α are relatively prime then $\langle \beta v \rangle$ also has order α.*
- *If $u_1, \ldots, u_n$ are nonzero elements of M with orders $\alpha_1, \ldots, \alpha_n$ that are pairwise relatively prime, then the sum*
$$v = u_1 + \cdots + u_n$$
has order $\mu = \alpha_1 \cdot \cdots \cdot \alpha_n$. Consequently, if M is an $\mathcal{R}$-module and
$$M = A_1 + \cdots + A_n$$

where the submodules A_i have orders α_i that are pairwise relatively prime, then the sum is direct.

Note: It can be shown that a submodule of a free module need not be free (e.g. the submodule $\mathbb{Z} \times \{0\}$ of $\mathbb{Z} \times \mathbb{Z}$ is not free.) However, if $\mathcal{R}$ is a principal ideal domain this cannot happen:

Theorem 14. *Let M be a free module over a principal ideal domain $\mathcal{R}$. Then any submodule S of M is also free and $\operatorname{rk}(S) \leq \operatorname{rk}(M)$.*

Note: If V is a vector space of dimension n, then any set of n linearly independent vectors in V is a basis for V. This fails for modules. For example, $\mathbb{Z}$ is a $\mathbb{Z}$-module of rank 1, but the independent set $\{2\}$ is not a basis. On the other hand, the fact that a spanning set of size n is a basis does hold for modules over a principal ideal domain, as we now show:

Theorem 15. *Let M be a free $\mathcal{R}$-module of rank n, where $\mathcal{R}$ is a principal ideal domain. Let $S = \{s_1, \ldots, s_n\}$ be a spanning set for M. Then S is a basis for M.*

Prelude to Decomposition: Cyclic Modules

The following result shows how cyclic modules can be composed and decomposed:

Theorem 16. *Let M be an $\mathcal{R}$-module. Then,*

- *If $u_1, \ldots, u_n$ are nonzero elements of M with orders $\alpha_1, \ldots, \alpha_n$ that are pairwise relatively prime, then*
$$\langle u_1 + \cdots + u_n \rangle = \langle u_1 \rangle \oplus \cdots \oplus \langle u_n \rangle.$$
- *If $v \in M$ has order $\mu = \alpha_1 \cdot \cdots \cdot \alpha_n$, where $\alpha_1, \ldots, \alpha_n$ are pairwise relatively prime, then v can be written in the form*
$$v = u_1 + \cdots + u_n$$
where u_i has order α_i. Moreover,
$$\langle v \rangle = \langle u_1 \rangle \oplus \cdots \oplus \langle u_n \rangle.$$

The First Decomposition

The first step in the decomposition of a finitely generated module M over a principal ideal domain $\mathcal{R}$ is an easy one:

Theorem 17. *Any finitely generated module M over a principal ideal domain $\mathcal{R}$ is the direct sum of a free $\mathcal{R}$-module and a torsion $\mathcal{R}$-module*
$$M = M_{free} \oplus M_{tor}.$$
As to uniqueness, the torsion part M_{tor} is unique (it must be the set of all torsion elements of M) whereas the free part M_{free} is not unique. However, all possible free summands are isomorphic and thus have the same rank.

Remark: Note that if $\{w_1, \ldots, w_n\}$ is a basis for M_{free}, then we can write
$$M = \langle w_1 \rangle \oplus \cdots \oplus \langle w_n \rangle \oplus M_{\text{tor}},$$

where each cyclic submodule $\langle w_i \rangle$ has zero annihilator. This is a partial decomposition of M into a direct sum of cyclic submodules.

The Primary Decomposition

The first step in the primary cyclic decomposition is to decompose the torsion module into a direct sum of primary submodules:

Definition. *Let p be a prime in $\mathcal{R}$. A p-**primary** (or just **primary**) module is a module whose order is a power of p.* ★

Remark: Note that a p-primary module M with order p^k must have an element of order p^k.

Theorem 18 (The Primary Decomposition Theorem). *Let M be a nonzero torsion module over a principal ideal domain $\mathcal{R}$ with order*

$$\mu = p_1^{e_1} \cdot \cdots \cdot p_m^{e_n},$$

where the p_i's are distinct nonassociate primes in $\mathcal{R}$.

- *Then M is the direct sum*

  $$M = M_{p_1} \oplus \cdots \oplus M_{p_n},$$

  where

  $$M_{p_i} = \{v \in M \mid p_i^{e_i} v = 0\}$$

  is a primary submodule with order $p_i^{e_i}$ and annihilator

  $$\operatorname{ann}(M_{p_i}) = \langle p_i^{e_i} \rangle.$$

- *This decomposition of M into primary submodules is unique up to order of the summands. That is, if*

  $$M = N_{q_1} \oplus \cdots \oplus N_{q_m},$$

  where N_{q_i} is primary of order $q_i^{f_i}$ and $q_1, \ldots, q_m$ are distinct nonassociate primes, then $m = n$ and after a suitable reindexing of the summands we have $N_{q_i} = M_{p_i}$. Hence q_i and p_i are associates and $f_i = e_i$ (and so $\mu = q_i^{f_i} \cdot \cdots \cdot q_n^{f_n}$ is also a prime factorization of μ).

The Cyclic Decomposition of a Primary Module

The next step in the decomposition process is to show that a primary module can be decomposed into a direct sum of cyclic submodules. While this decomposition is not unique, the set of annihilator ideals is unique, as we will see. To establish this uniqueness, we use the following result:

Lemma 1. *Let M be a module over a principal ideal domain $\mathcal{R}$ and let $p \in \mathcal{R}$ be a prime. Then,*

- *If $pM = \{0\}$, then M is a vector space over the field $\mathcal{R}/\langle p \rangle$ with scalar multiplication defined by*

  $$(r + \langle p \rangle)v = rv \qquad \forall\ v \in M.$$

- *For any submodule S of M, the set*
$$S^{(p)} = \{v \in S \mid pv = 0\}$$
is also a submodule of M.

  Moreover, if $M = S \oplus T$, then
$$M^{(p)} = S^{(p)} \oplus T^{(p)}.$$

Theorem 19 (The Cyclic Decomposition Theorem of a Primary Module). *Let M be a nonzero primary finitely generated torsion module over a principal ideal domain $\mathcal{R}$, with order p^e. Then,*

- *M is the direct sum*
$$M = \langle v_1 \rangle \oplus \cdots \oplus \langle v_n \rangle$$
of cyclic submodules with annihilators $\operatorname{ann}(\langle v_1 \rangle) = \langle p^{e_i} \rangle$ *that can be arranged in ascending order*
$$\operatorname{ann}(\langle v_1 \rangle) \subseteq \cdots \subseteq \operatorname{ann}(\langle v_n \rangle),$$
or equivalently
$$e = e_1 \geq e_2 \geq \cdots \geq e_n.$$
- *As to uniqueness, suppose that M is also the direct sum*
$$M = \langle u_1 \rangle \oplus \cdots \oplus \langle u_m \rangle$$
of cyclic submodules with annihilators $\operatorname{ann}(\langle u_i \rangle) = \langle q^{f_i} \rangle$ *arranged in ascending order*
$$\operatorname{ann}(\langle u_1 \rangle) \subseteq \cdots \subseteq \operatorname{ann}(\langle u_m \rangle),$$
or equivalently
$$f_1 \geq f_2 \geq \cdots \geq f_m.$$
Then the two chains of annihilators are identical, that is
$$\operatorname{ann}(\langle u_i \rangle) = \operatorname{ann}(\langle v_i \rangle) \qquad \forall\, i.$$
Thus, $m = n$, p and q are associates, and $f_i = e_i$ for all i.

Now we can combine the various decompositions:

Theorem 20 (The Primary Cyclic Decomposition Theorem). *Let M be a nonzero finitely generated module over a principal ideal domain $\mathcal{R}$. Then,*

- *We have*
$$M = M_{free} \oplus M_{tor}.$$
If M_{tor} has order
$$\mu = p_1^{e_1} \cdot \cdots \cdot p_n^{e_n},$$
where the p_i's are distinct nonassociate primes in $\mathcal{R}$, then M_{tor} can be uniquely decomposed (up to the order of the summands) into the direct sum
$$M = M_{p_1} \oplus \cdots \oplus M_{p_n},$$

where

$$M_{p_i} = \{v \in M_{tor} \mid p_i^{e_i} v = 0\}$$

is a primary submodule with annihilator $\langle p_i^{e_i} \rangle$*.*

Finally, each primary submodule M_{p_i} *can be written as a direct sum of cyclic submodules, so that*

$$M = M_{free} \oplus \underbrace{[\langle v_{1,1} \rangle \oplus \cdots \oplus \langle v_{1,k_1} \rangle]}_{M_{p_1}} \oplus \cdots \oplus \underbrace{[\langle v_{n,1} \rangle \oplus \cdots \oplus \langle v_{n,k_n} \rangle]}_{M_{pn}}$$

where $\operatorname{ann}(\langle v_{i,j} \rangle) = \langle p_i^{e_{i,j}} \rangle$ *and the terms in each cyclic decomposition can be arranged so that, for each* i*, we have*

$$\operatorname{ann}(\langle v_{i,1} \rangle) \subseteq \cdots \subseteq \operatorname{ann}(\langle v_{i,k_i} \rangle)$$

or, equivalently,

$$e_i = e_{i,1} \geq e_{i,2} \geq \cdots \geq e_{i,k_i}.$$

- *As for uniqueness, suppose that*

  $$M = N_{free} \oplus \langle x_1 \rangle \oplus \cdots \oplus \langle x_\ell \rangle$$

  is a decomposition of M *into the direct sum of a free module* M_{free} *and primary cyclic submodules* $\langle x_i \rangle$*. Then,*

  - $\operatorname{rk}(N_{free}) = \operatorname{rk}(M_{free})$.
  - *The number of summands is the same in both decompositions, that is*

    $$\ell = k_1 + \cdots + k_n.$$

  - *The summands in this decomposition can be reordered to get*

    $$M = N_{free} \oplus [\langle u_{1,1} \rangle \oplus \cdots \oplus \langle u_{1,k_1} \rangle] \oplus \cdots \oplus [\langle u_{n,1} \rangle \oplus \cdots \oplus \langle u_{n,k_n} \rangle],$$

    where the primary submodules are the same

    $$\langle u_{i,1} \rangle \oplus \cdots \oplus \langle u_{i,k_i} \rangle = \langle v_{i,1} \rangle \oplus \cdots \oplus \langle v_{i,k_i} \rangle$$

    for $i = 1, \ldots, n$*. In addition, the annihilator chains are the same, that is,*

    $$\operatorname{ann}(\langle u_{i,j} \rangle) = \operatorname{ann}(\langle v_{i,j} \rangle) \qquad \forall\ i, j.$$

In summary, the free rank, primary submodules and annihilator chain are uniquely determined by the module M*.*

Theorem 21 (The Invariant Factor Decomposition Theorem). *Let* M *be a finitely generated module over a principal ideal domain* $\mathcal{R}$*. Then*

$$M = M_{free} \oplus \cdots \oplus D_m,$$

where M_{free} *is a free submodule and* D_i *is a cyclic submodule of* M*, with order* d_i*, where*

$$d_m \mid d_{m-1} \mid \cdots \mid d_2 \mid d_1.$$

This decomposition is called an ***invariant factor decomposition*** *of* M*, and the scalars* d_i *are called the* ***invariant factors*** *of* M*. The invariant factors are uniquely determined, up to multiplication by a unit, by the module* M*. Also, the rank of* M_{free} *is uniquely determined by* M*.*

Remark: The annihilators of an invariant factor decomposition are called the ***invariant ideals*** of M. The chain of invariant ideals is unique, as is the chain of annihilators in the primary cyclic decomposition. Note that d_1 is an order of M, that is

$$\operatorname{ann}(M) = \langle d_1 \rangle.$$

Note also that the product

$$\gamma = d_1 \cdot \cdots \cdot d_m$$

of the invariant factors of M has some nice properties. For example, γ is the product of all the elementary divisors of M. We will see later on that in the context of a linear operator τ on a vector space, γ is the characteristic polynomial of τ.