

MATH 101A: ALGEBRA I
PART C: TENSOR PRODUCT AND MULTILINEAR
ALGEBRA

This is the title page for the notes on tensor products and multilinear algebra.

CONTENTS

1. Bilinear forms and quadratic forms	1
1.1. definition of bilinear form	1
1.2. quadratic form	2
1.3. nondegenerate bilinear forms	3
1.4. nonsingular bilinear forms	3
2. Matrix of a bilinear form	6
2.1. matrix as homomorphism	6
2.2. dual bases	7
2.3. basis for homomorphisms	7
3. Naturality and contravariant functors	9
3.1. natural transformations	9
3.2. contravariant functors	10
3.3. unnaturalness of the dual	10
4. Tensor product	12
4.1. definition	12
4.2. exact functors and flat modules	14
4.3. list of properties	15
4.4. right exactness of tensor product	17
4.5. localization is exact	19
4.6. extension of scalars	20
5. Modules over a PID	22
5.1. rank	22
5.2. \mathfrak{p} -rank	22
5.3. p -primary modules	24

1. BILINEAR FORMS AND QUADRATIC FORMS

To save time, I am talking about bilinear forms and quadratic forms at the same time. We assume throughout that R is a commutative ring. (This will make $E \otimes_R F$ into an R -module for R -modules E, F .)

1.1. definition of bilinear form.

Definition 1.1. If E, F are R -modules, a *bilinear form* on $E \times F$ is an R -bilinear map

$$f : E \times F \rightarrow R.$$

I.e.,

- (1) $f(x, -) : F \rightarrow R$ is linear for each $x \in E$ and
- (2) $f(-, y) : E \rightarrow R$ is linear for each $y \in F$.

In the case $E = F$, f is called a *bilinear form on E* .

Example 1.2. $E = F = R^n$ and $f : E \times F \rightarrow R$ is given by

$$f(x, y) = \sum_{i=1}^n x_i y_i.$$

In this example you can see why R needs to be commutative:

$$f(x, ry) = \sum x_i r y_i = r \sum x_i y_i = r f(x, y)$$

holds because $x_i r = r x_i$. This is an example of a *symmetric* bilinear form on E where symmetric means

$$f(x, y) = f(y, x).$$

Example 1.3. $E = R^n = F$ and f is given by

$$f(x, y) = \sum_{i < j} x_i y_j - x_j y_i.$$

This is an example of an *alternating form* which means

$$f(x, y) = -f(y, x).$$

Note that “symmetric” and “alternating” only apply to the case $E = F$.

Example 1.4. Take $R = \mathbb{R}$ and $E = F = C^0(I)$, the ring of continuous functions $I = [0, 1] \rightarrow \mathbb{R}$ considered as an \mathbb{R} -module. Then f is given by

$$f(\phi, \psi) = \int_0^1 \phi(x) \psi(x) dx.$$

This is a symmetric bilinear form.

The notation

$$f(x, y) = \langle x, y \rangle$$

is sometimes used, especially in this last example.

Here is a general example where $E \neq F$.

Example 1.5. Let E be any R -module and let $F = \text{Hom}_R(E, R)$. Let

$$f : E \times \text{Hom}_R(E, R) \rightarrow R$$

be given by

$$f(x, g) = g(x).$$

This is R -linear in x by definition and it is R -linear in g because of the way the R -module structure of $\text{Hom}_R(E, R)$ is defined, namely by pointwise addition and scalar multiplication given by

$$rg(x) = g(rx)$$

This definition only works if R is commutative:

$$s(rg)(x) = rg(sx) = g(rsx) = (rs)g(x).$$

1.2. quadratic form. I gave two definitions of a quadratic form and showed that one implies the other.

Definition 1.6. (This definition requires $\frac{1}{2} \in R$.) A *quadratic form* on E is a function $f : E \rightarrow R$ so that

$$f(x) = \frac{1}{2}g(x, x)$$

for some symmetric bilinear form g on E .

The second definition works for any ring R .

Definition 1.7. A *quadratic form* on E is a function $f : E \rightarrow R$ so that

- (1) $f(rx) = r^2f(x)$ for every $r \in R, x \in E$.
- (2) The function $g(x, y) := f(x + y) - f(x) - f(y)$ is a symmetric bilinear form on E .

To see that the second definition implies the first, suppose that $x = y$. Then

$$g(x, x) = f(2x) - 2f(x) = 4f(x) - 2f(x) = 2f(x).$$

This implies that $f(x) = \frac{1}{2}g(x, x)$ if $\frac{1}{2} \in R$. Conversely, $f(x) := \frac{1}{2}g(x, x)$ is easily seen to satisfy the second definition.

1.3. nondegenerate bilinear forms.

Definition 1.8. Given a bilinear form $f : E \times F \rightarrow R$ and $S \subseteq E$, I defined

$$S^\perp := \{y \in F \mid f(x, y) = 0 \forall x \in S\}$$

Similarly, if $T \subseteq F$ then

$${}^\perp T := \{x \in E \mid f(x, y) = 0 \forall y \in T\}$$

Proposition 1.9. Suppose $E = F$ and $f : E \times E \rightarrow R$ is symmetric or alternating. Then

$$S^\perp = {}^\perp S$$

for any $S \subseteq E$.

It is easy to see that S^\perp is always a submodule of F and ${}^\perp T$ is always a submodule of E . However, in class I only pointed this out in the case of ${}^\perp F \subseteq E$ and $E^\perp \subseteq F$. These are important because they are the kernels of the maps

$$\phi_f : E \rightarrow \text{Hom}_R(F, R)$$

and

$$\psi_f : F \rightarrow \text{Hom}_R(E, R).$$

Definition 1.10. We say that $f : E \times F$ is *nondegenerate on the left* if $F^\perp = 0$, i.e., ϕ_f is a monomorphism. We can that f is *nondegenerate on the right* if $E^\perp = 0$, i.e., ψ_f is a monomorphism.

Lang uses the notation $E_0 = {}^\perp F$ and $F_0 = E^\perp$.

Proposition 1.11. Every bilinear form $f : E \times F \rightarrow R$ induces a nondegenerate (on both sides) bilinear form

$$\bar{f} : E/E_0 \times F/F_0 \rightarrow R$$

by the equation

$$\bar{f}(x + E_0, y + F_0) = f(x, y).$$

1.4. nonsingular bilinear forms.

Definition 1.12. A bilinear form $f : E \times F \rightarrow R$ is *nonsingular on the left* if

$$\phi_f : E \xrightarrow{\cong} \text{Hom}_R(F, R)$$

is an isomorphism. It is *nonsingular on the right* if

$$\psi_f : F \xrightarrow{\cong} \text{Hom}_R(E, R)$$

is an isomorphism. f is called *nonsingular* if it is nonsingular on both sides.

We discussed why nonsingularity on the left and right were different. It is because a module is not always equal to its “double dual.”

Definition 1.13. The *dual* E^* of any R module E is defined by

$$E^* = \text{Hom}_R(E, R).$$

If $f : E \times F \rightarrow R$ is nonsingular on the left then $\phi_f : E \cong F^*$. Nonsingularity on the right would mean that

$$\psi_f : F \cong \text{Hom}_R(F^*, R) = F^{**}$$

But there are well-known examples where this is not true. There are also easy examples: If F is a torsion module over a PID R then $F^* = 0$.

The well-known example is V a countably infinite dimensional vector space over \mathbb{Q} . Then V^* is uncountable dimensional and V^{**} is even bigger dimensional.

There is a related isomorphism:

Proposition 1.14. *The mapping which sends a bilinear form f to $\phi_f : E \rightarrow F^*$ and to $\psi_f : F \rightarrow E^*$ gives isomorphisms of R -modules:*

$$\begin{aligned} L^2(E \times F, R) &\cong \text{Hom}_R(E, \text{Hom}_R(F, R)) \\ &\cong \text{Hom}_R(F, \text{Hom}_R(E, R)) \end{aligned}$$

Proof. The inverse of the first mapping is given by sending $\phi : E \rightarrow F^*$ to

$$f(x, y) = \phi(x)(y).$$

□

This proposition is about all possible f . For a fixed nonsingular f , we get a different formula:

Theorem 1.15. *If $f : E \times F \rightarrow R$ is nonsingular then we get an induced isomorphism of R -modules*

$$\text{End}_R(E) \cong L^2(E \times F, R)$$

where $A \in \text{End}_R(E)$ is mapped to the function fA given by

$$fA(x, y) = f(Ax, y).$$

Remark 1.16. On the second day, I pointed out that this theorem requires only that $f : E \times F \rightarrow R$ be nonsingular on the left.

Proof. We know that

$$L^2(E \times F, R) \cong \text{Hom}_R(E, F^*)$$

and that a bilinear form g maps to the homomorphism $\phi_g : E \rightarrow F^*$ given by

$$\phi_g(x) = g(x, -).$$

The definition of nonsingular on the left means that $\phi_f : E \rightarrow F^*$ is an isomorphism. But, $F^* \cong E$ implies that

$$\text{Hom}_R(E, F^*) \cong \text{Hom}_R(E, E) = \text{End}_R(E).$$

We conclude that

$$L^2(E \times F, R) \cong \text{Hom}_R(E, F^*) \cong \text{Hom}_R(E, E) = \text{End}_R(E).$$

The only question is: What is the formula for this isomorphism?

The isomorphism is given by composition with the inverse $\phi_f^{-1} : F^* \rightarrow E$. So, g corresponds to $A = \phi_f^{-1} \circ \phi_g$ which, when applied to $x \in E$ gives

$$Ax = \phi_f^{-1}(\phi_g(x)).$$

Applying ϕ_f to both sides we got:

$$f(Ax, -) = \phi_g(x) = g(x, -)$$

which is the formula in the theorem. \square

The significance of this theorem is that it shows the need for a second bilinear form, namely f , in order to express g in matrix form.

2. MATRIX OF A BILINEAR FORM

Suppose that $E = R^n$ and $F = R^m$ are free R -modules with bases $\{a_1, \dots, a_n\}$ and $\{b_1, \dots, b_m\}$. If $f : E \times F \rightarrow R$ is any bilinear form, we get a bunch of scalars:

$$f(a_i, b_j) = g_{ij} \in R.$$

These scalars determine the bilinear form f uniquely since arbitrary elements $x \in E, y \in F$ are given by

$$x = \sum x_i a_i, \quad y = \sum y_j b_j.$$

Then

$$f(x, y) = f\left(\sum x_i a_i, \sum y_j b_j\right) = \sum_i \sum_j x_i y_j f(a_i, b_j) = \sum_i \sum_j x_i y_j g_{ij}$$

This can be written in matrix form as

$$f(X, Y) = {}^t X G Y$$

where X, Y are column vectors with coordinates x_i, y_j , ${}^t X$ is the transpose and $G = (g_{ij})$ is the $n \times m$ matrix with ij -entry equal to g_{ij} .

2.1. matrix as homomorphism. At this point I tried to explain that there are hidden nonsingular forms in the matrix equation. This is because the product of a row matrix and a column matrix is the their dot product:

$$f(X, Y) = \langle X, GY \rangle_E$$

where

$$\langle X, Z \rangle_E = \sum x_i z_i$$

is the dot product in E . This is a nonsingular symmetric bilinear form. The bilinear form can also be written in terms of the dot product in F :

$$f(X, Y) = \langle {}^t G X, Y \rangle_F$$

The point is that, given a fixed nonsingular form on E or F we can express bilinear forms as homomorphisms:

Proposition 2.1. *If E, F are free and finitely generated over R then a bilinear form f on $E \times F$ is given by*

$$f(X, Y) = \langle X, GY \rangle_E$$

where $G = (g_{ij}) \in \text{Hom}_R(F, E)$ is uniquely determined by f .

This is just a rewording of what I explained earlier (that the matrix determines f). I just needed to explain how matrices give homomorphisms. This is just standard linear algebra but over arbitrary commutative rings.

2.2. dual bases. First, we need the dual basis on F . If b_1, \dots, b_m is the basis for F then we have the dual basis $b_1^*, \dots, b_m^* \in F^*$ given by

$$b_j(x) = b_j^* \left(\sum x_i b_i \right) = x_j$$

I.e., b_j^* picks out the j th coordinate of x .

Theorem 2.2. *The b_i^* form a basis for $F^* \cong R^m$.*

Proof. First, the b_i generate F^* . To show this let $f : F \rightarrow R$ be any homomorphism. Then f is determined by the numbers $f(b_i) = c_i \in R$ and $f = \sum c_i b_i^*$ by the following:

$$f(x) = f \left(\sum x_i b_i \right) = \sum x_i f(b_i) = \sum x_i c_i = \sum c_i b_i^*(x).$$

This shows that $f = \sum c_i b_i^*$. Therefore, these dual elements b_i^* generate F^* and give an epimorphism

$$\phi : R^m \twoheadrightarrow F^*.$$

Next we have to show that ϕ is 1-1, i.e., its kernel is zero. So, suppose that

$$\phi(x_1, \dots, x_m) = \sum x_i b_i^* = 0 \in F^*.$$

If we apply this element of F^* to the basis element b_j we get

$$\sum x_i b_i^*(b_j) = \sum x_i \delta_{ij} = x_j = 0.$$

Since this is true for all j , $x = (x_1, \dots, x_m) = (0, \dots, 0)$. So, ϕ is an isomorphism and the b_i^* form a basis for F^* . \square

2.3. basis for homomorphisms.

Corollary 2.3. *If $E \cong R^n$ and $F \cong R^m$ are free with bases $\{a_i\}, \{b_j\}$ then $\text{Hom}_R(F, E) \cong R^{nm}$ is free with basis the functions $a_i b_j^*$ given by*

$$a_i b_j^*(y) = y_j a_i$$

if $y = \sum y_j b_j$.

This corollary says that a homomorphism is given by a linear combination

$$g = \sum_{i,j} g_{ij} a_i b_j^*$$

and the action of g is given by

$$g(x) = g \left(\sum x_j b_j \right) = \sum_{i,j} x_j g_{ij} a_i = (a_1, \dots, a_n) G X$$

(matrix multiplication) where $G = (g_{ij})$ and $X = (x_j)$.

I gave a (much longer than necessary) categorical proof of this corollary using the following lemma.

Lemma 2.4.

$$\mathrm{Hom}_R(M, A \oplus B) \cong \mathrm{Hom}_R(M, A) \oplus \mathrm{Hom}_R(M, B)$$

Proof. This follows from the universal property of the product

$$A \times B = A \oplus B$$

namely, a homomorphism into the product $f : M \rightarrow A \oplus B$ is given uniquely by the projections $p_1 f : M \rightarrow A$ and $p_2 f : M \rightarrow B$. So, the isomorphism in the lemma is given by

$$f \mapsto (p_1 f, p_2 f)$$

and the inverse is given by

$$(f, g) \mapsto s_1 f + s_2 g$$

where $s_1 : A \rightarrow A \oplus B$ and $s_2 : B \rightarrow A \oplus B$ are the inclusion maps. \square

Proof of Corollary. Since $E \cong R^n$ we have by the lemma that

$$\mathrm{Hom}_R(F, E) \cong \mathrm{Hom}_R(F, \bigoplus_n R) \cong \bigoplus_n \mathrm{Hom}_R(F, R) = (F^*)^n.$$

Since the i th inclusion map $s_i : R \rightarrow E \cong R^n$ is given by

$$s_i(r) = r a_i$$

the basis elements of $\mathrm{Hom}_R(F, E)$ are

$$s_i b_j^* = a_i b_j^*.$$

\square

3. NATURALITY AND CONTRAVARIANT FUNCTORS

Somehow, I got into a long explanation about contravariant functors and naturality.

3.1. natural transformations. The concept of “naturality” is made precise with the definition of a natural transformation. One example I used was the commutator subgroup $G' = [G, G]$ of a group G vs. its center $Z(G)$. I claimed that G' was natural but $Z(G)$ was not natural. This comes from the fact that any homomorphism $G \rightarrow H$ sends G' into H' but does not necessarily send $Z(G)$ to $Z(H)$.

Definition 3.1. Suppose that $F, G : \mathcal{A} \rightarrow \mathcal{B}$ are functors between categories \mathcal{A}, \mathcal{B} . Then a *natural transformation* $\eta : F \rightarrow G$ is defined to be an operation which assigns to each object $A \in \mathcal{A}$ a morphism in \mathcal{B} of the form $\eta_A : FA \rightarrow GA$ so that, for all morphisms $f : A \rightarrow B$ in \mathcal{A} , we have the following commuting square of morphisms in \mathcal{B} .

$$\begin{array}{ccc} FA & \xrightarrow{Ff} & FB \\ \eta_A \downarrow & & \downarrow \eta_B \\ GA & \xrightarrow{Gf} & GB \end{array}$$

For example, if $\mathcal{A} = \mathcal{B} = \mathcal{Gps}$, the inclusion map is a natural transformation from G' to G . This is a natural transformation from the commutator subgroup functor to the identity functor.

Another example is the torsion submodule tM of a module M over a PID R . The following commuting diagram shows that tM is a natural submodule of M and M/tM is a natural quotient module.

$$\begin{array}{ccccc} tN & \longrightarrow & N & \longrightarrow & N/tN \\ \downarrow & & \downarrow & & \downarrow \\ tM & \longrightarrow & M & \longrightarrow & M/tM \end{array}$$

The two squares in this diagram mean we have two natural transformations

$$t \rightarrow id \rightarrow id/t$$

“Natural” is not the same as “functorial.” It means more. In order to have naturality, we need two functors and a natural transformation.

The dual E^* of E is thus functorial but not natural. But it is contravariantly functorial.

3.2. contravariant functors.

Definition 3.2. If \mathcal{A} and \mathcal{B} are categories, a *contravariant functor*

$$F : \mathcal{A} \rightarrow \mathcal{B}$$

is a pair of mappings

- (1) a mapping $F : Ob(\mathcal{A}) \rightarrow Ob(\mathcal{B})$, i.e., for each $A \in \mathcal{A}$ we have $FA \in \mathcal{B}$.
- (2) for every morphism $f : A \rightarrow B$ in \mathcal{A} we get a morphism

$$Ff = f^* : FB \rightarrow FA$$

satisfying the two conditions:

- (a) $Fid_A = (id_A)^* = id_{FA}$
- (b) $(f \circ g)^* = g^* \circ f^*$.

Example 3.3. Suppose that X is any fixed R -module. Then we have a contravariant functor

$$\text{Hom}_R(-, X) : R\text{-Mod} \rightarrow \mathbb{Z}\text{-Mod}$$

sending M to $\text{Hom}_R(M, X)$.

Example 3.4. If X is a topological space, let $C^0(X)$ be the ring of all continuous functions $X \rightarrow \mathbb{R}$. This is a contravariant functor

$$C^0 : Top \rightarrow Rings$$

from the category of topological spaces and continuous maps to the category of rings and ring homomorphisms.

Duality $E \mapsto E^* = \text{Hom}_R(E, R)$ is a contravariant functor.

So, E^* is functorial and its elements behave in a functorial way. However, the dual basis is not natural.

3.3. unnaturality of the dual.

Theorem 3.5. *There is no natural isomorphism $E \cong E^*$ in the category of finitely generated free R -modules and isomorphism.*

First, what does this theorem say? We take the category \mathcal{C} whose objects are f.g. free R -modules and whose morphisms are isomorphisms. By a natural isomorphism $\phi_E : E \rightarrow E^*$ we mean an isomorphism which makes the following diagram commute for any isomorphism $f : E \cong F$ of f.g. free R modules:

$$\begin{array}{ccc} E & \xrightarrow{f} & F \\ \phi_E \downarrow & & \downarrow \phi_F \\ E^* & \xleftarrow{f^*} & F^* \end{array}$$

Proof. I proved this by contradiction. But the proof assumes the $1+1 \neq 0$, i.e., the characteristic of the ring is not 2. Suppose there is such a natural isomorphism. Let $E = F \cong R^2$ be free on two generators v, w . Then E^* is free on the dual basis elements v^*, w^* . Let $f : E \rightarrow E$ be the isomorphism given by $f(v) = v$ and $f(w) = v \pm w$ (doing two cases at once). Then $f^*(w^*) = \pm w^*$ since

$$f^*w^*(xv + yw) = w^*f(xv + yw) = w^*(xv + yv \pm yw) = \pm y$$

and $f^*(v^*) = v^* + w^*$ since

$$f^*v^*(xv + yw) = v^*f(xv + yw) = v^*(xv + yv \pm yw) = x + y.$$

Now suppose that there is some isomorphism $\phi : E \rightarrow E^*$ which makes the diagram commute. Then $\phi = f^*\phi f$. Suppose that $\phi(v) = xv^* + yw^*$. Then

$$\phi(v) = f^*\phi f(v) = f^*\phi(v) = f^*(xv^* + yw^*) = xv^* + xw^* \pm yw^*.$$

In order for this to be equal to $f(v) = xv^* + yw^*$ we must have

$$y = x + y = x - y$$

since the same isomorphism ϕ must work for both functions f . This implies that $x = 0$ and $2y = 0$. But, for ϕ to be an isomorphism, we must have y invertible in the ring. So, $2 = 0$. \square

When you looked at this counterexample, you can see one of the reasons that the dual basis is not natural: When we changed the second basis element from w to $v + w$, it was the dual basis element v^* which changed. This dual element v^* depends not on v but on your choice of the other basis element w (or, in higher dimensions, v_i^* depends on all v_j where $j \neq i$). The reason is that the other basis elements must span the kernel of v_i^* by definition. So, they are the ones that determine what v_i^* are up to a scalar multiple.

4. TENSOR PRODUCT

Here is an outline of what I did:

- (1) categorical definition
- (2) construction
- (3) list of basic properties
- (4) distributive property
- (5) right exactness
- (6) localization is flat
- (7) extension of scalars
- (8) applications

4.1. **definition.** First I gave the categorical definition and then I gave an explicit construction.

4.1.1. *universal condition.* Tensor product is usually defined by the following universal condition.

Definition 4.1. If E, F are two modules over a commutative ring R , their *tensor product* $E \otimes F$ is defined to be the R -module having the following universal property. First, there exists an R -bilinear mapping

$$f : E \times F \rightarrow E \otimes F.$$

Second, this mapping is universal in the sense that, for any other R -module M and bilinear mapping $g : E \times F \rightarrow M$, there exists a unique R -module homomorphism $h : E \otimes F \rightarrow M$ making the following diagram commute.

$$\begin{array}{ccc} E \times F & \xrightarrow{f} & E \otimes F \\ & \searrow g & \swarrow \exists! h \\ & & M \end{array}$$

As with all universal conditions, this definition only gives the uniqueness of $E \otimes F$ up to isomorphism. For the existence we need a construction.

4.1.2. *construction of $E \otimes F$.* The mapping $f : E \times F \rightarrow E \otimes F$ is not onto. However, the image must generate $E \otimes F$ otherwise we get a contradiction. The elements in the image of f are denoted

$$f(x, y) = x \otimes y.$$

Definition 4.2. The tensor product $E \otimes F$ is defined to be the R module which is generated by the symbols $x \otimes y$ for all $x \in E, y \in F$ modulo the following conditions

- (1) $x \otimes -$ is R -bilinear. I.e.
- (a) $x \otimes ry = r(x \otimes y)$ for all $r \in R$
 - (b) $x \otimes (y + z) = (x \otimes y) + (x \otimes z)$
- (2) $- \otimes y$ is R -bilinear. I.e.,
- (a) $rx \otimes y = r(x \otimes y)$ for all $r \in R$
 - (b) $(x + y) \otimes z = (x \otimes z) + (y \otimes z)$

I pointed out that these conditions require R to be commutative since

$$rs(x \otimes y) = r(sx \otimes y) = sx \otimes ry = s(x \otimes ry) = sr(x \otimes y).$$

Proposition 4.3. $E \otimes F$ as given in the second definition satisfies the universal condition of the first definitions and therefore, the tensor product exists and is unique up to isomorphism.

Proof. I said in class that this is obvious. If there is a bilinear mapping $g : E \times F \rightarrow M$, the induced mapping $h : E \otimes F \rightarrow M$ must take the generators $x \otimes y$ to $g(x, y)$. Otherwise the diagram will not commute. Therefore, h is given on the generators and is thus unique. The only thing we need is to show that h is a homomorphism. But this is equivalent to showing that the elements of the form

$$rx \otimes y - r(x \otimes y)$$

and elements corresponding to the other three conditions in the second definition go to zero in M . But this element goes to

$$g(rx, y) - rg(x, y) = 0$$

since g is R -bilinear and similarly for the other three elements. So, h is an R -module homomorphism and we are done. \square

4.1.3. *functorial properties of tensor product.* The first properties I mentioned were the categorical properties which follow directly from the definition.

Proposition 4.4. For a fixed R -module M , tensor product with M is a functor

$$M \otimes - : R\text{-Mod} \rightarrow R\text{-Mod}.$$

What this means is that, given an homomorphism $f : A \rightarrow B$ there is an R -module homomorphism

$$1 \otimes f : M \otimes A \rightarrow M \otimes B$$

which satisfies two conditions:

- (1) $1 \otimes id_A = id_{M \otimes A}$

$$(2) 1 \otimes fg = (1 \otimes f)(1 \otimes g).$$

The definition is $(1 \otimes f)(x \otimes y) = x \otimes f(y)$. This gives a homomorphism since the mapping $M \times A \rightarrow M \otimes B$ given by

$$(x, y) \mapsto x \otimes f(y)$$

is bilinear and therefore induces the desired mapping $1 \otimes f$.

More generally, given two homomorphisms $f : M \rightarrow N, g : A \rightarrow B$ we get a homomorphism

$$f \otimes g : M \otimes A \rightarrow N \otimes B$$

by the formula

$$(f \otimes g)(x \otimes y) = f(x) \otimes g(y).$$

4.2. exact functors and flat modules. Flat modules are those for which the functor $M \otimes -$ is exact. An exact functor is one that takes short exact sequences to short exact sequences. So, first I explained the definitions.

Definition 4.5. An *exact sequence* is a sequence of modules and homomorphisms so that the image of each map is equal to the kernel of the next map. A *short exact sequence* is an exact sequence of the following form:

$$0 \rightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \rightarrow 0.$$

In other words, $\alpha : A \rightarrow B$ is a monomorphism, $\beta : B \rightarrow C$ is an epimorphism and $\text{im } \alpha = \ker \beta$ or: $C \cong B/\alpha A$.

Sometimes short exact sequences are written:

$$A \twoheadrightarrow B \twoheadrightarrow C.$$

Definition 4.6. A functor $F : R\text{-Mod} \rightarrow R\text{-Mod}$ is called *exact* if it takes short exact sequences to short exact sequences. Thus the short exact sequence above should give the short exact sequence

$$0 \rightarrow FA \xrightarrow{F\alpha} FB \xrightarrow{F\beta} FC \rightarrow 0.$$

Definition 4.7. An R -module M is called *flat* if $M \otimes -$ is an exact functor. I.e.,

$$0 \rightarrow M \otimes A \xrightarrow{1 \otimes \alpha} M \otimes B \xrightarrow{1 \otimes \beta} M \otimes C \rightarrow 0$$

is exact for all short exact sequences $A \twoheadrightarrow B \twoheadrightarrow C$.

One of the main results (which we will see is actually trivial) is that $S^{-1}R$ is flat for any multiplicative set S . I.e., localization is exact.

4.3. list of properties. I explained that the exactness of localization was one of the key ideas. However, the explanation required an understanding of the basic properties of tensor product. So, I went back to the beginning with this list.

- (0) (unity) $R \otimes M \cong M$.
- (1) (commutative) $M \otimes N \cong N \otimes M$
- (2) (distributive) $N \otimes \bigoplus M_i \cong \bigoplus (N \otimes M_i)$
- (3) (associative) $(A \otimes B) \otimes C \cong A \otimes (B \otimes C)$
- (4) (right exactness) $M \otimes -$ is right exact, i.e., a short exact sequence $A \rightarrow B \rightarrow C$ gives an exact sequence

$$M \otimes A \xrightarrow{1 \otimes \alpha} M \otimes B \xrightarrow{1 \otimes \beta} M \otimes C \rightarrow 0$$

- (5) (localization is exact) I.e., we get an exact sequence:

$$0 \rightarrow S^{-1}A \rightarrow S^{-1}B \rightarrow S^{-1}C \rightarrow 0.$$

- (6) (extension of scalars) Given a ring homomorphism $R \rightarrow S$, every R -module M gives an S module $S \otimes_R M$.

4.3.1. *Grothendieck ring.* I did not prove properties (1) and (3). I said they were obvious. However, I put the first three conditions into a conceptual framework by pointing out that these are the axioms of a ring. The only thing that we don't have is an additive inverse. The algebraic construction is as follows.

First, you take the set of all isomorphism classes of finitely generated R -modules $[M]$. This set has addition and multiplication given by

$$[M] + [N] = [M \oplus N]$$

$$[M][N] = [M \otimes N]$$

Addition and multiplication are associative and commutative and have units: $[0]$ is the additive unit and $[R]$ is the multiplicative unit. It just doesn't have additive inverses. So, Grothendieck said to just put in formal inverses:

$$[M] - [N]$$

which are defined like fractions:

$$[M] - [N] = [A] - [B]$$

if there exists another module C so that

$$M \oplus B \oplus C \cong N \oplus A \oplus C.$$

This gives a ring whose name is $G(R)$. The notation $K_0(R)$ is for the ring of formal differences of f.g. projective R -modules.

4.3.2. $R \otimes M \cong M$. After using this formula many times in the lecture, I decided I should prove it. I put the proof at the beginning in the notes where it belongs.

Theorem 4.8. $R \otimes M \cong M$ for any R -module M .

Proof. Since the mapping

$$R \times M \rightarrow M$$

given by $(r, x) \mapsto rx$ is bilinear it induces a mapping

$$\mu : R \otimes M \rightarrow M$$

so that $\mu(r \otimes x) = rx$. The inverse mapping $\phi : M \rightarrow R \otimes M$ is given by $\phi(x) = 1 \otimes x$. We carefully checked that these are inverse to each other:

$$\phi\mu(r \otimes x) = \phi(rx) = 1 \otimes rx = r(1 \otimes x) = r \otimes x$$

$$\mu\phi(x) = \mu(1 \otimes x) = 1x = x.$$

So, these maps are both isomorphisms of R -modules. \square

4.3.3. *distributive property.* I gave a category theory proof of the distributivity of tensor product over direct sum. First I pointed out that the following formal characterization of direct sum.

Lemma 4.9. M is the direct sum of modules M_1, \dots, M_n if and only if there are inclusion maps $s_i : M_i \rightarrow M$ and projection maps $p_i : M \rightarrow M_i$ so that

- (1) $p_j \circ s_i = \delta_{ij}$, i.e., equal to the identity mapping on M_i if $i = j$ and equal to 0 if $i \neq j$.
- (2) $\sum s_i \circ p_i = id_M$.

I drew the following diagrams to illustrate these equations.

$$\begin{array}{ccc}
 M_i & \xrightarrow{\delta_{ij}} & M_j \\
 & \searrow s_i & \nearrow p_j \\
 & & M
 \end{array}
 \quad p_j \circ s_i = \delta_{ij}$$

$$\begin{array}{ccc}
 M & \xrightarrow{\quad} & M \\
 & \searrow p_i & \nearrow s_i \\
 & & M
 \end{array}
 \quad \sum_{i=1}^n s_i \circ p_i = id_M$$

This lemma was proved in any preadditive category in Part B, Theorem 7.4.

Theorem 4.10. *If $M \cong \bigoplus_{i=1}^n M_i$ then*

$$N \otimes M = N \otimes \bigoplus_{i=1}^n M_i \cong \bigoplus_{i=1}^n (N \otimes M_i).$$

Proof. Consider the homomorphisms:

$$N \otimes M_i \xrightarrow{1 \otimes s_i} N \otimes M \xrightarrow{1 \otimes p_j} N \otimes M_j$$

- a) $(1 \otimes p_j)(1 \otimes s_i) = 1 \otimes p_j s_i = 1 \otimes \delta_{ij} = \delta_{ij}(1 \otimes 1)$.
 b) $\sum (1 \otimes s_i)(1 \otimes p_i) = 1 \otimes \sum s_i p_i = 1 \otimes 1 = id_{N \otimes M}$.

These conditions imply that $N \otimes M \cong \bigoplus N \otimes M_i$ by the above lemma. \square

Remark 4.11. This proof works in any preadditive category to show that any linear functor distributes over direct sum.

4.4. right exactness of tensor product. I didn't prove the right exactness of tensor product this first time because the elementary proof is messy and not very instructive. I just explained that this is a special case of a much more general principle that: "All linear left adjoint functors are right exact." I will explain this later. The statement of the theorem is the following.

Theorem 4.12. *Tensor product with any R -module M sends any exact sequence of R -modules of the form:*

$$A \xrightarrow{\alpha} B \xrightarrow{\beta} C \rightarrow 0$$

to another exact sequence of the same form:

$$M \otimes A \rightarrow M \otimes B \rightarrow M \otimes C \rightarrow 0.$$

This statement appears stronger than the original statement since the hypothesis is weaker. But I explained that the first statement implies this second version. Suppose that we know that $M \otimes -$ sends short exact sequences to right exact sequences as above. Then how can we conclude that it sends the more general right exact sequences $A \rightarrow B \rightarrow C \rightarrow 0$ to right exact sequences?

The first statement implies that $M \otimes -$ takes epimorphisms to epimorphisms. (In fact this is obvious since the generators $x \otimes y \in M \otimes C$ come from generators $x \otimes \tilde{y} \in M \otimes B$.) Therefore $M \otimes A$ maps onto $M \otimes \alpha(A)$. If we assume the weaker condition that the functor $M \otimes -$

takes short exact sequences to right exact sequences, then it will take the short exact sequence

$$0 \rightarrow \alpha(A) \hookrightarrow B \xrightarrow{\beta} C \rightarrow 0$$

to an exact sequence

$$M \otimes \alpha(A) \rightarrow M \otimes B \xrightarrow{1 \otimes \beta} M \otimes C \rightarrow 0$$

This says that $M \otimes \alpha(A)$ maps onto the kernel of $1 \otimes \beta$. But $M \otimes A$ maps onto $M \otimes \alpha(A)$. So, $M \otimes A$ also maps onto $\ker(1 \otimes \beta)$. So, we get an exact sequence

$$M \otimes A \xrightarrow{1 \otimes \alpha} M \otimes B \xrightarrow{1 \otimes \beta} M \otimes C \rightarrow 0.$$

Here is an example of how this is used.

Corollary 4.13. *Suppose that $I \subset R$ is an ideal. Then*

$$R/I \otimes M \cong M/IM$$

where IM is the submodule of M generated by all products of the form ax where $a \in I$ and $x \in M$. In particular, when $I = (p)$ is principal, we have

$$R/(p) \otimes M \cong M/pM$$

where $pM = \{px \mid x \in M\}$.

Proof. Suppose that I is generated by elements a_i . Then we have an epimorphism of R modules

$$\bigoplus_i R \twoheadrightarrow I$$

sending $(r_i) \in \bigoplus_i R$ to $\sum r_i a_i \in I$. This gives an exact sequence

$$\bigoplus_i R \xrightarrow{\alpha} R \rightarrow R/I \rightarrow 0.$$

Tensor with M to give

$$\bigoplus_i R \otimes M \xrightarrow{\alpha \otimes 1} R \otimes M \rightarrow R/I \otimes M \rightarrow 0.$$

Using the isomorphisms $\mu : R \otimes M \cong M$ and $\phi : M \cong R \otimes M$ we get an exact sequence

$$\bigoplus_i M \xrightarrow{\mu(\alpha \otimes 1)\phi} M \rightarrow R/I \otimes M \rightarrow 0$$

where $\mu(\alpha \otimes 1)\phi$ sends $(x_i) \in \bigoplus_i M$ to $\sum a_i x_i \in M$. The image is equal to IM by definition. So, $R/I \otimes M \cong M/IM$ as claimed. \square

For finitely generated modules over a PID we can now compute the tensor product:

$$M \otimes \left(R^n \oplus \bigoplus R/(p_i^{n_i}) \right) \cong M^n \oplus \bigoplus M/p_i^{n_i} M.$$

4.5. localization is exact. Recall that a *multiplicative set* is a subset $S \subseteq R$ which is closed under multiplication, contains 1 and does not contain 0. The *localization* $S^{-1}R$ was defined to be the ring of all fractions r/s where $r \in R$ and $s \in S$ modulo the equivalence relation

$$\frac{r}{s} \sim \frac{r'}{s'}$$

if there is an element $t \in S$ so that $rs't = r'st$. This ring is also an R -module since we have an action of R given by

$$r \cdot \frac{x}{s} = \frac{rx}{s}.$$

Proposition 4.14. *For any R -module M let $S^{-1}M$ be the set of equivalence classes of fractions x/s where $x \in M, s \in S$ modulo the equivalence relation $x/s \sim y/s'$ if there is a $t \in S$ so that $ts'x = tsy$. Then $S^{-1}M$ is an R -module with action of R given by $r(x/s) = rx/s$ and*

$$S^{-1}M \cong S^{-1}R \otimes M.$$

Proof. There is an obvious map $S^{-1}R \otimes M \rightarrow S^{-1}M$ sending $r/s \otimes x$ to rx/s . The inverse map sends x/s to $1/s \otimes x$. To show that this is well-defined, take an equivalent element tx/ts . This goes to

$$\frac{1}{ts} \otimes tx = t \left(\frac{1}{ts} \otimes x \right) = \frac{t}{ts} \otimes x = \frac{1}{s} \otimes x.$$

The rest of the proof is straightforward. □

Theorem 4.15. *$S^{-1}R$ is a flat R -module. Equivalently, every short exact sequence of R -modules $A \rightarrow B \rightarrow C$ induces an exact sequence*

$$0 \rightarrow S^{-1}A \rightarrow S^{-1}B \rightarrow S^{-1}C \rightarrow 0.$$

Proof. Since tensor product is right exact, it suffices to show that $S^{-1}A \rightarrow S^{-1}B$ is a monomorphism. This is easy. We can assume that $A \subseteq B$ and suppose that $a \in A$ and $s \in S$ so that the element $a/s \in S^{-1}A$ goes to zero in $S^{-1}B$. This means

$$\frac{a}{s} \sim \frac{0}{s}$$

in $S^{-1}B$. By definition this is equivalent to saying that there exists $t \in S$ so that $tsa = 0$. But this same equation implies that $a/s = 0/1$ in $S^{-1}A$. So, we are done. \square

The ring $S^{-1}R$ acts on the module $S^{-1}M$ in the obvious way:

$$\frac{r}{s} \frac{x}{t} = \frac{rx}{st}.$$

This makes $S^{-1}M$ into a module over $S^{-1}R$. This is an example of “extension of scalars.”

4.6. extension of scalars. We had a concept before called “restriction of scalars.” That was when we had a subring S of R or, more generally, a ring homomorphism $\phi : S \rightarrow R$ and we got an induced map

$$\phi^* : R\text{-Mod} \rightarrow S\text{-Mod}$$

which sent an R -module M to the same thing with the action of S given by $s \cdot x = \phi(s)x$. I.e., we restricted the action of the ring to S .

“Extension of scalars” goes the other way.

Proposition 4.16. *Given a ring homomorphism $\phi : R \rightarrow S$ and an R -module M , $S \otimes_R M$ is an S -module with action of S given by*

$$s(t \otimes x) = st \otimes x.$$

The module is sometimes written as $S \otimes_\phi M$ because the R -module structure is given by

$$r(s \otimes x) = (\phi(r)s) \otimes x = s \otimes rx.$$

This is the R -module structure induced from the S -module structure by restriction of scalars.

Proof. Multiplication by elements of S gives an R -linear map $S \rightarrow S$ and therefore gives an R -linear map $S \otimes M \rightarrow S \otimes M$ by naturality of tensor product. This gives a sequence of ring homomorphisms

$$S \rightarrow \text{End}_R(S) \rightarrow \text{End}_R(S \otimes M)$$

which defines the S -module structure on $S \otimes M$. \square

One special case of this is when R is a domain and $F = Q(R)$ is the field of fractions.

Definition 4.17. Suppose that M is a module over a domain R . Then the *rank* of M is defined to be the dimension of $Q(R) \otimes M$ as a vector space over the field $Q(R)$.

$$r(M) = \dim_{Q(R)} Q(R) \otimes M.$$

Theorem 4.18. *For a f.g. module M over a PID R , if*

$$M \cong R^r \oplus \bigoplus R/(p_i^{n_i}),$$

the number r is equal to the rank of M and is therefore uniquely determined.

Proof. This is a calculation using the fact that

$$R/(a) \otimes Q(R) \cong Q(R)/aQ(R) = 0$$

since $aQ(R) = Q(R)$ for $a \neq 0$:

$$Q(R) \otimes M = Q(R) \otimes R^r \oplus \bigoplus Q(R)/p_i^{n_i}Q(R) \cong Q(R)^r.$$

□

It still remains to show that the numbers $p_i^{n_i}$ are uniquely determined.

5. MODULES OVER A PID

I spent one more day to finish the uniqueness part of the structure theorem for f.g. modules over a PID. First I reviewed properties of the rank.

5.1. **rank.** Recall that if R is any domain, $Q(R)$ is a field. So, for any R -module M , we can define the *rank* of M to be

$$rM = \dim_{Q(R)} M \otimes Q(R).$$

We know that $Q(R) = S^{-1}R$ is a flat R -module. Therefore, any short exact sequence of R -modules

$$0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$$

gives a short exact sequence of vector spaces

$$0 \rightarrow Q(R) \otimes A \rightarrow Q(R) \otimes B \rightarrow Q(R) \otimes C \rightarrow 0.$$

Lemma 5.1. *If $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ is a short exact sequence of vector spaces over a field F then*

- (1) $B \cong A \oplus C$
- (2) $\dim B = \dim A + \dim C$.

Proof. This follows from the fact that all modules over fields are free and thus projective. \square

Theorem 5.2. *If $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ is a short exact sequence of f.g. R -modules where R is any domain, then*

$$r(B) = r(A) + r(C).$$

5.2. **p-rank.** Suppose that $\mathfrak{p} \subseteq R$ is a prime ideal. Then R/\mathfrak{p} is a domain. So, modules over R/\mathfrak{p} have rank.

Definition 5.3. Define the *p-rank* of an R -module M to be the rank of the R/\mathfrak{p} -module

$$R/\mathfrak{p} \otimes M = M/\mathfrak{p}M.$$

This is the dimension of the vector space

$$Q(R/\mathfrak{p}) \otimes M.$$

Example 5.4. Let $R = \mathbb{Z}$ and

$$M = \mathbb{Z}/20 \oplus \mathbb{Z}/8.$$

The prime number $p = 5$ is irreducible and thus generates a prime ideal $\mathfrak{p} = (5) = 5\mathbb{Z}$. Here $R/\mathfrak{p} = \mathbb{Z}/5$ is a field.

The 5-rank of M is the dimension of the vector space:

$$\begin{aligned} \mathbb{Z}/5 \otimes M &= \mathbb{Z}/5 \otimes (\mathbb{Z}/20 \oplus \mathbb{Z}/8) \\ &= (\mathbb{Z}/5 \otimes \mathbb{Z}/20) \oplus (\mathbb{Z}/5 \otimes \mathbb{Z}/8) \\ &= \mathbb{Z}/(5, 20) \oplus \mathbb{Z}/(5, 8) \\ &= \mathbb{Z}/5 \end{aligned}$$

which is 1. In the first step we used the distributivity of tensor product over direct sum. In the second step we used the rule that

$$M \otimes R/(p) = M/pM.$$

So,

$$\mathbb{Z}/5 \otimes \mathbb{Z}/20 = \frac{\mathbb{Z}}{5\mathbb{Z} + 20\mathbb{Z}} = \frac{\mathbb{Z}}{5\mathbb{Z}}$$

and

$$\mathbb{Z}/5 \otimes \mathbb{Z}/8 = \frac{\mathbb{Z}}{5\mathbb{Z} + 8\mathbb{Z}} = \frac{\mathbb{Z}}{\mathbb{Z}} = 0$$

Similarly, the 2-rank of M is the dimension over $\mathbb{Z}/2$ of

$$\mathbb{Z}/2 \otimes M = \mathbb{Z}/2 \otimes (\mathbb{Z}/20 \oplus \mathbb{Z}/8) = \mathbb{Z}/2 \oplus \mathbb{Z}/2$$

which is 2. For all other prime numbers p , the p -rank of M is zero.

With this example we decided that we could state without proof the general formula.

Proposition 5.5. (1) Suppose $R = \mathbb{Z}$ and

$$M = \bigoplus_{i=1}^k \mathbb{Z}/n_i.$$

Then the p -rank of M is the number of indices i so that $p|n_i$.

(2) More generally, suppose that R is a PID and

$$M = \bigoplus_{i=1}^k R/(p_i^{n_i})$$

where $p_i \in R$ are irreducible. Then the p -rank of M is the number of indices i so that $p = p_i$.

We will use the following observation.

Corollary 5.6. The p -rank of a cyclic module is either 0 or 1.

5.3. p -primary modules. Now suppose that R is a PID and p is a fixed irreducible element. Suppose that M is f.g. p -primary. Then

$$M = \bigoplus_{i=1}^k R/(p^{n_i}).$$

The p -rank of M is the number of summands k . We want to find a formula for the numbers n_i . In order to do this, we asked: *What is the p -rank of $p^m M$?*

We took one summand $R/(p^n)$ and noted that the annihilator of this module is (p^n) and $p^m \in (p^n)$ if and only if $m \geq n$. Therefore, $p^m R/(p^n) = 0$ if and only if $m \geq n$. If $m < n$ then $p^m R/(p^n)$ is nonzero and cyclic. Being p -primary, this makes its p -rank equal to 1. So:

$$p\text{-rank}(p^m R/(p^n)) = \begin{cases} 1 & \text{if } m < n \\ 0 & \text{if } m \geq n \end{cases}$$

So, the p -rank of

$$p^m M = \bigoplus_{i=1}^k p^m R/(p^{n_i})$$

is equal to the number of indices i for which $n_i > m$. Now we have enough invariants to show that the formula given in the structure theorem for f.g. modules over a PID is unique.

Example 5.7. Suppose that $R = \mathbb{Z}$ and $M = \mathbb{Z}^5 \oplus \mathbb{Z}/6 \oplus \mathbb{Z}/27$.

(1) First, take the rank: $\mathbb{Q} \otimes M = \mathbb{Q}^5$. So, $rM = 5$.

(2) The 2-rank of M is $5 + 1 = 6$ since

$$\mathbb{Z}/2 \otimes M = M/2M = (\mathbb{Z}/2)^5 \oplus \mathbb{Z}/(2, 6) \oplus \mathbb{Z}/(2, 27) = (\mathbb{Z}/2)^6.$$

(3) This implies that M has one cyclic 2-primary summand $\mathbb{Z}/2^n$. To find n we compute the 2-ranks of $2M, 4M$, etc. until we reach 5. But

$$2M = (2\mathbb{Z})^5 \oplus 2\mathbb{Z}/6\mathbb{Z} \oplus 2\mathbb{Z}/27 \cong \mathbb{Z}^5 \oplus \mathbb{Z}/3 \oplus \mathbb{Z}/27$$

which has 2-rank 5. So, we see that the 2-primary summand of M is $\mathbb{Z}/2$.

(4) The 3-rank of M is $5 + 2 = 7$ since

$$\mathbb{Z}/3 \otimes M = M/3 = (\mathbb{Z}/3)^5 \oplus \mathbb{Z}/(3, 6) \oplus \mathbb{Z}/(3, 27) = (\mathbb{Z}/3)^7.$$

(5) So, M has 2 cyclic 3-primary summands. We need to calculate the 3-ranks of $3M, 9M$, etc.

$$3M = (3\mathbb{Z})^5 \oplus 3\mathbb{Z}/6 \oplus 3\mathbb{Z}/27 \cong \mathbb{Z}^5 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/9.$$

$$9M \cong \mathbb{Z}^5 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/3.$$

$$27M \cong \mathbb{Z}^5 \oplus \mathbb{Z}/2.$$

So, $M, 3M, 9M, 27M$ have 3-rank 7,6,6,5 respectively. We stop when we reach the rank of M which is 5. These numbers show that the 3-primary part of M is $\mathbb{Z}/3 \oplus \mathbb{Z}/3^3$.

- (6) For all other primes p , the p -rank of M is 5. So, the decomposition of M is

$$M = \mathbb{Z}^5 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/3 \oplus \mathbb{Z}/3^3.$$

Example 5.8. Suppose that M is a finitely generated abelian group with $rM = 2$, 2-rank of $M, 2M, 4M, 8M, 16M$ equal to 5, 5, 4, 3, 2 and 3-rank of $M, 3M, 9M$ equal to 4, 4, 2 and p -rank of M equal to 2 for all other primes. Then

$$\begin{aligned} M &\cong \mathbb{Z}^2 \oplus (\mathbb{Z}/4)^2 \oplus \mathbb{Z}/8 \oplus \mathbb{Z}/16 \oplus (\mathbb{Z}/9)^2 \\ &\cong \mathbb{Z}^2 \oplus \mathbb{Z}/144 \oplus \mathbb{Z}/72 \oplus \mathbb{Z}/8 \oplus (\mathbb{Z}/4)^2. \end{aligned}$$

(In this order each denominator divides the previous one.)

Theorem 5.9. *In the decomposition of a finitely generated module over a PID:*

$$M \cong R^r \oplus \bigoplus R/(p_i^{n_i})$$

the numbers r and pairs (p_i, n_i) are uniquely determined up to re-ordering and can be determined from the rank of M and the p -rank of M, pM, p^2M , etc. for each irreducible p .