

## Math 551 – Algebra – Fall 2000

Richard Lyons  
Rutgers University  
New Brunswick, New Jersey, USA

### B. Abelian Groups and Modules over Principal Ideal Domains

#### 1. Abelian Groups.

##### 1a. Direct Products

The nicest way a group  $G$  can decompose is as the direct product of a number of other groups (which are then isomorphic to subgroups of  $G$ ). We give a criterion here for  $G$  to be isomorphic to  $G_1 \times \cdots \times G_r$  for certain subgroups  $G_1, \dots, G_r$  of  $G$ .

**Definition.** Let  $G_1, \dots, G_r$  be groups. The (external) direct product  $G_1 \dot{\times} \cdots \dot{\times} G_r$  is the group whose underlying set is the Cartesian product  $G_1 \times \cdots \times G_r$ , with the operation

$$(g_1, \dots, g_r)(h_1, \dots, h_r) = (g_1 h_1, \dots, g_r h_r),$$

the product in the  $i$ -th place being formed in the group  $G_i$ .

A similar definition can be made for an infinite family of groups  $\{G_i\}_{i \in I}$ : the external direct product

$$\prod_{i \in I} G_i$$

is the group whose underlying set is the Cartesian product of the  $G_i$ . The elements of this set are functions  $f$  on  $I$  such that  $f(i) \in G_i$  for each  $i$ ; the multiplication is pointwise, i.e.  $(ff')(i) = f(i)f'(i)$ .

(External) direct products come with a family of projection homomorphisms

$$\pi_j : G_1 \dot{\times} \cdots \dot{\times} G_r \rightarrow G_j, \quad j = 1, \dots, r$$

or more generally

$$\pi_j : \prod_{i \in I} G_i \rightarrow G_j, \quad j \in I,$$

and satisfy the universal property that for any group  $G$  and family of homomorphisms  $\gamma_j : G \rightarrow G_j$ ,  $j \in I$ , there is a unique homomorphism

$$\gamma : G \rightarrow \prod_{i \in I} G_i \text{ such that } \pi_j \gamma = \gamma_j \quad \forall j \in I.$$

Namely, for any  $g \in G$ ,  $\gamma(g)$  has  $\gamma_j(g)$  for its  $j$ -th coordinate.

There is another *internal* notion of direct product, at least for the case of direct products of finitely many groups:

**Definition.** Let  $G$  be a group and  $G_1, \dots, G_r$  be subgroups of  $G$ . We write

$$G = G_1 \times \cdots \times G_r$$

and say that  $G$  is the direct product of its subgroups  $G_1, \dots, G_r$  if and only if the mapping

$$\phi : G_1 \times \cdots \times G_r \rightarrow G, \quad \phi(g_1, \dots, g_r) = g_1 \cdots g_r$$

is an isomorphism.

It is not always the case that  $\phi$  is even a homomorphism; the requirements that it be a homomorphism, and that it be injective and surjective, each carry weight. When  $G = G_1 \times \cdots \times G_r$ , we are free to think of  $G$  interchangeably with the external direct product.

**Theorem.** Let  $G_1, \dots, G_r$  be subgroups of a group  $G$ . Then (a), (b) and (c) are equivalent.

- (a)  $G = G_1 \times \cdots \times G_r$ .
- (b) (1)  $G_i \triangleleft G$  for all  $i$ ;  
 (2)  $G = \langle G_1, \dots, G_r \rangle$ ;  
 (3) For each  $i = 1, \dots, r$ , if we put  $G^i = \prod_{j \neq i} G_j$  (in order), then  $G^i \cap G_i = 1$ .
- (c) (1) For any  $i \neq j$ , and any  $g_i \in G_i$  and  $g_j \in G_j$ ,  $g_i g_j = g_j g_i$ ;  
 (2)  $G = G_1 \cdots G_r$ ;  
 (3)  $G^i \cap G_i = 1$  for all  $i$  (with  $G^i$  defined as in (b)).

**Proof.** (a) implies (b): Let  $\Gamma = G_1 \times \cdots \times G_r$ , and let  $\Gamma_i$  be the subgroup consisting of all elements of  $\Gamma$  all of whose coordinates are 1, except possibly the  $i$ -th coordinate. Clearly  $\Gamma_i \leq \Gamma$  and  $\phi$  maps  $\Gamma_i$  isomorphically onto  $G_i$ . Now if (a) holds, then  $\Gamma \cong_\phi G$ , and so to prove the various statements of (b) it suffices to check the corresponding statements for  $\Gamma$  and the  $\Gamma_i$ . First,  $\Gamma_i$  is the intersection of the kernels of the projections  $\pi_j$ ,  $j \neq i$ , so  $\Gamma_i \triangleleft \Gamma$ . A typical element  $(g_1, \dots, g_r) \in \Gamma$  is the product of the elements  $(g_1, 1, \dots, 1)(1, g_2, 1, \dots, 1) \cdots$  so  $\Gamma = \Gamma_1 \cdots \Gamma_r$ . Under  $\phi$ ,  $G^i$  corresponds to the kernel of the projection  $\pi_i$ , and  $\Gamma_i \cap \ker \pi_i = 1$ .

(b) implies (c): For  $g_i \in G_i$ ,  $g_j \in G_j$  and  $i \neq j$ ,  $[g_i, g_j] = g_i g_j (g_j^{-1}) = g_i (g_j g_j^{-1}) \in G_i \cap G_j \leq G_i \cap G^i = 1$ . This implies (1). Then any word in elements of  $G_1, \dots, G_r$  can be shuffled to a word  $g_1 \cdots g_r$ , so (b2) implies (c2). Trivially (b3) implies (c3).

(c) implies (a): The three properties imply in turn that  $\phi$  is a homomorphism,  $\phi$  is surjective, and  $\phi$  is injective. Namely,

$$\begin{aligned} \phi[(g_1, \dots, g_r)(h_1, \dots, h_r)] &= \phi(g_1 h_1, \dots, g_r h_r) = g_1 h_1 \cdots g_r h_r = g_1 \cdots g_r \cdot h_1 \cdots h_r; \\ &= \phi(g_1, \dots, g_r) \phi(h_1, \dots, h_r) \end{aligned}$$

$\phi(\Gamma)$  is a subgroup containing  $G_1, \dots, G_r$  so equals  $G$ ;

and if  $g = (g_1, \dots, g_r) \in \ker \phi$ , then  $g_1 \cdots g_r = 1$ , and for each  $i$  if we solve for  $g_i$  we get  $g_i \in G_i \cap G^i = 1$ , so  $\ker \phi = 1$ . QED

The case of two factors is important:

$$G = H \times K \iff H \triangleleft G, K \triangleleft G, H \cap K = 1 \text{ and } G = \langle H, K \rangle.$$

Of course  $H \times K$  has the normal subgroup  $H \times 1 \cong H$ , and the quotient  $H \times K / H \times 1 \cong K$  (by the first isomorphism theorem applied to the projection onto  $K$ ). We routinely identify these subgroups and quotients with  $H$  and  $K$ . What distinguishes the direct product among all “extensions of  $H$  by  $K$ ” are the facts that (1)  $H$  has a complement (a subgroup  $K$  such that  $HK = G$  and  $H \cap K = 1$ ), and (2) that complement commutes elementwise with  $H$ .

Not every subgroup of a direct product is a direct product of subgroups. However, the following is fundamental.

**Proposition.** *Suppose that  $H_1 \triangleleft G_1$  and  $H_2 \triangleleft G_2$ . Then  $H_1 \times H_2 \triangleleft G_1 \times G_2$ , and*

$$(G_1 \times G_2) / (H_1 \times H_2) \cong G_1 / H_1 \times G_2 / H_2.$$

**Proof.** Define  $\phi : G_1 \times G_2 \rightarrow G_1 / H_1 \times G_2 / H_2$  by  $\phi(g_1, g_2) = (g_1 H_1, g_2 H_2)$ . It is easily checked that this is a surjective homomorphism whose kernel is  $H_1 \times H_2$ . Now apply the first isomorphism theorem.

Finite direct products have another universal property, for which they are also called “sums”, particularly in the context of abelian groups. Namely, given groups  $G_1, \dots, G_n$ , there are canonical injections

$$\iota_j : G_j \rightarrow G_1 \times \cdots \times G_n,$$

with  $\iota_j(g)$  being the  $n$ -tuple whose  $j$ -th coordinate is  $g$  and all of whose other coordinates are 1. The images of the various  $\iota_j$  are “supported” in different coordinates and so commute elementwise with one another. The universal property is that for any group  $H$ , and any  $n$ -tuple of homomorphisms  $\phi_i : G_i \rightarrow H$  such that

$$[\phi_i(g_i), \phi_j(g_j)] = 1 \text{ for all } i \neq j, \text{ all } g_i \in G_i \text{ and all } g_j \in G_j,$$

there is a unique homomorphism

$$\Phi : G_1 \times \cdots \times G_n \rightarrow H, \quad (g_1, \dots, g_n) \mapsto \phi_1(g_1)\phi_2(g_2)\cdots\phi_n(g_n)$$

such that  $\phi_i = \Phi \circ \iota_i$  for each  $i = 1, \dots, n$ . The unique mapping  $\Phi$  is sometimes notated  $\phi_1 \times \cdots \times \phi_n$ , so that by definition

$$\phi_1 \times \cdots \times \phi_n(g_1, \dots, g_n) = \phi_1(g_1)\phi_2(g_2)\cdots\phi_n(g_n).$$

For example the mapping constructed in the proof of the preceding proposition is  $\pi_{H_1} \times \pi_{H_2}$ . The commutator condition  $[\phi_i(g_i), \phi_j(g_j)] = 1$  is needed to prove (actually equivalent to the statement) that  $\phi_1 \times \cdots \times \phi_n$  is a homomorphism.

## 1b. Direct Sums and Free Abelian Groups

For small abelian groups there are decisive structure theorems, giving essentially unique decompositions as direct products of cyclic groups. By “decisive” is meant that the theorems are strong enough in many cases to enable one to check whether a given statement about (small) abelian groups is true, to check whether two abelian groups arising in different contexts are isomorphic, etc. The word “small” here could be interpreted in two senses: either finitely generated, or of finite exponent. We shall prove the decomposition theorem for the first of these.

It is customary to use additive notation for abelian groups, and we shall do so. Nevertheless, the direct product of a family  $\{G_i\}_{i \in I}$  of abelian groups will still be denoted

$$\prod_{i \in I} G_i.$$

However, for infinite index sets  $I$ , it is the direct sum (or coproduct) which best suits the theory of abelian groups.

**Definition.** Let  $\{G_i\}_{i \in I}$  be a family of abelian groups. The direct sum

$$\prod_{i \in I} G_i \text{ (or } \bigoplus_{i \in I} G_i$$

is the subgroup of the direct product  $\prod_{i \in I} G_i$  consisting of all elements which have only finitely many non-identity coordinates.

Then there are canonical (injective) homomorphisms  $\iota_j : G_j \rightarrow \prod_{i \in I} G_i$ , one for each  $j \in I$ , such that  $\iota_j(g)$  is the element whose  $j$ -th coordinate is  $g$  and all of whose other coordinates are the identity (in the appropriate group). These mappings have the universal property that for any abelian group  $H$  and any family of homomorphisms  $\{\phi_i\}_{i \in I}$  with  $\phi_i : G_i \rightarrow H$ , there is a unique homomorphism

$$\Phi = \bigoplus_{i \in I} \phi_i : \bigoplus_{i \in I} G_i \rightarrow H \text{ such that } \phi_i = \Phi \circ \iota_i \text{ for all } i \in I;$$

namely  $\bigoplus_{i \in I} \phi_i$  maps  $(g_i)_{i \in I}$  to  $\sum_{i \in I} \phi_i(g_i)$ , this (possibly infinite) sum being well-defined since  $g_i = 0$  for all but finitely many  $i$ , and hence  $\phi_i(g_i) = 0$  for all but finitely many  $i$ .

This direct sum therefore plays the same role in the theory of abelian groups that the free product plays in the theory of (all) groups. We have really defined an “external” direct sum, and then we say that an abelian group  $G$  is the “internal” direct sum of subgroups  $G_i$  if and only if the mapping  $\bigoplus_{i \in I} : G_i \rightarrow G$  induced by the inclusion mappings (i.e.,  $\bigoplus_{i \in I} : (g_i)_{i \in I} \mapsto \sum_{i \in I} g_i$ ) is an isomorphism. Generally the distinction between internal and external is blurred, since it can always be bridged by replacing groups by isomorphic copies.

**Definition.** A free abelian group is the direct sum

$$\bigoplus_{i \in I} \mathbf{Z}$$

of copies of  $\mathbf{Z}$  (indexed by some set  $I$ ).

If we let  $e_i$  be the element of this direct sum which is 1 in the  $i$ -th coordinate and 0 in every other coordinate, then every element of  $\bigoplus_{i \in I} \mathbf{Z}$  is uniquely expressible as a sum  $\sum_{i \in I} n_i e_i$ , where the  $n_i$  are all integers, all but finitely many (“almost all”) of them being 0. The set  $\{e_i\}$  is called a basis, by analogy with the theory of vector spaces.

A free abelian group has the expected (?) universal property, which as usual characterizes it: there is a (set) mapping  $\iota : I \rightarrow \bigoplus_{i \in I} \mathbf{Z}$ , taking  $i$  to the element  $e_i$  which is 1 in the  $i$ -th coordinate and 0 in every other coordinate; moreover for any abelian group  $H$  and any (set) mapping  $\psi : I \rightarrow H$  there exists a unique homomorphism  $\Psi : \bigoplus_{i \in I} \mathbf{Z} \rightarrow H$  such that  $\Psi \circ \iota = \psi$ . Namely,

$$\Psi\left(\sum_i n_i e_i\right) = \sum_i n_i \psi(e_i).$$

This has the following consequence, completely analogous to the corresponding result for arbitrary groups and free groups.

**Theorem 0.** Every abelian group is a quotient of a free abelian group. More precisely, if  $G$  is an abelian group and  $S \subseteq G$  is a subset such that  $\langle S \rangle = G$ , then there is a surjective homomorphism

$$\phi : F \rightarrow G,$$

where  $F$  is free abelian on  $S$ ; thus  $G \cong F / \ker \phi$ .

Pursuing the analogy with vector spaces a bit further, we may define a subset  $\{f_i\}_{i \in I} \subseteq H$  of an arbitrary abelian group  $H$  to be linearly independent if and only if whenever  $\sum_{i \in I} n_i f_i = 0$ , the  $n_i$  being integers almost all zero, it follows that  $n_i = 0$  for all  $i$ . Then a basis is just a linearly independent generating set. It is easily seen that a basis can be equivalently defined as a subset  $\{f_i\}$  such that every element of the group is uniquely expressible as a sum  $\sum_i n_i f_i$ ,  $n_i \in \mathbf{Z}$ , almost all  $n_i$  being 0.

**Proposition.** An abelian group is free abelian on some set if and only if it has a basis. In that case, the cardinality of a basis is uniquely determined.

The cardinality of a basis is called the “rank” of a free abelian group.

**Proof.** We saw above that a free abelian group has a basis  $\{e_i\}$ . Conversely, if  $G$  has the basis  $\{f_i\}_{i \in I}$ , then  $G$ , together with the mapping  $i \mapsto f_i$ , has the above universal property since every element of  $G$  may be uniquely expressed  $\sum_i n_i f_i$ , so that the analogue of  $\Psi$  above is well-defined.

Next suppose that  $F = \bigoplus_{i \in I} \langle e_i \rangle$  is free abelian with basis  $\{e_i\}_{i \in I}$ . Thus each  $e_i \cong \mathbf{Z}$ . Pick a prime  $p \in \mathbf{Z}$  and set  $pF = \{pg \mid g \in F\}$ . It is easily checked that  $H \leq F$  and indeed  $pF = \bigoplus_{i \in I} \langle pe_i \rangle$ . Consequently

$$F/pF \cong \bigoplus_{i \in I} \langle e_i \rangle / \langle pe_i \rangle \cong \bigoplus_{i \in I} \mathbf{Z}/p\mathbf{Z},$$

the direct sum of  $|I|$  copies of  $\mathbf{Z}/p\mathbf{Z}$ . But this direct sum may be considered a vector space over  $\mathbf{Z}/p\mathbf{Z}$ , and  $|I|$  is its dimension. so is uniquely determined. Thus the rank of  $F$  is  $\dim_{\mathbf{Z}/p\mathbf{Z}}(F/pF)$ , an expression independent of the basis.

(In the finite-dimensional case it is familiar that the dimension is uniquely determined. In the infinite-dimensional case it is also true, and just as easy to prove given the Schröder-Bernstein theorem in set theory. For vector spaces over  $\mathbf{Z}/p\mathbf{Z}$ , one can also easily argue that if  $V$  is an infinite-dimensional vector space, then  $|V| = \dim V$ . However, this last approach doesn't work for PID's in general, see next section.)

An important property of free abelian groups is the following splitting property (free abelian groups are “projective” abelian groups):

**Theorem 1.** *Suppose that  $G$  is an abelian group and  $H$  is a subgroup such that  $G/H$  is free. Then  $G = H \oplus K$  for some subgroup  $K \leq G$ .*

**Proof.** We prove the equivalent statement: if  $\phi : G \rightarrow F$  is a surjective homomorphism of abelian groups with  $F$  free abelian, then  $G = \ker \phi \oplus K$  for some subgroup  $K \leq G$ . (This implies the desired statement when applied to the projection  $\pi_H : G \rightarrow G/H$ .)

Let  $\{f_i\}_{i \in I}$  be a basis of  $F$ . Choose for each  $i \in I$  an element  $g_i \in G$  such that  $\phi(g_i) = f_i$ . Let  $K = \langle g_i \mid i \in I \rangle$ . Then  $G = H + K$ : given  $g \in G$  we write  $\phi(g) = \sum n_i f_i$ , set  $g' = \sum n_i g_i$  and observe that  $\phi(g') = \phi(g)$ . Thus  $\phi(g - g') = 0$ , and  $g = (g - g') + g'$  with  $g - g' \in H$  and  $g' \in K$ . Also  $H \cap K = 0$ : if  $g \in H \cap K$ , then  $g = \sum n_i g_i$  for some integers  $n_i$ , and applying  $\phi$  gives  $0 = \sum n_i f_i$ , so  $n_i = 0$  for all  $i$  whence  $g = 0$ .

### 1c. Finitely Generated Free Abelian Groups

The main theorems on finitely generated abelian groups rest on (and are equivalent to) theorems on finitely generated *free* abelian groups.

**Theorem 2.** *Any subgroup  $H$  of a finitely generated free abelian group  $G$  is a free abelian group. Moreover the rank of  $H$  is at most the rank of  $G$ .*

**Proof.** Let  $\{e_1, \dots, e_n\}$  be a basis of  $G$ . The proof is by induction on  $n$ . Let  $G_0 = \mathbf{Z}e_1 + \dots + \mathbf{Z}e_{n-1}$  and  $H_0 = H \cap G_0$ . Then by induction  $H_0$  is free abelian of rank  $r \leq n - 1$ . Moreover  $H/H_0 \cong H + G_0/G_0 \leq G/G_0 \cong \mathbf{Z}e_n \cong \mathbf{Z}$ . Hence  $H/H_0 \cong \mathbf{Z}$  or  $0$ . In the first case there exists  $K \leq H$  such that  $H = H_0 \oplus K$ , so  $H$  is free abelian of rank  $r + 1 \leq n$ . In the second case the desired conclusion is obvious.

**Corollary.** *Any subgroup of a finitely generated abelian group is finitely generated.*

**Proof.** If  $H \leq G$  with  $G$  finitely generated, we may write  $G = F/R$  where  $F$  is finitely generated free abelian. Then  $H = F_0/R$  for some  $R \leq F_0 \leq F$  by the third isomorphism theorem, and the theorem implies that  $F_0$  is finitely generated. *A fortiori*,  $H$  is finitely generated.

The main theorem is formulated as a theorem about the relationship between appropriate bases of a free abelian group and a subgroup. It will be applied later in the context of Theorem 0 to the inclusion  $\ker \phi \rightarrow F$  (note that Theorem 2 tells us that  $\ker \phi$  is itself finitely generated and free, given that  $F$  is). It will yield structural information about the quotient  $F/\ker \phi$ , which as Theorem 0 shows is an arbitrary finitely generated abelian group.

The theorem has an existence and a uniqueness statement.

**Fundamental theorem on finitely generated abelian groups (I: free abelian group version).** *Let  $F$  be a finitely generated free abelian group, of rank  $s$ , and  $E$  a subgroup of  $F$ . Then  $E$  is a finitely generated free abelian group, of rank  $r \leq s$ . Moreover there exist bases  $e_1, \dots, e_r$  of  $E$  and  $f_1, \dots, f_s$  of  $F$  and uniquely determined positive integers  $m_1, \dots, m_r$  such that*

- a)  $e_i = m_i f_i, i = 1, \dots, r$ , and
- b)  $m_1 | m_2 | \dots | m_r$ .

However, the bases  $\{e_i\}$  and  $\{f_i\}$  are not uniquely determined. The integers

$$m_1, m_2, \dots, m_r$$

of the theorem are sometimes called the “invariant factors” of the inclusion mapping  $E \rightarrow F$ .

Before proceeding with the proof of this theorem, we make two digressions.

## 1d. Integer matrices and equivalence

The first digression is to interpret the Fundamental Theorem (version Ia) in matrix language. The reader should be able to supply proofs for all statements in this section. Like finite-dimensional vector spaces and linear transformations, free abelian groups of finite rank and homomorphisms between them have concrete realizations as column vectors and matrices; setting up these realizations for abelian groups is essentially identical to setting them up for vector spaces, except that the entries of the matrices and column vectors now come from  $\mathbf{Z}$  instead of from a field.

The group  $\mathbf{Z}^n$  of all integer  $n \times 1$  column vectors is clearly a free abelian group, and one of its bases is  $\{e_1^n, \dots, e_n^n\}$ , where  $e_i^n$  is the  $n \times 1$  column vector whose  $i$ -th entry is 1 and all of whose other entries are 0.

Moreover, given any rank  $n$  free abelian group  $G$  and basis  $B = \{e_1, \dots, e_n\}$ , and given any  $g \in G$ , we write  $g = \sum_{i=1}^n m_i e_i$  and define  $[g]^B = [m_1 \ \dots \ m_n]^T$ . The mapping

$$G \rightarrow \mathbf{Z}^n, \quad g \mapsto [g]^B,$$

is then an isomorphism.

Now, given a homomorphism  $\phi : G \rightarrow H$  and bases  $B = \{e_1, \dots, e_n\}$  and  $B' = \{f_1, \dots, f_m\}$  of  $G$  and  $H$ , we write  $\phi(e_j) = \sum_{i=1}^m c_{ij} f_i$ , ( $c_{ij} \in \mathbf{Z}$ ) for each  $j = 1, \dots, n$ , and define

$$[\phi]_B^{B'} = [c_{ij}]_{1 \leq i \leq m, 1 \leq j \leq n}.$$

The mapping

$$\text{Hom}(G, H) \rightarrow \mathbf{Z}^{m \times n}, \quad \phi \mapsto [\phi]_B^{B'}, \quad 1A$$

is then an isomorphism of abelian groups, and

$$[\phi(g)]^{B'} = [\phi]_B^{B'} [g]^B \text{ for all } g \in G,$$

with ordinary matrix multiplication on the right. Indeed, given  $\phi$ ,  $[\phi]_B^{B'}$  is the unique  $m \times n$  matrix for which this equation is true for all  $g \in G$ . This last remark (or direct computation) quickly implies in turn that for any  $\phi, \psi \in \text{Hom}(G, H)$  and  $\chi \in \text{Hom}(H, K)$ , and for any bases  $B, B', B''$  of  $G, G, H$ , respectively, we have

$$[\phi + \psi]_B^{B'} = [\phi]_B^{B'} + [\psi]_B^{B'} \text{ and } [\chi \circ \phi]_B^{B''} = [\chi]_B^{B''} [\phi]_B^{B'},$$

again with matrix multiplication on the right.

If  $B$  and  $B'$  are two bases of the same free abelian group  $H$ , then

$$[1_H]_B^{B'}$$

is the “change of basis” matrix whose columns give the  $B$ -expansion of the elements of  $B'$ . In particular

$$[1_H]_B^B = I,$$

the identity matrix. Moreover different choices  $C, C'$  of bases of  $H$  and  $K$ , respectively, give the related matrix

$$[\phi]_{C'}^C = [id_K]_{C'}^{B'} [\phi]_{B'}^B [id_H]_B^C = P [\phi]_{B'}^B Q, \quad 1B$$

where  $P = [id_K]_{C'}^{B'}$  and  $Q = [id_H]_B^C$ .

If  $H$  and  $K$  are free abelian groups of ranks  $m$  and  $n$ , respectively, and  $\phi : H \rightarrow K$  and  $\psi : K \rightarrow H$  are homomorphisms, then with respect to bases  $B$  and  $B'$  of  $H$  and  $K$  respectively we have

$$[\phi]_{B'}^B [\psi]_B^{B'} = [\phi \circ \psi]_{B'}^{B'} \text{ and } [\psi]_B^{B'} [\phi]_{B'}^B = [\psi \circ \phi]_{B'}^{B'}.$$

Because of the isomorphisms  $\phi \mapsto [\phi]_{B'}^B$  and  $\psi \mapsto [\psi]_B^{B'}$  of  $\text{Hom}(H, K)$  and  $\text{Hom}(K, H)$ , respectively, with  $\mathbf{Z}^{m \times n}$  and  $\mathbf{Z}^{n \times m}$ , we conclude that

$$\phi \text{ is invertible with inverse } \psi \text{ if and only if } [\phi]_{B'}^B \text{ is invertible with inverse } [\psi]_B^{B'}.$$

In particular,

$$[id_H]_B^{B'} = ([id_H]_{B'}^B)^{-1}.$$

for any two bases  $B, B'$  of  $H$ .

This permits us to establish bijections (not canonical) between the set of all bases of  $H$  and the set of all invertible matrices in  $\mathbf{Z}^{m \times m}$ . Namely, fix a basis  $B$  of  $H$ ; the correspondence

$$B' \mapsto [id_H]_B^{B'}$$

is a bijection. So is the correspondence  $B' \mapsto [id_H]_{B'}^B$ .

As a consequence we can determine, given  $\phi : H \rightarrow K$ , all the matrices representing  $\phi$  with respect to all bases of  $H$  and  $K$ . We first define an equivalence relation  $\sim$  (called “equivalence”) on  $\mathbf{Z}^{m \times n}$  by:

$$A \sim A' \iff A' = PAQ \text{ for some invertible } P \in \mathbf{Z}^{m \times m} \text{ and } Q \in \mathbf{Z}^{n \times n}.$$

Fix bases  $B$  and  $C$  of  $H$  and  $K$  respectively. Let  $\phi : H \rightarrow K$  be a homomorphism and  $A = [\phi]_C^B$ . The matrices  $P$  and  $Q$  allowable above are precisely the matrices  $[id_H]_B^{B'}$  and  $[id_H]_{C'}^C$ , as  $B'$  and  $C'$  range over the sets of bases of  $H$  and  $K$ , respectively. Because of (1B), we conclude:

**Proposition.** *Let  $H$  and  $K$  be free abelian groups of finite ranks  $m$  and  $n$ , respectively. Let  $\phi : H \rightarrow K$  be a homomorphism, and let  $A = [\phi]_C^B$  for some bases  $B$  and  $C$  of  $H$  and  $K$ , respectively. Then for any  $m \times n$  matrix  $A'$  over  $\mathbf{Z}$ ,  $A \sim A'$  if and only if  $A' = [\phi]_{C'}^{B'}$  for some bases  $B'$  and  $C'$  of  $H$  and  $K$ , respectively.*

The following theorem therefore largely follows from the main theorem of the last section.

**Fundamental theorem on finitely generated abelian groups (Ib:  $\mathbf{Z}$ -matrix version).** *Let  $A$  be an integer  $m \times n$  matrix. Then there exists a uniquely determined integer  $r \geq 0$ ,  $r \leq \min(m, n)$ , and uniquely determined positive integers  $m_1, \dots, m_r$  such that*

- a)  $A \sim \text{diag}(m_1, m_2, \dots, m_r, 0, \dots, 0)$ ; and
- b)  $m_1 \mid m_2 \mid \dots \mid m_r$ .

Here  $\text{diag}(m_1, m_2, \dots, m_r, 0, \dots, 0)$  is the  $m \times n$  matrix with all entries 0 except the first  $r$  entries down the main diagonal, which are  $m_1, \dots, m_r$ , in that order.

**Proof.** Let  $H$  and  $K$  be free abelian groups of ranks  $m$  and  $n$ , respectively. By the isomorphism (1A), there is a homomorphism  $\phi : H \rightarrow K$  and bases  $B$  and  $C$  of  $H$  and  $K$ , respectively, such that  $[\phi]_C^B = A$ .

Set  $G = \phi(H) \leq K$  and  $r = \text{rank}(G)$ . By Theorem 2,  $G$  is free, and hence by Theorem 1,  $H = H_1 \oplus \ker \phi$  for some subgroup  $H_1$ . Then  $\psi = \phi|_{H_1}$  is an isomorphism  $H_1 \cong G$ .

By version Ia, there exists  $r \geq 0$  and uniquely determined positive integers  $m_1, \dots, m_r$  such that there are bases  $C' = \{e_1, \dots, e_n\}$  of  $K$  and  $\{f_1, \dots, f_r\}$  of  $G$  with  $f_i = m_i e_i$

for each  $i = 1, \dots, r$ . The elements  $\psi^{-1}f_1, \dots, \psi^{-1}f_r$ , together with an arbitrarily chosen basis of  $\ker \phi$  form a basis  $B'$  of  $H$ . We then have

$$[\phi]_{C'}^{B'} = \text{diag}(m_1, \dots, m_r, 0, \dots, 0), \quad 1C$$

establishing existence. Conversely, if  $A$  is equivalent to such a matrix, then bases  $B'$  and  $C'$  exist such that (1C) holds. Writing  $C' = \{e_1, \dots, e_n\}$  and  $B' = \{f_1, \dots, f_r, \dots\}$  we have that  $\phi(f_1), \dots, \phi(f_r)$  form a basis of  $G$ , and  $\phi(f_i) = m_i e_i$  for each  $i = 1, \dots, r$ . So the uniqueness follows from version Ia.

In using this theorem, the following observation is useful:

**Proposition.** *Let  $P$  be a square matrix with entries in  $\mathbf{Z}$ . Then  $P$  is invertible in  $\mathbf{Z}^{m \times m}$  if and only if  $\det(P)$  is a unit in  $\mathbf{Z}$ , i.e.,  $\det(P) = \pm 1$ .*

On the one hand if  $P$  is invertible then  $\det(P) \det(P^{-1}) = \det I = 1$ , with both  $\det(P)$  and  $\det(P^{-1})$  in  $\mathbf{Z}$ . On the other hand if  $\det(P)$  is a unit in  $\mathbf{Z}$  then the familiar formula

$$P^{-1} = \det(P)^{-1} \text{adj}(P),$$

$\text{adj}(P)$  being the transpose of the matrix of cofactors, shows that  $P^{-1} \in \mathbf{Z}^{m \times m}$ .

## 1e. Principal Ideal Domains

The second digression is to observe that the proofs we are giving generalize without change to modules over PID's (instead of just abelian groups). We might as well formalize this.

**Definition.** *A principal ideal domain (PID) is a commutative ring  $R$  with unit 1, such that  $R$  is an integral domain ( $xy = 0$  implies either  $x = 0$  or  $y = 0$ ) and such that every ideal in  $R$  is principal, i.e. consists of all the  $R$ -multiples of a single element of  $R$ .*

If we consider  $R$  to be an  $R$ -group (an abelian group with operators  $R$ , acting by left multiplication) then the principal ideal condition is just the condition that every  $R$ -subgroup (i.e. ideal) is “ $R$ -cyclic”—i.e., is generated as an  $R$ -group by a single element.

Examples of principal ideal domains include the following two essential examples:  $\mathbf{Z}$ , and  $k[X]$ , the polynomial ring in one variable over a field. In both cases a stronger statement is actually true: there is a division algorithm. In the case of  $\mathbf{Z}$ , for every  $d \neq 0$  and every  $n \in \mathbf{Z}$ , there exist  $q, r \in \mathbf{Z}$  such that  $n = qd + r$  and  $|r| < |d|$ . In the case of  $k[X]$ , for every  $d, n \in k[X]$  with  $d \neq 0$ , there exist  $q, r \in k[X]$  such that  $n = qd + r$  and  $\deg r < \deg d$ . Thus these are “Euclidean domains”.

**Definition.** *A Euclidean domain (ED) is an integral domain  $R$  possessing a function  $\phi : R - \{0\} \rightarrow \mathbf{Z}^+$ , the set of nonnegative integers, such that*

- a)  $\phi(ab) \geq \phi(a)$  for all  $a, b \in R - \{0\}$ ;
- b) for every  $d, n \in R$  with  $d \neq 0$  there exist  $q, r \in R$  such that  $n = qd + r$ , and either  $r = 0$  or  $\phi(r) < \phi(d)$ .

**Proposition.** *Every ED is a PID.*

**Proof.** Given an ideal  $I \subseteq R$ , we must find a generator for it. If  $I = 0$ , then 0 is a generator. Otherwise choose  $x \in I$  such that  $\phi(x) \leq \phi(y)$  for all  $y \in I$ ,  $y \neq 0$ . Then for any  $u \in I$ , write  $u = qx + r$  with  $\phi(r) < \phi(x)$  or  $r = 0$ . But then  $r = u - qx \in I$  so  $r = 0$  and  $u = qx \in Rx$ . Therefore  $I \subseteq Rx$ , and the reverse inclusion is obvious.

In any integral domain  $R$  we may define  $a \mid b$ , for  $a, b \in R$ , to mean:  $b = qa$  for some  $q \in R$ . Equivalently:

$$a \mid b \iff Rb \subseteq Ra.$$

We may also define a unit to be an element  $u$  such that  $Ru = R$ , or equivalently such that  $uv = 1$  for some  $v \in R$ . Two elements  $a, b \in R$  are said to be associates if and only if  $a = ub$  for some unit  $u$ .

**Exercise.** *The relation*

$$a \sim b \iff a \text{ and } b \text{ are associates}$$

*is an equivalence relation.*

Then the relation  $\mid$  is transitive, and also is “antisymmetric”, at least relative to: if  $a \mid b$  and  $b \mid a$ , then  $a = qb$  and  $b = q'a$  for some  $q, q'$ , so  $a = qq'a$  and  $a(1 - qq') = 0$ . If  $a = 0$ , then  $b = 0$ . If  $a \neq 0$ , then  $qq' = 1$  so  $q$  is a unit and  $a$  and  $b$  are associates.

We may also define a gcd of two nonzero elements  $a, b \in R$  to be an element  $d$  such that

- a)  $d \mid a$  and  $d \mid b$ ;
- b) for any  $d' \in R$  such that  $d' \mid a$  and  $d' \mid b$ , we have  $d' \mid d$ .

In any integral domain, GCD's are unique up to associates (if they exist). For if  $d$  and  $d'$  are two gcd's of the same  $a, b$ , then by definition  $d \mid d'$  and  $d' \mid d$ , so  $d$  and  $d'$  are associates.

**Proposition.** *Let  $R$  be a PID and let  $a, b \in R$ . Then there exists a gcd  $d$  of  $a$  and  $b$  in  $R$ . Moreover,  $Rd = Ra + Rb$ , so that  $d = ma + nb$  for some  $m, n \in R$ .*

**Proof.** In a PID, the set of ideals is in one-to-one correspondence with the set of associate-classes of elements of  $R$ , under  $Rx \leftrightarrow [x]$ , where  $[x]$  denotes the set of associates of  $x$ . Moreover  $x \mid y \iff Rx \supseteq Ry$ . Moreover, by definition a gcd is simply a “greatest lower bound” with respect to the divisibility relation. Hence we must prove that in the set of ideals,  $Ra + Rb$  is the least ideal containing  $Ra$  and  $Rb$ . But this is obvious.

The maximum condition holds in any PID:

**Theorem.** *In a PID, the maximum condition holds on the set of all ideals.*

**Proof.** Let  $R$  be a PID and let  $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$  be an infinite ascending chain of ideals of  $R$ . Set

$$I = \bigcup_{n=1}^{\infty} I_n.$$

Then  $I$  is an ideal, and so  $I = Rx$  for some  $x \in R$  as  $R$  is a PID. But then  $x \in I_i$  for some  $i$ , and therefore  $I \subseteq I_i$ , so  $I = I_i$ . QED

**Remark.** Virtually the same proof shows that for any commutative ring  $R$ , if every ideal of  $R$  is finitely generated then  $R$  satisfies the maximum condition on ideals. The converse to this statement is also true:

**Theorem–Definition.** If  $R$  is a commutative ring, then the following statements about  $R$  are equivalent:

- a) Every ideal of  $R$  is finitely generated.
- b) The set of ideals of  $R$  satisfies the maximum condition.
- c)  $R$  is a noetherian ring.

(Part c) is just the definition of “noetherian ring”.)

To show that b) implies a), take an ideal  $I$ . If  $I$  were not finitely generated then we could find an infinite sequence of elements  $x_1, \dots, x_n, \dots$  of  $I$  such that if  $I_i$  is the ideal generated by  $x_1, \dots, x_i$ , then

$$I_1 < I_2 < \dots < I_n \dots < I,$$

contradicting the maximum condition.

The maximum condition has two equivalent formulations: a) no infinite ascending chain  $I_1 < I_2 < \dots$  of ideals exists; b) every nonempty set of ideals has a maximal element. Indeed an infinite ascending chain has no maximal element, so b) implies a). If some nonempty set of ideals had no maximal element, then an infinite ascending chain could be obtained, starting with any ideal in the set, then any ideal proving that the first wasn't maximal in the set, then any ideal proving that *that* one wasn't maximal, etc.

Now we can generalize the theorem of the previous section, with the identical proof. First of all we make the following definition.

**Definition.** Let  $R$  be a ring with 1. A (left)  $R$ -module is an abelian group  $M$  equipped with a “scalar multiplication”

$$R \times M \rightarrow M, \quad \text{written } (r, m) \mapsto rm,$$

such that the following conditions hold for all  $r, s \in R$  and all  $m, n \in M$ :

- a)  $r(m + n) = rm + rn$ ;
- b)  $(r + s)m = rm + sm$ ;
- c)  $r(sm) = (rs)m$ ;
- d)  $1m = m$ .

The usual trivial consequences follow, as with vector spaces:  $0m = 0$ ,  $r0 = 0$  and  $r(-m) = -(rm) = (-r)m$  for all  $r \in R$  and  $m \in M$ .

**Definition.** Let  $M$  and  $N$  be  $R$ -modules. An  $R$ -homomorphism from  $M$  to  $N$ , or a homomorphism of  $R$ -modules from  $M$  to  $N$ , is a homomorphism  $\phi : M \rightarrow N$  of abelian groups such that  $\phi(rm) = r\phi(m)$  for all  $r \in R$ ,  $m \in M$ .

Thus an  $R$ -module is in particular an abelian group with operators  $R$  (satisfying the extra conditions b), c) and d) above), and an  $R$ -homomorphism is precisely a homomorphism of  $R$ -groups.

**Definition.** *If  $M$  is an  $R$ -module, then an  $R$ -submodule of  $M$  is an additive subgroup  $N$  of  $M$  such that  $rN \subseteq N$  for all  $r \in R$ .*

An  $R$ -submodule is thus an  $R$ -subgroup, in the terminology of groups with operators.

Thus

The Noether isomorphism theorems hold for  $R$ -modules.

and the Jordan-Hölder theorem does as well.

The terms “homomorphism”, “subgroup” have to be replaced by “ $R$ -homomorphism” and “ $R$ -submodule”. The parallelogram law reads

$$(N + P)/N \cong P/(N \cap P)$$

for any  $R$ -submodules  $N$  and  $P$  of an  $R$ -module  $M$ . (The analogue of the hypothesis  $H \leq N_G(K)$  is automatically true since the group operation on  $M$  is commutative.)

Given an  $R$ -module  $M$  and a subset  $S \subseteq M$ , the  $R$ -submodule of  $M$  generated by  $S$  is defined to be the intersection of all submodules of  $M$  containing  $S$ , or equivalently the set of all elements of  $M$  representable as “ $R$ -linear combinations”  $\sum_i r_i s_i$  with all  $r_i \in R$ , all  $s_i$  in  $S$ , and almost all  $r_i = 0$ .

An  $R$ -module  $M$  is “cyclic” if and only if it is generated by a single element. We claim that  $M$  is cyclic if and only if  $M \cong {}_R R/A$  for some ideal  $A$  of  $R$ . If  $M$  is generated by  $m$ , then

$${}_R R \rightarrow M, r \mapsto rm$$

is a surjective homomorphism and so  $M \cong R/A$  where  $A = \{r \in R \mid rm = 0\}$  is the “annihilator” of  $m$ . Conversely, Conversely,  ${}_R R$  is generated as an  $R$ -module by 1, hence is cyclic, and so any quotient of it is generated by a single element as well.

The notions of direct sum and product go over as well to  $R$ -modules: the direct product and sum of  $R$ -modules are both  $R$ -modules, with scalar multiplication being defined coordinate by coordinate, e.g., in the  $R$ -module  $M \oplus N$ ,  $r(m, n) = (rm, rn)$  by definition. The usual universal properties hold for direct sums and products. In particular, if  $N$  and  $P$  are submodules of the  $R$ -module  $M$ , then  $M = N \oplus P$  if and only if  $N + P = M$  and  $N \cap P = 0$ .

The ring  $R$  is itself a (left)  $R$ -module; its submodules are precisely its (left) ideals. The notation for this module is  ${}_R R$ .

**Definition.** *Let  $R$  be a ring. A free (left)  $R$ -module (on a set  $I$ ) is the direct sum of copies of the  $R$ -module  ${}_R R$  (indexed by  $I$ ).*

We may also define a basis of an  $R$ -module  $M$  to be a subset  $B \subseteq M$  such that each  $m \in M$  has a unique expression

$$m = \sum_{b \in B} r_b b$$

with almost all coefficients  $r_b = 0$ .

As with free abelian groups,  $M$  is a free (left)  $R$ -module on  $I$  if and only if it has a (left) basis indexed by  $I$ , and these conditions are equivalent to the existence of a mapping  $\iota : I \rightarrow M$  satisfying the usual universal mapping property.

Namely, if  $M = \bigoplus_{i \in I} R$ , then  $\iota$  takes  $i \in I$  to  $\iota(i) =$  the element of  $M$  which is 0 in all coordinates but the  $i$ -th coordinate, and which is 1 in that coordinate. This mapping has the usual universal property: for any  $R$ -module  $N$  and any (set) map  $\psi : I \rightarrow N$  there is a unique homomorphism  $\Psi : M \rightarrow N$  (of  $R$ -modules) such that  $\Psi \circ \iota = \psi$ .

As with abelian groups any two free  $R$ -modules on the same set  $I$  are isomorphic. The commutativity of  $R$  allows us to prove as well that the cardinality of  $I$  is determined by the isomorphism type of the corresponding free module.

**Proposition.** *Let  $R$  be a PID, or indeed any commutative ring with 1. Let  $M$  be an  $R$ -module which is free on a set  $I$  and also free on a set  $J$ . Then  $|I| = |J|$ .*

**Proof.** Choose any maximal ideal\*  $A$  of  $R$ . Define  $AM$  to be the submodule of  $M$  generated by all products  $am$ ,  $a \in A$ ,  $m \in M$ . Set  $M_I = \bigoplus_{i \in I} R$ , so that  $M \cong M_I$ . Under such an isomorphism,  $AM$  corresponds to  $AM_1$ , so  $M/AM \cong M_I/AM_I$ . However, it is clear that  $AM_I = \bigoplus_{i \in I} A$ , and so  $M_I/AM_I \cong \bigoplus_{i \in I} R/A$ .

Now  $M/AM$  is an  $R$ -module and  $ax = 0$  for all  $a \in A$  and  $x \in M/AM$ . We may therefore try (and succeed) making  $M/AM$  into an  $R/A$ -module by defining

$$(r + A)x = rx$$

for all  $r \in R$ . The fact that  $Ax = 0$  makes this a good definition, and the module axioms may be checked without incident.

In the same way we may make  $M_1/AM_1$  an  $R/A$ -module, and our  $R$ -isomorphism between  $M/AM$  and  $M_1/AM_1$  is also an  $R/A$ -isomorphism, because of the way the  $R/A$ -module structure has been defined on these modules. Therefore, as  $R/A$ -modules, we have

$$M/AM \cong M_1/AM_1 \cong \bigoplus_{i \in I} R/A$$

But since  $A$  is a maximal ideal,  $R/A$  is a field, and the three objects above are vector spaces over  $R/A$ . Thus  $|I| = \dim_{R/A}(M/AM)$ , which equals  $|J|$  by a similar argument.

QED

Moreover, the universal property as usual implies:

---

\* That is,  $A < R$  and there exist no ideals  $B$  of  $R$  such that  $A < B < R$ . The existence of maximal ideals in a (commutative) ring follows quickly from Zorn's Lemma, q.v. In the case of PID's, we know that the set of all ideals satisfies the maximum condition and so maximal ideals of course exist.

**Theorem 0<sup>R</sup>.** *Let  $R$  be any ring. Then every (left)  $R$ -module is a quotient of a free (left)  $R$ -module. More precisely, if  $M$  is an  $R$ -module and  $S \subseteq G$  is a subset such that  $\langle S \rangle = M$ , then there is a surjective homomorphism*

$$\phi : F \rightarrow M,$$

where  $F$  is a free  $R$ -module on  $S$ ; thus  $M \cong F/\ker \phi$ .

Now we can repeat the development of the previous section.

**Theorem 1<sup>R</sup>.** *Suppose that  $G$  is an  $R$ -module and  $H$  is a submodule such that  $G/H$  is free. Then  $G = H \oplus K$  for some  $R$ -submodule  $K \leq G$ .*

**Proof.** Choose a basis  $B$  for  $G/H$  and choose an arbitrary preimage of each element of  $B$ , thereby forming a subset  $C \subset G$ . Let  $K$  be the  $R$ -submodule generated by  $C$ . The freeness of  $G/H$  implies that  $\pi_H|_K$  is an isomorphism between  $K$  and  $G/H$ . This in turn means that  $H \cap K = 0$  and  $H + K = G$ , as required.

**Theorem 2<sup>R</sup>.** *Let  $R$  be a PID. Any submodule  $H$  of a finitely generated free  $R$ -module  $G$  is a free  $R$ -module. Moreover the rank of  $H$  is at most the rank of  $G$ .*

**Proof.** Let  $\{e_1, \dots, e_n\}$  be a basis of  $G$ . The proof is by induction on  $n$ . Let  $G_0 = Re_1 + \dots + Re_{n-1}$  and  $H_0 = H \cap G_0$ . Then by induction  $H_0$  is a free  $R$ -module of rank  $r \leq n-1$ . Moreover  $H/H_0 \cong H + G_0/G_0 \leq G/G_0 \cong Re_n \cong R$ . Hence  $H/H_0 \cong R$  or  $0$ . In the first case there exists  $K \leq H$  such that  $H = H_0 \oplus K$ , so  $H$  is a free  $R$ -module of rank  $r+1 \leq n$ . In the second case the desired conclusion is obvious.

**Corollary.** *Let  $R$  be a PID. Then any submodule of a finitely generated  $R$ -module is finitely generated.*

**Proof.** If  $H \leq G$  with  $G$  finitely generated, we may write  $G = F/R$  where  $F$  is finitely generated free. Then  $H = F_0/R$  for some  $R \leq F_0 \leq F$  by the third isomorphism theorem, and the theorem implies that  $F_0$  is finitely generated. *A fortiori*,  $H$  is finitely generated.

The main theorem is formulated as a theorem about the relationship between appropriate bases of a free module over a PID  $R$ , and a submodule. It will be applied in the next section in the context of Theorem 0 to the inclusion  $\ker \phi \rightarrow F$  (note that Theorem 2 tells us that  $\ker \phi$  is itself finitely generated and free, given that  $F$  is). It will yield structural information about the quotient  $F/\ker \phi$ , which as Theorem 0 shows is an arbitrary finitely generated  $R$ -module.

The theorem has an existence and a uniqueness statement. We shall prove the existence now; the uniqueness assertion will be argued after we formulate and prove the main theorem (see Section 1g) for arbitrary finitely generated modules over the PID  $R$ .

**Fundamental theorem on finitely generated modules over a PID (Ia: free module version).** *Let  $R$  be a PID. Let  $M$  be a finitely generated free  $R$ -module, of rank  $s$ ,*

and  $N$  a submodule of  $M$ . Then  $N$  is a finitely generated free  $R$ -module, of rank  $r \leq s$ . Moreover there exist bases  $h_1, \dots, h_r$  of  $N$  and  $e_1, \dots, e_s$  of  $M$ , and nonzero elements  $m_1, \dots, m_r \in R$ , the  $m_i$ 's being uniquely determined up to associates, such that

- a)  $f_i = m_i e_i, i = 1, \dots, r$ , and
- b)  $m_1 | m_2 | \dots | m_r$ .

Again, the bases  $\{e_i\}$  and  $\{h_i\}$  are not uniquely determined.

**Proof of existence.** First some observations about ( $R$ -module) homomorphisms  $M \rightarrow {}_R R$ . These form an  $R$ -module  $\text{Hom}_R(M, {}_R R)$  under  $(\phi + \psi)(m) = \phi(m) + \psi(m)$  and  $(r\phi)(m) = r(\phi(m))$  for all  $m \in M$  and  $r \in R$ . Checking that  $\phi + \psi$  is a homomorphism requires the commutativity of addition in the image  $R$ ; checking that  $r\phi$  is a homomorphism (in particular, that it preserves scalar multiplication) requires the commutativity of multiplication in  $R$ ; for any  $r, s \in R$  and  $m \in M$ , and  $\phi \in \text{Hom}_R(M, {}_R R)$ ,

$$(r\phi)(sm) = r(\phi(sm)) = r(s\phi(m)) = (rs)\phi(m) = (sr)\phi(m) = s(r\phi(m)) = s[(r\phi)(m)].$$

The identity element of  $\text{Hom}_R(M, {}_R R)$  is the 0 mapping  $0(m) = 0$  for all  $m \in M$ ; the inverse of  $\phi$  is  $-\phi$ , defined by  $(-\phi)(m) = -(\phi(m))$  for all  $m \in M$ . Furthermore, every choice of an (ordered) basis  $B = \{e_1, \dots, e_n\}$  of  $M$  gives rise to coordinate mappings  $\phi_i : M \rightarrow R$  (depending on  $B$ ), namely with  $\phi_i(\sum_j n_j g_j) = n_i$ ; each such coordinate mapping lies in  $\text{Hom}_R(M, {}_R R)$ .

Now to the proof of the theorem. By Theorem 2,  $N$  is free abelian of rank  $r \leq n$ .

We consider the set of all images

$$\Phi = \{\phi(N) \mid \phi \in \text{Hom}(M, {}_R R).\}$$

Each  $\phi(N)$  is an ideal of  $R$ , and so the maximum condition implies that we may select and fix  $\phi \in \text{Hom}(M, {}_R R)$  such that  $\phi(N)$  is maximal in  $\Phi$ , i.e., whenever  $\phi' \in \text{Hom}(M, {}_R R)$  and  $\phi'(N) \geq \phi(N)$ , then  $\phi'(N) = \phi(N)$ . As an ideal of  $R$ ,

$$\phi(N) = Rm_1$$

for some  $m_1 \in R$ .

If  $m_1 = 0$ , then  $\phi(N) = 0$  for all  $\phi \in \text{Hom}(M, {}_R R)$ . But for any basis of  $M$ , each basis-coordinate function is a homomorphism, so annihilates  $N$ . Therefore  $N = 0$ , and the theorem holds with  $r = 0$ . So we may assume that

$$m_1 \neq 0.$$

Next let us show that  $\phi$  is surjective, i.e.,

$$\phi(M) = R.$$

Of course  $\phi(M) = Ra$  for some  $a$ , since  $\phi(M)$  is an ideal of  $R$ . Since  $R$  is an integral domain, every element of  $Ra$  has the form  $ra$  for a unique  $r \in R$ . Therefore we may write

$$\phi(m) = \psi(m)a$$

where  $\psi$  is a well-defined function  $M \rightarrow R$ . The additivity of  $\phi$ , and the fact that  $R$  is an integral domain so obeys the cancellation law, implies that  $\psi$  is additive, and similarly,  $\psi$  is an  $R$ -homomorphism. From the above equation,  $\phi(N) = a\psi(N) \subseteq \psi(N)$ . The maximality of  $\phi(N)$  implies therefore that  $\psi(N) = a\psi(N)$ . Therefore  $a$  is a unit, and so  $\phi(M) = Ra = R$ , as claimed.

Now we can choose and fix  $h_1 \in N$ , as any element of  $N$  such that  $\phi(h_1) = m_1$ . The homomorphism  $\phi|_N : N \rightarrow Rm_1$  maps the submodule  $Rh_1$  of  $N$  onto  $Rm_1 = \phi(N)$ , and so

$$N = Rh_1 \oplus \ker(\phi|_N) = Rh_1 \oplus (K \cap N),$$

where we have put

$$K = \ker(\phi).$$

Likewise  $\phi : M \rightarrow R$  is surjective, and if we choose any  $f_1 \in M$  such that  $\phi(f_1) = 1$ , we similarly get

$$M = Rf_1 \oplus K$$

The next objective is to show that  $f_1$  may be replaced by  $e_1 \in M$  satisfying  $h_1 = m_1e_1$ . The submodule  $K$  of  $M$  is free, and we choose a basis  $f_2, \dots, f_n$  of it. Then  $f_1, \dots, f_n$  form a basis of  $M$ , and so  $h_1 = r_1f_1 + \dots + r_nf_n$  for some  $r_i \in R$ . Applying  $\phi$  we get  $m_1 = r_1 + 0 = r_1$ . Thus  $h_1 = m_1f_1 + r_2f_2 + \dots + r_nf_n$ .

We show that  $m_1 | r_i$  for all  $i \geq 2$ . Let  $\phi_i$  be the  $i$ -th coordinate function on  $M$  with respect to  $f_1, \dots, f_n$ . Then  $\phi_2(h_1) = r_2$ . Let  $d$  be a gcd of  $m_1$  and  $r_2$  and write  $d = am_1 + br_2$ ,  $a, b \in R$ . Then  $(a\phi + b\phi_2)(h_1) = d$ . The image of  $a\phi + b\phi_2$  thus contains  $Rd$  and hence  $Rm_1$ . The maximality of  $Rm_1$  then implies that  $Rd = Rm_1$ , so  $m_1$  divides  $r_2$ . Similarly it divides  $r_i$  for all  $i \geq 2$ , and we write  $r_i = m_1s_i$ .

Set  $e_1 = f_1 + s_2f_2 + \dots + s_nf_n$ . Then  $h_1 = m_1f_1 + m_1s_2f_2 + \dots = m_1e_1$ . Moreover,  $\phi(e_1) = 1$  since  $\phi(f_i) = 0$  for all  $i \geq 2$ . Therefore

$$M = Re_1 \oplus K \text{ and } h_1 = m_1e_1.$$

Clearly  $K$  has rank  $n - 1$ . If  $K = 0$  (i.e.,  $n = 1$ ), then there is nothing more to prove. If  $K \neq 0$ , then by induction on  $n$ , applied to  $K \cap N \subseteq K$ , there are bases  $e_2, \dots, e_n$  of  $K$  and  $h_2, \dots, h_r$  of  $K \cap N$  and positive integers  $m_2, \dots, m_r \in R$  such that  $h_j = m_je_j$ ,  $2 \leq j \leq r$ , and  $m_2 \mid \dots \mid m_r$ . Then  $e_1, e_2, \dots, e_n$  form a basis of  $M$ , and the  $h_i$  form a basis of  $N$ , so to complete the proof of existence it remains only to check that

$$m_1 \mid m_2.$$

Let  $\phi_i$  now be the coordinate functions on  $M$  with respect to  $e_1, \dots, e_n$ . Then as  $h_1 + h_2 = m_1e_1 + m_2e_2$ , we have  $\phi_1(h_1 + h_2) = m_1$  and  $\phi_2(h_1 + h_2) = m_2$ . Thus for suitable  $a, b \in R$ ,

$(a\phi_1 + b\phi_2)(h_1 + h_2) = d$ , a gcd of  $m_1$  and  $m_2$ . As before,  $Rm_1 \subseteq Rd \subseteq \text{im}(a\phi_1 + b\phi_2)$ , so the maximality of  $Rm_1$  implies that  $Rm_1 = Rd$ , so  $m_1|m_2$ . This completes the proof of existence in Theorem Ia.

We have only proved existence here; the uniqueness assertion will be proved later.

The association classes  $[m_1], [m_2], \dots, [m_r]$ , or more sloppily the elements  $m_1, \dots, m_r \in R$ , are sometimes called the “invariant factors” of the inclusion mapping  $E \rightarrow F$ .

**Exercise.** *State and prove the analogue of version Ib for matrices with entries in PID.*

## 1f. Finitely Generated Abelian Groups and Modules over PID's

In the next two sections we apply the previous theorem to determine the structure of finitely generated modules over a PID. We also complete the (uniqueness) proof of the previous theorem!

In any abelian group  $G$ , the set

$$T(G) = \{g \in G \mid g \text{ has finite order}\}$$

is a subgroup of  $G$ , since  $mg = nh = 0$  implies  $mn(g - h) = 0$ . It is called the torsion subgroup of  $G$ . The group  $G$  is called torsion-free if and only if  $T(G) = 0$ .

Likewise if  $M$  is a module over a PID  $R$ , we define

$$T(M) = \{m \in M \mid \text{for some } 0 \neq r \in R, rm = 0\}.$$

In a similar way we see that  $T(M)$  is a submodule of  $M$ . (This actually only requires  $R$  to be an integral domain.) The module  $M$  is called torsion-free if and only if  $T(M) = 0$ .

**Exercise.**  $T(M)$  is “fully invariant”, that is, for every homomorphism  $\phi : M \rightarrow M$  of  $R$ -modules, we have  $\phi(T(M)) \leq T(M)$ .

**Proposition.** *Let  $R$  be a PID (or any integral domain). Let  $M$  be an  $R$ -module. Then  $T(M)$  is a submodule of  $M$ , and  $M/T(M)$  is torsion-free.*

**Proof.** If  $rm = sn = 0$  with  $r \neq 0 \neq s$ , then  $rs(m \pm n) = 0$  with  $rs \neq 0$ . Hence  $T(M)$  is a submodule of  $M$ . If  $x + T(M) \in T(M/T(M))$ , then  $rx \in T(M)$  for some  $r \neq 0$ . Therefore  $srx = 0$  for some  $s \neq 0$ , and as  $sr \neq 0$ , this gives  $x \in T(M)$ . This proves that  $T(M/T(M)) = 0$ .

**Fundamental theorem on finitely generated modules over a PID (II: invariant factor version).** *Let  $R$  be a PID. Let  $M$  be finitely generated module over a PID  $R$ . Then  $M = T(M) \oplus N$  for some submodule  $N \leq M$ . Moreover  $N$  is a free  $R$ -module, and there exist  $m_1, \dots, m_r \in R$  such that no  $m_i$  is a unit,  $m_1 \mid \dots \mid m_r$  and*

$$T(M) \cong Z_{m_1} \oplus \dots \oplus Z_{m_r}.$$

*The rank of  $N$ , and the association classes  $[m_1], \dots, [m_r]$  are uniquely determined (by  $M$ ).*

This theorem implies, and indeed is equivalent to the following three results:

**Theorem 3.** *Finitely generated torsion-free modules over a PID are free modules.*

**Theorem 4.** *If  $M$  is a finitely generated module over a PID, then  $M \cong T(M) \oplus M/T(M)$ .*

**Theorem 5.** *If  $M$  is a finitely generated torsion module over a PID (“torsion” means  $M = T(M)$ ), then  $M \cong R/m_1R \oplus \cdots \oplus R/m_rR$  for some  $r \geq 0$  and some nonunits  $m_1, \dots, m_r \in R$  such that  $m_1 \mid \cdots \mid m_r$ . The association classes  $[m_1], \dots, [m_r]$  are uniquely determined by these conditions.*

**Exercise.** *Demonstrate the equivalence just asserted.*

**Proof** The “existence” statements are an application of version I of the theorem. Namely, by Theorem 0 there is a finitely generated free module  $F$  and a submodule  $K$  such that  $M \cong F/K$ . By Theorem 1,  $K$  is free, and by the main theorem there are bases  $\{e_i\}_{1 \leq i \leq s}$  and  $\{f_i\}_{1 \leq i \leq r}$  of  $F$  and  $K$  respectively such that  $r \leq s$  and  $f_i = m_i e_i$  for each  $i \leq r$ , where  $m_i \in R$  and  $m_1 \mid \cdots \mid m_r$ . Letting  $F_i = \langle e_i \rangle$ , and setting  $m_i = 0$  for  $r < i \leq s$  we have

$$M \cong F/K = (\oplus_{i=1}^s F_i) / (\oplus_{i=1}^s m_i F_i) \cong \oplus_{i=1}^s F_i / m_i F_i \cong (\oplus_{i=1}^r R/m_i R) \bigoplus (\oplus_{i=r+1}^s R).$$

Obviously the first summand corresponds to  $T(M)$ , and the second summand is free of rank  $s - r$ . Furthermore, for those  $m_i$  which are units,  $R/m_i R = 0$ , so we may delete them from the final expression. This proves everything but uniqueness.

Now  $s - r$  is the rank of  $M/T(M)$ , so is uniquely determined by  $M$ . It remains to show that the  $m_i$  in the statement of the theorem (i.e., the nonunits) are uniquely determined up to associates.

Notice that our argument shows more, namely that the  $m_i$  coming from a submodule  $N \leq M$  in version I are the same as the  $m_i$  coming from the module  $M/N$  in version II, except that enough units are added to bring the rank of  $N$  up to  $r = s - (s - r)$ , the rank of  $M$  minus the torsion-free rank of  $M/N$ . Consequently knowing the rank of  $M$  and the invariant factors of  $M/N$  determines the  $m_i$  in version I. Therefore

*uniqueness in version II implies uniqueness in version I.*

What remains for us to do, therefore, is prove uniqueness in version II.

## 1g. Primary Decomposition; PID's are UFD's

A further decomposition can be made, using the Chinese Remainder Theorem. For the case  $R = \mathbf{Z}$  this theorem states that  $\mathbf{Z}_n$  is isomorphic to the direct product (or sum!) of the groups  $\mathbf{Z}_{p_i^{e_i}}$ , where  $n = \prod_i p_i^{e_i}$  is the factorization of  $n$  into powers of *distinct* primes. (In a homework exercise you showed that the direct product of two finite cyclic groups of relatively prime orders is a cyclic group, and this implies the C.R.T. for the integers.) By applying the C.R.T. to each of the summands  $\mathbf{Z}_{m_i}$  in the fundamental theorem on finitely generated abelian groups, we get a decomposition of  $T(G)$  as the direct sum of cyclic groups of prime power order. Moreover, a uniqueness statement can be obtained here as well. But before doing this for PID's, we need the C.R.T. for them. Indeed we need to prove the fundamental theorem of arithmetic for them!

**Definition.** Let  $R$  be an integral domain, and let  $p \in R$ . Then  $p$  is prime if and only if  $p \neq 0$ ,  $p$  is not a unit, and whenever  $a, b \in R$  are such that  $p \mid ab$ , then either  $p \mid a$  or  $p \mid b$ .

**Definition.** Let  $R$  be an integral domain, and let  $p \in R$ . Then  $p$  is irreducible if and only if  $p \neq 0$ ,  $p$  is not a unit, and in any factorization  $p = ab$ ,  $a, b \in R$ , either  $a$  or  $b$  is a unit.

These two notions, identical if  $R = \mathbf{Z}$ , are conceptually different and are not identical in general. For example, in  $R = \mathbf{Z}[\sqrt{-5}]$ , the ring of all integer combinations  $a + b\sqrt{-5}$ , if we put  $z = 1 + 2\sqrt{-5}$ , then

$$3 \cdot 7 = z \cdot \bar{z}$$

the bar denoting complex conjugation. Thus  $3 \mid z \cdot \bar{z}$ , although it is easily checked that 3 does not divide  $z$  or  $\bar{z}$ . Hence 3 is not prime. However, 3 is irreducible. Indeed the norm mapping  $N : R \rightarrow \mathbf{Z}$ ,  $N(x) = x\bar{x}$ , is multiplicative, and  $N(3) = 9$ . A factorization  $3 = xy$  would give  $N(x)N(y) = 9$ . However, using  $N(a + b\sqrt{-5}) = a^2 + 5b^2$ , we see that no element of  $R$  has norm 3, so either  $N(x) = 1$  or  $N(y) = 1$ , which in turn implies that  $x$  or  $y$  is  $\pm 1$ , a unit. Hence “irreducible” does not imply “prime” in general. (The problem is that the F.T. of Arithmetic does not extend from  $\mathbf{Z}$  to  $R$ .)

**Lemma.** In any integral domain, prime implies irreducible.

**Proof.** Suppose that  $p = ab$  and  $p$  is prime. Then  $p \mid ab$ , so  $p$  divides one of the factors, which we may as well assume is  $a$ . Thus  $a = pc$  for some  $c$ . Now  $p = pcb$ , so  $1 = cb$  as we are in an integral domain. Therefore  $b$  is a unit. QED

**Lemma.** In a PID, irreducible implies prime.

**Proof.** The key is that GCD's of two elements exist in a PID (Section 1d), and are linear combinations of the two elements. Suppose that  $R$  is a PID and  $p \in R$  is irreducible, and  $p \mid ab$ . Suppose that  $p$  does not divide  $a$ . Let  $d = \gcd(p, a)$ , well-defined up to associates. If  $[d] = [p]$ , then  $p \mid a$ , contradiction. But by irreducibility the only other divisors of  $p$  are units, so  $[d] = [1]$ . Hence there are  $m, n \in R$  such that  $mp + na = 1$ . Then  $b = bmp + nab$ , and as  $p \mid ab$  we get  $p \mid b$ . QED

**Definition.** A unique factorization domain (UFD) is an integral domain  $R$  such that for every  $x \in R$  such that  $x \neq 0$ , there exists a unit  $u$ , an integer  $n \geq 0$ , primes  $p_1, \dots, p_n$ , no two of which are associates, and positive integers  $e_1, \dots, e_n$  such that

$$x = up_1^{e_1} \cdots p_n^{e_n};$$

moreover, this decomposition is unique, except for “trivial changes” of the following sorts: rearrange the order of terms, and replace some  $p_i$  by an associated element (changing  $u$  in the process as well).

**Theorem.** Every PID is a UFD.

**Proof.** Let  $R$  be a PID. The existence of a factorization uses only the property that the ideals of  $R$  satisfy the maximum condition: Suppose by way of contradiction that some

element  $x \neq 0$  of  $R$  has no factorization as a product of a unit and irreducibles, and among all counterexamples choose one such that the ideal  $Rx$  is maximal. Now  $x$  is itself not irreducible, otherwise it would have the factorization  $x = x$ . So  $x = yz$  for some nonunits  $y$  and  $z$ . Clearly  $x \in Ry$ , so  $Rx \subseteq Ry$ . Likewise  $Rx \subseteq Rz$ . If both these inclusions are proper, then  $y$  and  $z$  would have factorizations, which when put together would give a factorization of  $x$ , contradiction. Therefore  $Rx = Ry$ , say. But then  $x$  and  $y$  are associates and so  $z$  is a unit, contradiction.

The uniqueness uses only the fact that every irreducible is prime. Suppose that

$$x = u \prod_i p_i^{e_i} = v \prod_j q_j^{f_j}$$

with the  $p_i$  distinct irreducibles,  $u$  a unit, the  $e_i$  positive integers, and similar conditions on the right side. Then  $p_1 \mid x$ . Since  $p_1$  is prime and divides the right side,  $p_1 \mid q_j$  for some  $j$ . But  $q_j$  is irreducible and so  $[p_1] = [q_j]$ . We may change notation so that  $[p_1] = [q_1]$ , so that  $p_1 = wq_1$ ,  $w$  a unit. We may now cancel one  $p_1$  from the left, cancel one  $q_1$  from the right and replace  $v$  by  $vw^{-1}$ , and then complete the proof by induction on  $\sum_i e_i$ . QED

**Corollary.** *In a PID, the gcd of two elements  $a$  and  $b$  is the product of all the “common” factors in the prime factorizations of  $a$  and  $b$ .*

Here “common” means “up to associates”; recall that gcd's are only well-defined up to associates, anyway.

**Chinese Remainder Theorem.** *Let  $R$  be a commutative ring with 1. Let  $I_1, \dots, I_n$  be ideals of  $R$  such that for each  $i \neq j$ ,  $I_i + I_j = R$ . Define  $I_1 \cdots I_n$  to be the ideal of  $R$  generated by all products  $r_1 \cdots r_n$  with  $r_i \in I_i$  for each  $i$ . Then there is an isomorphism of  $R$ -modules*

$$\frac{R}{I_1 \cdots I_n} \cong \frac{R}{I_1} \oplus \cdots \oplus \frac{R}{I_n}.$$

The hypothesis  $I_i + I_j = R$  is absolutely essential here!

**Proof.** The  $R$ -module homomorphism

$$\phi : R \rightarrow \frac{R}{I_1} \oplus \cdots \oplus \frac{R}{I_n}, \quad r \mapsto (r + I_1, \dots, r + I_n)$$

has kernel  $I_1 \cap \cdots \cap I_n$ . We finish the proof by showing

- a)  $I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$ ;
- b)  $\phi$  is onto.

Indeed,

$$R = R \cdot R \cdots R = (I_1 + I_2)(I_1 + I_3) \cdots (I_1 + I_n) \subseteq I_1 + (I_2 \cdots I_n).$$

In particular every coset of  $I_1$  in  $R$  contains an element of  $I_2 \cdots I_n$ , which shows that the image of  $\phi$  contains the first direct factor  $R/I_1$ . Similarly it contains the others, so  $\phi$  is

onto. To prove a), it is obvious that the product of ideals lies in their intersection, by definition of ideal. The displayed equation has an analogue  $R = I_i + I_1 \cdots \hat{I}_i \cdots I_n$  for each  $i$  ( $\hat{I}_i$  means to omit this term). Multiplying these  $n$  equations we find that

$$R = \hat{I}_1 I_2 \cdots I_n + I_1 \hat{I}_2 \cdots I_n + \cdots + I_1 I_2 \cdots \hat{I}_n.$$

Putting  $J = \cap_{i=1}^n I_i$  we see that the product of  $J$  with any one of these summands lies in  $I_1 I_2 \cdots I_n$ . Hence

$$J = RJ \subseteq I_1 I_2 \cdots I_n.$$

□

**Corollary.** *Let  $R$  be a PID and let  $x = up_1^{e_1} \cdots p_n^{e_n}$  be the primary decomposition of  $x \in R$ . Then*

$$R/Rx \cong R/Rp_1^{e_1} \oplus \cdots \oplus R/Rp_n^{e_n}.$$

It is vital here that the  $p_i$  be non-associated with one another.

**Proof.** Since the  $p_i$  are non-associated with one another,  $\gcd(p_i^{e_i}, p_j^{e_j}) = 1$  for  $i \neq j$  by the last corollary. So  $Rp_i^{e_i} + Rp_j^{e_j} = R$ . Now apply the previous result with  $I_i = Rp_i^{e_i}$ . □

Now we can formulate the third and last version of our main theorem on finitely generated modules over a PID.

**Fundamental theorem on finitely generated modules over a PID (III: elementary divisor version).** *Let  $R$  be a PID. Let  $M$  be finitely generated module over a PID  $R$ . Then  $M = T(M) \oplus N$  for some submodule  $N \leq M$ . Moreover  $N$  is a free  $R$ -module, and there exist prime powers  $p_1^{e_1}, \dots, p_s^{e_s}$  in  $R$  such that*

$$T(M) \cong Z_{p_1^{e_1}} \oplus \cdots \oplus Z_{p_s^{e_s}}.$$

*The rank of  $N$  is uniquely determined by  $M$ , as are the association classes  $[p_1^{e_1}], \dots, [p_s^{e_s}]$  (except for the order in which they appear).*

To prove the existence of this decomposition, use version II, factor each  $m_i$  as the product of powers of distinct primes, and apply the Chinese Remainder Theorem.

Conversely, the set of resulting prime powers (counting multiplicities!) determines the sequence  $m_1, \dots, m_r$ . That is, if  $m_1 \mid \cdots \mid m_r$ , we can recover  $m_1, \dots, m_r$  from the list of the prime powers appearing in the decompositions of  $m_1, \dots, m_r$ . Namely, for each prime which appears, the largest power of that prime divides some  $m_i$  and hence divides  $m_r$ . Hence  $m_r$  must be the product, over all (distinct) primes appearing, of the largest powers of those primes which occur. Removing these from consideration  $m_{r-1}$  must be the product, over all primes still remaining, of their largest powers still remaining, etc.

Thus

*Uniqueness in version III implies uniqueness in version II.*

Therefore it remains only to show uniqueness in version III.

**Exercise.** Show that the decomposition of  $T(G)$  into “primary” parts does not depend on the finite generation of  $G$ . More precisely, let  $G$  be a module over the PID  $R$ , and assume that  $G = T(G)$ . For each association class  $[p]$  of primes in  $R$  define

$$G_p = \{g \in G \mid p^n g = 0 \text{ for some positive integer } n\}.$$

Show that

- a) Each  $G_p$  is an  $R$ -submodule of  $G$ .
- b)  $G = \coprod G_p$ , with one summand for each association class of primes in  $R$ .

## 1h. Uniqueness

We finally complete the proof of the fundamental theorem by proving uniqueness in version III. We use the invariants  $M[x]$  and  $xM$  of a torsion module  $M$  over a PID  $R$ .

**Definition.** Let  $M$  be a module over the commutative ring  $R$ . For each  $x \in R$  define  $M[x] = \{m \in M \mid xm = 0\}$  and  $xM = \{xm \mid m \in M\}$ .

It is obvious that each of these is a submodule of  $M$  for any  $x \in R$ . Furthermore, we may consider  $M[x]$  to be an  $R/xR$ -module by defining  $(r + xR)m = rm$  for each  $m \in M[x]$ . Moreover the following lemmas are easy to prove.

**Lemma.** Suppose that  $M$  and  $N$  are  $R$ -modules and  $M = M[x]$ ,  $N = N[x]$ . Then a mapping  $\phi : M \rightarrow N$  is an  $R$ -homomorphism if and only if it is an  $R/xR$ -homomorphism.

**Lemma.** If  $R$  is a commutative ring and  $M$  and  $M_i$  are  $R$ -modules such that  $M = \coprod M_i$ , then  $M[x] = \coprod M_i[x]$  and  $xM = \coprod xM_i$  for each  $x \in R$ .

**Lemma.** Let  $R$  be a PID, and  $M = R/p^n R$ , where  $p^n$  is a prime power in  $R$ ,  $n \geq 0$ . Then

- a) If  $q \in R$  is a prime not associated with  $p$ , then  $M = qM$  and  $M[q] = 0$ .
- b)  $M[p] \cong R/pR$  (both as  $R$ -module and as  $R/pR$ -module).
- c) If  $r \in \mathbf{Z}^+$ , then

$$p^r M[p] \cong \begin{cases} R/pR & \text{if } r < n \\ 0 & \text{otherwise.} \end{cases}$$

- d) If  $p'$  is a prime associated with  $p$ , then  $M[p] = M[p']$  and  $p^r M = (p')^r M$  for any  $r$ .

**Proof.** Under the canonical projection  $\phi : R \rightarrow R/p^n R = M$ , we have  $\phi(qR) = qM$ . But  $\gcd(q, p^n) = 1$  so  $qR + p^n R = R$ . Hence  $M = \phi(R) = \phi(qR) = qM$ . Similarly, if  $m \in M[q]$ , then  $m = r + p^n R$  for some  $r \in R$ , and  $qr \in p^n R$ . Therefore  $p^n \mid qr$ , so  $p^n \mid r$  by unique factorization, so  $m = 0$ . This proves a).

Next, the preimage of  $M[p]$  is the ideal  $\{r \in R \mid pr \in p^n R\}$ , i.e., the ideal  $p^{n-1}R$ . So  $M[p] = p^{n-1}R/p^n R$ . Define  $\psi : R \rightarrow M[p]$  by  $\psi(r) = p^{n-1}r + p^n R$ . This is a surjective

module homomorphism, and  $\psi(r) = 0$  if and only if  $p^{n-1}r \in p^n R$ , i.e.,  $p|r$  (using unique factorization). This proves b).

Next, it is clear that  $p^n M = 0$ . If  $m < n$  then  $p^m M = p^m R/p^n R$ . But  $\alpha : R \rightarrow p^m R/p^n R$  defined by  $\alpha(r) = p^m r + p^n R$  is a surjective homomorphism, with kernel  $p^{n-m} R$  by unique factorization. So  $p^m M \cong R/p^{n-m} R$  and c) follows from b). The proof of d) is left to the reader.  $\square$

Now suppose that

$$M \cong_{\phi} \left( \prod_i \left( \prod_j R/p_i^{n_{ij}} R \right) \right) \oplus \prod_{j=1}^m R R, \quad (1D)$$

where the  $p_i$  are pairwise non-associated primes, and the  $n_{ij}$  are positive integers. We must show that the isomorphism type of  $M$  determines the rank  $m$ , as well as the primes  $p_i$  (up to association and the order in which they occur) and the  $n_{ij}$  (up to order). This we do as follows. First,  $\phi(T(M))$  is the first direct sum, so  $M/T(M) \cong \prod_{j=1}^m R R$ . Therefore

$$m = \text{rank}(M/T(M)).$$

Second, for any fixed  $i$ , and any integer  $a$ , we can compute  $p_i^a T(M)[p_i]$ , using the above lemmas. By the second lemma it is isomorphic to the direct sum of  $p_i^a N[p_i]$  as  $N$  ranges over the direct summands in (1D). But the third lemma implies that these terms are trivial a) for  $p_k$  not associated to  $p_i$ ; and b) for those  $N = R/p_i^{n_{ij}}$  terms for which  $n_{ij} \leq a$ . Moreover for the terms  $N = R/p_i^{n_{ij}}$  terms for which  $n_{ij} > a$ . we get  $N[p_i] \cong R/p_i R$ . Therefore if we let  $c_{i,a}$  be the number of  $n_{ij}$  for which  $n_{ij} > a$ , we find that  $p_i^a T(M)[p_i]$  is isomorphic to the direct sum of  $c_{i,a}$  copies of  $R/p_i R$ . By the first lemma they are isomorphic as  $R/p_i R$ -modules. But  $R/p_i R$  is a field:

**Lemma.** *In a PID, if  $p$  is a prime, then  $Rp$  is maximal.*

(Proof: if  $Rp < Rx$ , then  $x$  is a proper divisor of  $p$  so is a unit.)

Therefore

$$c_{i,a} = \dim_{R/p_i R}(p_i^a T(M)[p_i]).$$

Furthermore, the right side does not change if we replace  $p_i$  by an associate, by the second lemma (d).

Hence  $c_{i,a}$ , the is determined by the isomorphism type of  $M$ . (If  $\phi : M \rightarrow N$  is an isomorphism, then  $\phi$  carries  $T(M)$  to  $T(N)$ , so induces an isomorphism between the vector spaces, whence they have the same dimension.

Finally, for any given  $i$  and  $n$ , the number of terms  $p_i^n$  appearing in (1D) is  $c(i, a-1) - c(i, a)$  so is also determined by the isomorphism type of  $M$ .