MATH 5045C: ADVANCED ALGEBRA I (MODULE THEORY) COMPREHENSIVE EXAM EDITION

HEESUNG YANG

1. January 7: Rings

Definition 1.1. A *ring* R is a set with two binary operations called addition $(+)$ and multiplication $(\cdot)$ such that

(1) $\langle R, +\rangle$ is an abelian group
(2) $\cdot$ is associative (i.e., $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$)
(3) $\cdot$ and $+$ are distributive over one another (i.e., $a(b+c) = ab+ac$ and $(a+b)c = ac+bc$).

Definition 1.2. A ring R is *commutative* if $ab = ba$ for all $a, b \in R$. Otherwise a ring R is *non-commutative.* A ring R *has unity* (or *has identity*) if $\cdot$ has an identity, which we call it 1 (i.e., $1 \in R$ and $1 \cdot a = a$ for all $a \in R$). An element $a \in R$ is a *unit* if there exist a left multiplicative inverse a' and a right multiplicative inverse a'' such that $a'a = aa'' = 1$.

Example. $\mathbb{Z}, \mathbb{R}$, and $\mathbb{Z}[x]$ are examples of (commutative) rings. $M_2(\mathbb{Z})$, the 2×2-matrix ring over $\mathbb{Z}$ is a (non-commutative) ring.

Proposition 1.1. $a' = a''$. *In other words, a left multiplicative inverse of* a *and a right multiplicative inverse of* a *are the same.*

Proof. $a'a = 1$, so $a'aa'' = a''$. Thus $a' = a''$. □

Definition 1.3. A non-zero element $a \in R$ is a *zero-divisor* if there exists $b \neq 0 \in R$ such that $ab = 0$ or $ba = 0$. If R is commutative, has unity, and has no zero-divisors, then R is an *integral domain* (or *domain* in short). A *field* is an integral domain in which every non-zero element is a unit.

Example. $\mathbb{Z}$ is a commutative ring with unity 1 and units ± 1. $\mathbb{Z}$ has no zero divisors. Thus $\mathbb{Z}$ is an integral domain. On the other hand, $\mathbb{Z}/6\mathbb{Z}$ has unity 1 and the units are $1, 5$. However, $\mathbb{Z}/6\mathbb{Z}$ has three zero divisors, namely $2, 3, 4$. Notice that $2 \cdot 3 = 4 \cdot 3 = 0$. Therefore $\mathbb{Z}/6\mathbb{Z}$ is not an integral domain.

Example. $\mathbb{Z}/p\mathbb{Z}$ for p prime, $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{C}(x)$ are examples of fields.

Remark 1.1. Units *cannot* be zero divisors (left as an exercise).

Definition 1.4. Let R be a ring. A *left (resp. right) ideal* I *of* R is a non-empty subset $I \subseteq R$ such that:

- $ra \in I$ (resp. $ar \in I$) for any $a \in I$ and $r \in R$
- $a - b \in I$ for any $a, b \in I$.

An ideal usually means a left and right ideal.

Date: 9 April 2019.

Example. Let $R = \mathbb{Z}$ and $I = 3\mathbb{Z} = \{3x : x \in \mathbb{Z}\}$. Then $I = (3)$ (i.e., I is an ideal generated by 3). Since every ideal of $\mathbb{Z}$ is generated by a single element, R is in fact a PID (principal ideal domain). Every ideal is finitely generated in Noetherian rings, so $\mathbb{Z}$ is Noetherian.

$\mathbb{R}[x]$ is a ring (in fact it is a Euclidean domain). Then (x) and (x^2+3) are both ideals of $\mathbb{R}[x]$.

Example. However, $\mathbb{Z}[x]$ is not a PID (however, it is a UFD (unique factorization domain)). Note that there does not exist $f \in \mathbb{Z}[x]$ such that $(2, x) = (f(x))$.

Definition 1.5. Let R be a ring. A *left R-module* M over R is an abelian group $\langle M, + \rangle$ along with an action of R on M, denoted by multiplication such that

(1) $r(x + y) = rx + ry$ for all $r \in R$ and $x, y \in M$
(2) $(r + s)x = rx + sx$ for all $r, s \in R$ and $x \in M$
(3) $(rs)x = r(sx)$ for all $r, s \in R$ and $x \in M$.
(4) $1_R \cdot x = x$ for all $x \in M$, provided that R has unity.

A *right R-module* is defined similarly, but with the action of R from the right.

Remark 1.2. Every ring R is an R-module (and a $\mathbb{Z}$-module also).

Example. Every abelian group is a $\mathbb{Z}$-module. Every k-vector space is a k-module for a field k. $\mathbb{Z}[x]$ and $\mathbb{Z}/6\mathbb{Z}$ are $\mathbb{Z}$-modules.

Example. For every ring R and an ideal I, R/I is an R-module (left as an exercise). Let $r \in R$ and $a + I \in R/I$. Then the action is given by $r(a + I) = ra + I$.

Example. Let I be an ideal of ring R. Then I is an R-module.

2. January 9

Definition 2.1. Let R be a ring, and M an R-module. Then a *submodule of M* is a subgroup N of M which is also an R-module under the same action of R.

Lemma 2.1 (The submodule criterion)**.** *Let R be a ring* with unity*, M a (left) R-module, and $N \subseteq M$. Then N is a submodule of N of M if and only if*

(1) N is non-empty, and
(2) $x + ry \in N$ for an $r \in R$ and $x, y \in N$.

Remark 2.1. Notice that R having the unity is crucial, as we will see in the proof. If R has no unity, then we need to go back to the definition and check one by one instead.

Proof. ($\Rightarrow$) This is a routine application of the definition of an R-module to verify that those two conditions hold.

($\Leftarrow$) Suppose that N satisfies the listed criteria. Then N is a subgroup of M. The first condition implies that there exists $x \in N$. Thus $x + (-1)x = 0 \in N$ by the second condition. Finally, by the second condition, for any $x, y \in N$ we have $0 - x = -x \in N$ and $x + 1 \cdot y = x + y \in N$. Thus for any $x \in N$ and $r \in R$, we have $0 + rx = rx \in N$. Hence N is closed under action of R. The remaining properties (distributivity) follow because M is an R-module already: notice that they are inherited from M. ☐

Definition 2.2. Let R be a ring and M, N R-modules. A function $\varphi : M \to N$ is an *R-module homomorphism* if

(1) $\varphi(x+y) = \varphi(x) + \varphi(y)$ for all $x, y \in M$
(2L) (for left R-modules) $\varphi(rx) = r\varphi(x)$ for all $x \in M$ and $r \in R$.
(2R) (for right R-modules) $\varphi(xr) = \varphi(x)r$ for all $x \in M$ and $r \in R$.

Additionally, if $\varphi : M \to N$ is also

(1) injective, then φ is an *R-module monomorphism.*
(2) surjective, then φ is an *R-module epimorphism.*
(3) bijective, then φ is an *R-module isomorphism.*
(4) $M = N$, then $\varphi : M \to M$ is an *R-module endomorphism.*
(5) a bijective endomorphism, then φ is an *R-module automorphism.*

Proposition 2.1. *$\varphi(0) = 0$ for any R-module homomorphism φ.*

Proof. $\varphi(0) = \varphi(0+0) = 2\varphi(0)$, so $\varphi(0) = 0$. □

Example. We examine some examples of module homomorphisms.

- A group homomorphism of abelian groups is a $\mathbb{Z}$-module homomorphism.
- A linear transformation of k-vector spaces is a k-module homomorphism.
- If $\varphi : R \to S$ is a ring homomorphism, then S is an R-module with action of R defined as $r \cdot x = \varphi(r)x$ for all $r \in R, x \in S$. Then S is an R-module. Evidently, R is also an R-module, so φ is in fact an R-module homomorphism. Indeed,
  (1) $\varphi(x+y) = \varphi(x) + \varphi(y)$ for all $x, y \in R$ (since φ is a ring homomorphism)
  (2) $\varphi(rx) = \varphi(r)\varphi(x) = r \cdot \varphi(x) = r\varphi(x)$ for $r, x \in R$.

Lemma 2.2. *Let R be a ring with unity, and M and N are left R-modules. Then the following are equivalent:*

(i) $\varphi : M \to N$ is an R-module homomorphism.
(ii) $\varphi(x + ry) = \varphi(x) + r\varphi(y)$ for all $x, y \in M$ and $r \in R$.

Proof. Exercise. □

Definition 2.3. Let $\varphi : M \to N$ be a homomorphism of left R-modules. Then *kernel of* φ is

$$\ker \varphi = \{x \in M : \varphi(x) = 0\}.$$

The *image of* φ is

$$\operatorname{im} \varphi = \{y \in N : y = \varphi(x) \text{ for some } x \in M\}.$$

Lemma 2.3. *If $\varphi : M \to N$ is a left R-module homomorphism, then $\varphi(M) = \operatorname{im} \varphi$ is submodule of N, and $\ker \varphi$ is submodule of M.*

Proof. From group theory, we already know that $\ker \varphi$ and $\operatorname{im} \varphi$ are subgroups. Thus we only need to verify they are also modules. For $\varphi(M)$, for any $r \in R$ and $x \in \varphi(M)$ there exists $y \in M$ such that $x = \varphi(y)$. Thus, $rx = r\varphi(y) = \varphi(ry) \in \varphi(M)$ since $ry \in M$. Thus $\varphi(M)$ is a submodule of N.

As for the kernel, for any $r \in R$ and $x \in \ker \varphi$ we have $\varphi(rx) = r\varphi(x) = r0 = 0$. Thus $rx \in \ker \varphi$, as required. □

Definition 2.4. Let M, N be left R-modules, and let

$$\operatorname{Hom}_R(M, N) := \{\varphi : M \to N \mid \varphi \text{ is an } R\text{-module homomorphism}\}.$$

Define addition on $\mathrm{Hom}_R(M,N)$ as follows. For any $\varphi, \psi \in \mathrm{Hom}_R(M,N)$, define

$$(\varphi+\psi)(x) := \varphi(x) + \psi(x) \text{ for all } x \in M.$$

It is not hard to see that $\varphi + \psi : M \to N$ is an R-module homomorphism. We see $\varphi + \psi$ respects addition since for any $x, y \in M$,

$$\begin{aligned}(\varphi+\psi)(x+y) &= \varphi(x+y) + \psi(x+y)\\ &= \varphi(x) + \varphi(y) + \psi(x) + \psi(y)\\ &= (\varphi+\psi)(x) + (\varphi+\psi)(y).\end{aligned}$$

Similarly, we have, for any $r \in R$ and $x \in M$,

$$\begin{aligned}(\varphi+\psi)(rx) &= \varphi(rx) + \psi(rx) = r\varphi(x) + r\psi(x)\\ &= r(\varphi(x) + \psi(x)) = r((\varphi+\psi)(x)).\end{aligned}$$

Hence $\psi + \varphi \in \mathrm{Hom}_R(M,N)$ for all $\varphi, \psi \in \mathrm{Hom}_R(M,N)$. Let $0 \in \mathrm{Hom}_R(M,N)$ be the zero homomorphism $\mathbf{0} : M \to N$ (i.e., $\mathbf{0}(x) = 0$ for all $x \in M$), which serves as the identity element. It is not that hard to see that $-\varphi \in \mathrm{Hom}_R(M,N)$ defined as $x \mapsto -\varphi(x)$ is also an R-module homomorphism for any $\varphi \in \mathrm{Hom}_R(M,N)$. Therefore $\varphi + (-\varphi) = \mathbf{0}$.

Thus, we show that $\langle \mathrm{Hom}_R(M,N), +\rangle$ is an abelian group. Can we make $\mathrm{Hom}_R(M,N)$ into an R-module? The answer is yes, provided that R is *commutative*, with action of R defined as $(r\varphi)(x) = r\varphi(x) = \varphi(rx)$ for any $r \in R, x \in M, \varphi \in \mathrm{Hom}_R(M,N)$.

3. January 11

Let R be a commutative ring, M, N R-modules. We define an action of R on $\mathrm{Hom}_R(M,N)$ as follows: let $r\varphi : M \to N$ satisfy $(r\varphi)(x) = r\varphi(x)$ where φ is an R-module homomorphism from M to N. We need to verify that $r\varphi : M \to N$ is an R-module homomorphism.

(1) $(r\varphi)(x+y) = r \cdot \varphi(x+y) = r(\varphi(x) + \varphi(y)) = r \cdot \varphi(x) + r \cdot \varphi(y) = (r\varphi)(x) + (r\varphi)(y)$ fo rall $x, y \in M$ and $r \in R$.
(2) Let $r, s \in R$ and $x \in M$. Then $(r\varphi)(sx) = r \cdot \varphi(sx) = rs\varphi(x) = sr\varphi(x) = s(r\varphi)(x)$, as needed.

Proposition 3.1. $\mathrm{Hom}_R(M,N)$ *under the action of R defined above is an R-module.*

Proof. We know $\mathrm{Hom}_R(M,N)$ is an abelian group and is closed under the action. So it remains to verify the criteria for modules. Suppose that $r, s \in R$ and $\varphi, \psi \in \mathrm{Hom}_R(M,N)$.

(1) We need to show that $(r+s)\varphi = r\varphi + s\varphi$. (Exercise)
(2) We need to show that $r(\varphi + \psi) = r\varphi + r\psi$. (Exercise)
(3) We also need to show that $(rs)\varphi = r(s\varphi)$. Indeed, $((rs)\varphi)(x) = rs\varphi(x) = r(s\varphi(xx)) = r(s\varphi)(x)$.

Thus $\mathrm{Hom}_R(M,N)$ is an R-module as required. □

3.1. Composition of homomorphisms

Proposition 3.2. *Let M, N, L be R-modules, and suppose $\varphi \in \mathrm{Hom}_R(M,L)$ and $\psi \in \mathrm{Hom}_R(L,N)$. Then $\psi \circ \varphi : M \to N \in \mathrm{Hom}_R(M,N)$, i.e., $\psi \circ \varphi$ is a homomorphism.*

Proof. This is a straightforward verification.

$$\psi \circ \varphi(x+y) = \psi(\varphi(x+y)) = \psi(\varphi(x)+\varphi(y)) = \psi \circ \varphi(x) + \psi \circ \varphi(y)$$
$$\psi \circ \varphi(rx) = r(\psi \circ \varphi(x))(\text{Exercise.}),$$

since ψ and φ are R-module homomorphisms. □

Proposition 3.3. *Suppose R is a commutative ring and M an R-module. Let $+$ be the usual addition, and $\cdot$ be the composition of homomorphisms. Then $\mathrm{Hom}_R(M, M)$ is a ring with unity 1.*

Proof. Exercise. □

3.2. **Quotient modules**

Suppose M is an R-module, and N a submodule of M. Then M/N is the quotient group $\{x+N : x \in M\}$. Notice that R can act on M/N. For any $r \in R$ and $x+N \in M/N$, let the action be

$$r(x+N) := rx + N.$$

First, observe that this action is well-defined. Indeed, if $x+N = y+N$ in M/N, and $r \in R$, then $x-y \in N$. But N is a submodule, so $r(x-y) \in N$ also. Hence $rx - ry \in N$ so $rx + N = ry + N$, as required. Second, we want to show that M/N is an R-module under this action. That is, we need to verify the three following conditions:

(1) $r((x+y)+N) = (rx+N)+(ry+N)$ (Exercise)
(2) $(r+s)(x+N) = r(x+N)+s(x+N)$
(3) $(rs)(x+N) = r(sx+N)$

Definition 3.1. The *(group) projection map* $\pi : M \to M/N$ is defined by $\pi(x) = x+N$.

It is evident that π is a(n additive) group homomorphism. That π is R-linear is also evident: for any $r \in R$ and $x \in M$, we have $\pi(rx) = rx + N = r(x+N) = r\pi(x)$.

3.3. **Isomorphism theorems for modules**

Assume that M, N are R-modules, and that A and B are submodules of M.

Theorem 3.1 (First isomorphism theorem for modules)**.** *Let $\varphi : M \to N$ be a R-module homomorphism. Then $\ker\varphi$ is a submodule of M and $M/\ker\varphi \cong \varphi(M)$.*

Proof. First part: Exercise. Since $M/\ker\varphi \cong \varphi(M)$ as groups already, by the first isomorphism theorem for groups, it suffices to verify that the group isomorphism given by the first isomorphism theorem for groups is R-linear. (Exercise.) □

Theorem 3.2 (Second isomorphism theorem for modules)**.** $(A+B)/B \cong A/(A\cap B)$.

Proof. Pick an appropriate $\varphi : A+B \to A/(A\cap B)$. Show that φ is surjective and that $\ker\varphi = B$. Just show that φ is R-linear, and then apply the first isomorphism theorem. Do not try to show that the map is additive – this is already given by the theorem for group counterparts. □

Theorem 3.3 (Third isomorphism theorem for modules)**.** *If $A \subseteq B$, then $(M/A)/(M/B) \cong A/B$.*

Theorem 3.4 (Correspondence theorem for modules (Fourth isomorphism theorem for modules))**.** *There is an inclusion-preserving one-to-one correspondence between the set of submodules of M containing A and the set of submodules of M/A. This correspondence commutes with taking sums and intersections (i.e., there is an isomorphism of lattices between the submodule lattice of M/A and the lattice of submodules of M containing A).*

Remark 3.1. The last statement of the fourth isomorphism theorem for modules shows why the theorem is also called the "lattice isomorphism theorem".

4. January 14

Definition 4.1. A *category* is a collection of objects and morphisms between the objects. A category $\mathcal{C}$ comes with:

- $\mathrm{Obj}(\mathcal{C})$: collection of objects in $\mathcal{C}$.
- for every $A, B \in \mathrm{Obj}(\mathcal{C})$ a set $\mathrm{Hom}_{\mathcal{C}}(A, B)$ of morphisms $f : A \to B$ with domain A and codomain B of f such that:
  - (i) for every $A \in \mathrm{Obj}(\mathcal{C})$ there exists $\mathbf{1}_A \in \mathrm{Hom}_{\mathcal{C}}(A, A)$ which is the identity morphism on A. Therefore, there is always a morphism in $\mathrm{Hom}_{\mathcal{C}}(A, A) = \mathrm{End}_{\mathcal{C}}(A) \neq \emptyset$ (endomorphisms).
  - (ii) $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ and $g \in \mathrm{Hom}_{\mathcal{C}}(B, C)$ give a morphism $gf \in \mathrm{Hom}_{\mathcal{C}}(A, C)$. Hence, there exists a set function
  $$\begin{aligned}\mathrm{Hom}_{\mathcal{C}}(A, B) \times \mathrm{Hom}_{\mathcal{C}}(B, C) &\to \mathrm{Hom}_{\mathcal{C}}(A, C)\\ (f, g) &\mapsto gf.\end{aligned}$$
  - (iii) Composition is associative: $f \in \mathrm{Hom}_{\mathcal{C}}(A, B), g \in \mathrm{Hom}_{\mathcal{C}}(B, C), h \in \mathrm{Hom}_{\mathcal{C}}(C, D)$, then $h(gf) = (hg)f$.
  - (iv) For every $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$, $f\mathbf{1}_A = f$ and $\mathbf{1}_B f = f$.
  - (v) If $\mathrm{Hom}_{\mathcal{C}}(A, B) \cap \mathrm{Hom}_{\mathcal{C}}(C, D) \neq \emptyset$, then $A = C$ and $B = D$.

4.1. Generators for modules

Let R be a ring with unity 1. Let M be an R-module, and $N_1, N_2, \ldots, N_k$ submodules of M.

Definition 4.2. The *sum of* $N_1, \ldots, N_k$ is

$$N_1 + N_2 + \cdots + N_k := \{x_1 + \cdots + x_k \mid x_i \in N_i \text{ for all } i\}.$$

Proposition 4.1. *$N_1 + \cdots + N_k$ is a submodule of M.*

Proof. Exercise. □

Remark 4.1. If $N_1, \ldots, N_k$ are submodule of N, then $N_1 + \cdots + N_k$ is a submodule of M generated by $N_1 \cup \cdots \cup N_k$.

Definition 4.3. Let $A \subseteq M$ be a subset (not necessarily a submodule). Then define

$$RA := \{r_1 a_1 + \cdots + r_n a_n : a_1, \ldots, a_n \in A, r_1, \ldots, r_n \in R\},$$

which generates a submodule. We call RA the *submodule of M generated by A* (the smallest submodule of M containing A). If $A = \emptyset$ we say $RA = \{0\}$. If A is finite, then RA is *finitely generated*. If $|A| = 1$, then RA is a *cyclic module*.

It is not entirely obvious if RA is actually a module, but it is not a difficult exercise to prove this is indeed the case.

Proposition 4.2. *RA is indeed a submodule of M.*

Proof. Exercise. □

Example. R is a cyclic R-module because $R = R1_R$. R/I is another example of a cyclic R-module since $R/I = R(1_R + I)$. $\mathbb{Z}[x]/(x^2) = \langle 1, x\rangle$ as a $\mathbb{Z}$-module. However, $\mathbb{Z}[x]$ is not a finitely generated $\mathbb{Z}$-module, since $\mathbb{Z}[x]$ is generated by $\{1, x, x^2, x^3, \dots\}$.

Definition 4.4. If $M_1, \dots, M_k$ are R-modules, then the *direct product of* $M_1, \dots, M_k$ is the collection

$$\prod_{i=1}^{k} M_i = M_1 \times M_2 \times \cdots \times M_k = \{(m_1, \dots, m_k) : m_i \in M_i \ \forall i\}.$$

This is also called the *external direct sum of* $M_1, \dots, M_k$, denoted by $M_1 \oplus M_2 \oplus \cdots \oplus M_k$.

Remark 4.2. For a family of abelian groups $\{G_i : i \in I\}$ (note that I may be uncountable), the direct product and the direct sum as follows:

$$\prod_{i\in I} G_i = \left\{ f : I \to \bigcup G_i \mid f(i) \in G_i \ \forall i \in I \right\}$$

$$\sum_{i\in I} G_i = \left\{ f \in \prod G_i \mid f(i) = 0 \text{ for all but finitely many } i \in I \right\}.$$

For any $f, g \in \prod G_i$, define the composition $fg : I \to \bigcup G_i$ be $i \mapsto f(i) + g(i)$. Therefore, if I is finite, then the direct sum and the direct product are equal. Finally, it is a straightforward verification to check that $\prod G_i$ is a group.

Proposition 4.3. *$M_1 \times \cdots \times M_k$ is an abelian group under component-wise addition. Furthermore, we can define a component-wise action on R*

$$r(x_1, \dots, x_k) = (rx_1, \dots, rx_k),$$

making $M_1 \times \cdots \times M_k$ into an R-module.

Proposition 4.4 (Direct sum of submodules)**.** *Let R be a ring with unity and M an R-module. Let $N_1, \dots, N_k$ be submodules of M. Then the following are equivalent:*

(i) The map $\pi : N_1 \times \cdots \times N_k \to N_1 + \cdots + N_k$ defined by

$$(n_1, \dots, n_k) \mapsto n_1 + \cdots + n_k$$

is an isomorphism of R-modules.

(ii) $N_j \cap (N_1 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_k) = \{0\}$ for all $j \in \{1, 2, \dots, k\}$ (mod k).

(iii) For any $x \in N_1 + \cdots + N_k$, x can be written uniquely *as $a_1 + \cdots + a_k$ where $a_i \in N_i$.*

Definition 4.5. If $N_1 + \cdots + N_k$ satisfies any of the conditions listen in Proposition 4.4, then $N_1 + \cdots + N_k$ is the *internal direct sum of* $N_1, \dots, N_k$, and we write $N_1 \oplus N_2 \oplus \cdots \oplus N_k$.

5. January 16

Proof of Proposition 4.4. ((1) ⇒ (2)) If $N_j \cap \sum_{i\neq j} N_i$ contains an element $a_j \neq 0$, then there exists $a_i \in N_i$ where $i \neq j$ such that

$$a_j = \sum_{i\neq j} a_i.$$

So $a_1+\cdots+a_{j-1}-a_j+a_{j+1}+\cdots+a_k = 0$. So if $\pi((a_1,\ldots,a_k)) = 0$, then $a_1 = \cdots = a_k = 0$. Thus $a_j = 0$, but it is a contradiction.

((2) ⇒ (3)) Suppose that $a_1+\cdots+a_k = b_1+\cdots+b_k$. Then there exist $a_i, b_i \in N_i$ where $i = 1,2,\ldots,k$. Fix $j \in \{1,2,\ldots,k\}$, and one can write

$$a_j-b_j = (b_1-a_1)+(b_2-a_2)+\cdots+(b_{j-1}-a_{j-1})+(b_{j+1}-a_{j+1})+\cdots+(b_k-a_k) \in N_j\cap\sum_{i\neq j} N_i = 0.$$

Thus $a_j - b_j = 0$, so $a_j = b_j$ for every j as required.

((3) ⇒ (1)) Let $\pi : N_1\times\cdots\times N_k \to N_1+\cdots+N_k$ is an isomorphism because $\pi(a_1,\ldots,a_k) = 0$ implies $a_1+\cdots+a_k = 0$. Thus $a_1 = a_2 = \cdots = a_k = 0$. Therefore π is injective. Clearly, π is surjective (clear from the definition of π). Also, it is straightforward to verify that π is a module homomorphism, so this will be left as an exercise. □

5.1. Universal property of direct sum of modules

Theorem 5.1. *Let R be a ring, let $\{M_i \mid i \in I\}$ be a family of R-modules, N an R-module, and $\{\psi_i : M_i \to N \mid i \in I\}$ a family of R-module homomorphisms. Then there exists a unique R-module homomorphism*

$$\psi : \sum_{i\in I} M_i \to N$$

such that $\psi_i = \psi_{M_i}$ for all $i \in I$. Furthermore, this $\sum M_i$ is uniquely determined *up to isomorphism by this property (i.e., $\sum M_i$ is a co-product in the category of R-modules).*

Proof. It is known that this works for all groups – we can define

$$\psi : \sum_{i\in I} M_i \to N$$

by $\psi((a_i)_{i\in I}) = \sum \psi_i(a_i)$. Verify that this is a group homomorphism and is R-linear (exercise). Also, it is a routine exercise to verify the rest of the claims. □

5.2. Exact sequences

Definition 5.1. Let M, N, L be R-modules. Then the sequence of R-module homomorphisms

$$M \xrightarrow{f} N \xrightarrow{g} L$$

is called *exact at N* if f is injective, g is surjective, and $\operatorname{im} g = \ker f$. Similarly, a *long exact sequence* is

$$\cdots \to M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \to \cdots$$

such that for every M_i, $\ker f_{i+1} = \operatorname{im} f_i$ for all i. A *short exact sequence* is of the form

$$0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0$$

such that f is injective, g is surjective, and $\operatorname{im} f = \ker g$.

Remark 5.1. If $0 \xrightarrow{f} M \xrightarrow{g} N$ is exact at M, then $\ker g = \operatorname{im} f = 0$. Therefore g is injective. Similarly, if $M \xrightarrow{f} E \xrightarrow{g} 0$ is exact at N, so $\ker g = N = \operatorname{im} f$. Thus f is surjective in this case.

Example. If M is an R-module and N a submodule of M, then $0 \to N \xrightarrow{i} M$ is exact; similarly, $M \xrightarrow{\pi} N \to 0$ is exact as well. Thus we get the short exact sequence

$$0 \mapsto N \xrightarrow{i} M \xrightarrow{\pi} M/N \to 0$$

where i is the injection map and M the projection map.

Definition 5.2. The *co-kernel* of an R-module homomorphism $f : M \to N$ is $\operatorname{CoKer}(f) := N/\operatorname{im} f$.

Remark 5.2. Let $f : M \to N$ be an R-module homomorphism. Then we have an exact sequence

$$0 \to \ker f \to M \xrightarrow{f} N \xrightarrow{\pi} \operatorname{CoKer}(f) \to 0.$$

How many short exact sequences can we extract out of this? We can generate at least two short exact sequences. $0 \to \ker f \to M \to \operatorname{im} f \to 0$ and $0 \to \operatorname{im} f \to N \to N/\operatorname{im} f \to 0$.

Example. For any M, N, and their direct sum $M \oplus N$, the sequence

$$0 \to M \xrightarrow{i} M \oplus N \xrightarrow{\pi} N \to 0$$

is a short exact sequence. Note that $\operatorname{im} i = M \oplus 0$, and clearly $\ker \varphi = M \oplus 0$.

6. January 18

Definition 6.1. Suppose that

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

is a short exact sequence. Then this short exact sequence is *split exact* if $B \cong A \oplus C$.

Definition 6.2. Two short exact sequences $0 \to A \to B \to C \to 0$ and $0 \to A' \to B' \to C' \to 0$ of R-modules are *isomorphic* if there is a commutative diagram of R-module homomorphisms such that $g \circ \alpha = \alpha' \circ f$ and $h \circ \beta = \beta' \circ g$.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A & \xrightarrow{\alpha} & B & \xrightarrow{\beta} & C & \longrightarrow & 0 \\
 & & \downarrow f & & \downarrow g & & \downarrow h & & \\
0 & \longrightarrow & A' & \xrightarrow{\alpha'} & B' & \xrightarrow{\beta'} & C' & \longrightarrow & 0
\end{array}$$

Theorem 6.1. *Let R be a ring, and let $0 \to A \to B \to C \to 0$ be a short exact sequence of R-module. Then the following are equivalent:*

(i) There exists an R-module homomorphism $h : C \to B$ such that $g \circ h = \mathrm{id}_C$.
(ii) There exists an R-module homomorphism $k : B \to A$ such that $k \circ f = \mathrm{id}_A$.
(iii) $B \cong A \oplus C$ and the sequence above can be isomorphically written as

$$0 \to A \xrightarrow{i_1} A \oplus C \xrightarrow{\pi_2} C \to 0.$$

Therefore the short exact sequence is split exact.

To prove the equivalent conditions for split exact sequence, we need the following lemma.

Lemma 6.1 (Short five lemma)**.** *Let R be a ring, and where is a commutative diagram of R-modules and R-module homomorphisms*

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\
0 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \longrightarrow & 0
\end{array}$$

such that each row is a short exact sequence. Then

(i) If α and γ are monomorphisms, then β is also a monomorphism.
(ii) If α and γ are epimorphisms, then β is also an epimorphism.
(iii) If α and γ are isomorphisms, then β is also an isomorphism.

Proof. (i) Suppose $x \in \ker \beta$. Then $\beta(x) = 0$, so $(g' \circ \beta)(x) = 0$. But then $g' \circ \beta = \gamma \circ g$. But then γ is a monomorphism, so $g(x) = 0$. Hence $x \in \ker g = \operatorname{im} f$. So there exists $y \in A$ such that $x = f(y)$. Hence $(\beta \circ f)(y) = (f' \circ \alpha)(y) = 0$; but f' is a monomorphism, so $\alpha(y) = 0$. But again α is also a monomorphism, so $y = 0$. Hence $x = f(y) = 0$ as needed.

(ii) Let $y \in B'$. Then $g'(y) \in C'$. But since γ is an epimorphism, there exists $z \in C$ such that $g'(y) = \gamma(z)$. But g is an epimorphism, so there is $u \in B$ such that $z = g(u)$. So $g'(y) = \gamma(z) = (\gamma \circ g)(u) = (g' \circ \beta)(u)$. It thus follows that $g'(\beta(u) - y) = 0$, so $\beta(u) - y \in \ker g' = \operatorname{im} f'$. Since $\beta(u) - y \in \operatorname{im} f'$, there is $v \in A'$ such that $\beta(u) - y = f'(v)$. α is an epimorphism, so one can find $w \in A$ such that $\beta(u) - y = (f' \circ \alpha)(w) = (\beta \circ f)(w)$. So $\beta(u - f(w)) = y$. This proves that β is surjective.

(iii) This is immediate from (i) and (ii). $\square$

Proof of Theorem 6.1. ((i) $\Rightarrow$ (iii)) Consider the two short exact sequences

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A & \xrightarrow{f} & B & \underset{h}{\overset{g}{\rightleftarrows}} & C & \longrightarrow & 0 \\
 & & {\scriptstyle \mathrm{id}}\uparrow & & {\scriptstyle \varphi}\uparrow & & {\scriptstyle \mathrm{id}}\uparrow & & \\
0 & \longrightarrow & A & \xrightarrow{\iota_1} & A \oplus C & \xrightarrow{\pi_2} & C & \longrightarrow & 0
\end{array}$$

We need to show that these two sequences are isomorphic. Thus we need to find an isomorphism φ such that the diagram above commutes. Define $\varphi : A \oplus C \to B$ by $(a, c) \mapsto f(a) + h(c)$. Note that φ is well-defined since (a, c) is a unique representative for this element, and both f and h are well-defined. φ is a homomorphism since

$$\varphi(r(a, c)) = \varphi((ra, rc)) = f(ra) + h(rc) = r(f(a) + h(c)) = r\varphi(a, c)$$

$$\begin{aligned}
\varphi((a, c) + (a', c')) &= \varphi((a + a', c + c')) = f(a + a') + h(c + c') \\
&= f(a) + h(c) + f(a') + h(c') = \varphi((a, c)) + \varphi((a', c')).
\end{aligned}$$

We want to show that the diagram commutes. Pick $(a, c) \in A \oplus C$. Then $(g \circ \varphi(a, c) = g(f(a) + h(c)) = (g \circ f)(a) + (g \circ h)(c) = c$. On the other hand, $(\mathrm{id} \circ \pi_2)(a, c) = \mathrm{id}(c) = c$. Thus $g \circ \varphi \equiv \mathrm{id} \circ \pi_2$. We can use the similar argument to show that the other side commutes, i.e., $\varphi \circ i_1 \equiv f \circ \mathrm{id}$. That φ is an isomorphism follows from the short five lemma.

((ii) ⇒ (iii)) Assume that there is k such that $k \circ f = \mathrm{id}_A$. Define $\varphi : B \to A \oplus C$ so that $b \mapsto (k(b), g(b))$. φ is well-defined since k and g are well-defined also. φ is also an R-module homomorphism since k and g are. Indeed, $\varphi(b_1 + b_2) = (k(b_1 + b_2), g(b_1 + b_2)) = (k(b_1), g(b_1)) + (k(b_2), g(b_2)) = \varphi(b_1) + \varphi(b_2)$; also for any $r \in R$, $\varphi(rb_1) = (k(rb_1), g(rb_1)) = (rk(b_1), rg(b_1)) = r(k(b_1), g(b_1)) = r\varphi(b_1)$. So by the short five lemma, φ is an isomorphism, so the two short exact sequences are isomorphic as desired.

((iii) ⇒ (i), (ii)) We have an isomorphism of short exact sequences, i.e., φ_1, φ_2, and φ_3 are all isomorphisms.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A & \underset{k}{\overset{f}{\rightleftarrows}} & B & \underset{h}{\overset{g}{\rightleftarrows}} & C & \longrightarrow & 0 \\
 & & \uparrow{\scriptstyle \mathrm{id}} & & \uparrow{\scriptstyle \varphi} & & \uparrow{\scriptstyle \mathrm{id}} & & \\
0 & \longrightarrow & A & \underset{\pi_1}{\overset{\iota_1}{\rightleftarrows}} & A \oplus C & \underset{\iota_2}{\overset{\pi_2}{\rightleftarrows}} & C & \longrightarrow & 0
\end{array}$$

We let $h : C \to B$ where $h = \varphi_2^{-1} i_2 \varphi_3$. Note that h is well-defined since it is just the composition of three homomorphisms. For any $c \in C$, observe that $\varphi_2^{-1} i_2 \varphi_3(c) \in B$. So by the commutativity, $\varphi_3 g(b) = \pi_2 \varphi_2(b) = \pi_2 \varphi_2(\varphi_2^{-1} i_2 \varphi_3(c)) = \pi_2(i_2 \varphi_3(c)) = \varphi_3(c)$. But then φ_3 is an isomorphism, so $g(b) = c$ from which $gh(c) = c$ follows. Hence $gh = \mathrm{id}_C$.

Now define $k : B \to A$ by $k := \varphi_1^{-1} \pi_1 \varphi_2$ which is a well-defined homomorphism for the same reason h is. For any $a \in A$, we have $kf(a) = \varphi_1^{-1} \pi_1 \varphi_2 f(a) = \varphi_1^{-1} \pi_1 i_1 \varphi_1(a) = a$, as desired. □

Remark 6.1. If M a R-module and M_1, M_2 submodules of M, we have a short exact sequence

$$0 \longrightarrow M_1 \cap M_2 \xrightarrow{f} M_1 \oplus M_2 \xrightarrow{g} M_1 + M_2 \longrightarrow 0,$$

where $f : m \mapsto (m, -m)$ and $g : (m_1, m_2) \mapsto m_1 + m_2$.

7. Detour: Nakayama's lemma

Definition 7.1. Let R be a commutative ring with unity. If R has a unique maximal ideal $\mathfrak{m}$, then $(R, \mathfrak{m})$ is a *local ring.*

Lemma 7.1. *Let R be a ring, I an ideal of R, and M an R-module. Then*

$$IM = \{am \mid a \in I, m \in M\}$$

is a submodule of M.

Lemma 7.2. *If M is a R-module, and I an ideal of R, then M/IM is an R/I-module, where the action of R/I is defined by $(r + I)(x + IM) : f = rx + IM$.*

Remark 7.1. Recall that if $(R, \mathfrak{m})$ is a local ring, then the only non-units of R are precisely the elements of $\mathfrak{m}$. Suppose that is not the case. Pick $x \in R \setminus \mathfrak{m}$. Consider the ideal $I = (x)$, and that $1 \notin I$ (since x is not a unit). Thus $I \neq R$. Since $\mathfrak{m}$ is the only maximal ideal, it follows that $(x) \leq \mathfrak{m}$. But this means $x \in \mathfrak{m}$ which is a contradiction.

Theorem 7.1 (Nakayama's lemma)**.** *Let R be a commutative ring with unity 1, I be an ideal of R, and M a finitely generated R-module. If $IM = M$, then there exists $r \in R$ satisfying $r \equiv 1 \pmod I$ that vanishes M (i.e., $rM = 0$).*

Theorem 7.2 (Nakayama's lemma, local ring version)**.** *Let $(R, \mathfrak{m})$ be a local ring, and M an R-module. Suppose that $x_1, \ldots, x_n \in M$. Then the following are equivalent:*

(i) $M = \langle x_1, x_2, \ldots, x_n \rangle$ is a finitely generated R-module.

(ii) $M/\mathfrak{m}M = \langle \overline{x_1}, \overline{x_2}, \ldots, \overline{x_n} \rangle$ is an $R/\mathfrak{m}$-vector space ($\overline{x_i}$ is the image of x_i under the map $M \to M/\mathfrak{m}M$. Note that $R/\mathfrak{m}$ is a field, so any $R/\mathfrak{m}$-module is automatically an $R/\mathfrak{m}$-vector space.

8. January 23: Free modules

Suppose that M is an R-module where R is a ring with unity 1.

Definition 8.1. A subset R of M is called *linearly independent* if $a_1x_1 + \cdots + a_nx_n = 0$ implies $a_1 = a_2 = \cdots = a_n = 0$ for all $a_1, \ldots, a_n \in R$ and $x_1, x_2, \ldots, x_n \in X$. If M is generated by a linearly independent subset X, then X is called a *basis* of M. A *free module* is a module with a non-empty basis.

Theorem 8.1. *Suppose that R is a ring with identity, and F an R-module. Then the following are equivalent:*

(i) F has a non-empty basis.

(ii) F is the internal direct sum of cyclic submodules.

(iii) F is isomorphic to a direct sum of copies of R (i.e., $F \cong R^n$ for some n; alternatively, $F \cong \oplus R$.)

Proof. ((ii) $\Leftrightarrow$ (iii)) They are equivalent statements since $Rx \cong R$ for any non-zero $x \in X$.

((i) $\Rightarrow$ (ii) & (iii)) If $X \neq \emptyset$ is a basis of F and $x \in X$, then we have a surjective R-module homomorphism $\varphi_x : R \to Rx$ defined by $\varphi_x(r) := rx$. φ_x is injective, since if $rx = 0$ then $r = 0$ (note that $x \in X$ is a basis, so $x \neq 0$). Thus $\ker \varphi_x = 0$ as needed. It is not hard to check that φ_x is a homomorphism.

Hence, we have

$$F \cong \bigoplus_{x \in X} Rx \cong \bigoplus_{x \in X} R.$$

Note that the second direct sum is internal, whereas the third direct sum is external; note also that the second isomorphism follows since φ_x is an isomorphism (and replace each Rx with R).

((iii) $\Rightarrow$ (i)) Suppose that $F \overset{\Psi}{\cong} \bigoplus_{x \in X} R$ where X is the index set of this direct sum. Define $\iota_x \in F$ to be the tuple such that

$$(\iota_x)_y = \begin{cases} 1 & (x = y) \\ 0 & \text{otherwise.} \end{cases}$$

Then $\{\iota_x : x \in X\}$ is a basis for $\bigoplus_{x \in X} R$. The image of $\{\iota_x : x \in X\}$ under Ψ is a basis for F. $\square$

Definition 9.1. A *division ring* (or a *skew field*) is a ring with 1 such that every non-zero element in a unit. A *field* is a commutative division ring, and a *vector space* is a module over a division ring.

Example. The quaternion ring is a standard example of a division ring.

Lemma 9.1. *Let V be a vector space over a division ring D, and let X be a maximal linearly independent subset of V. Then X is a basis of V.*

Proof. If $V' = \langle X \rangle \subseteq V$, we want to show that $V' = \langle V \rangle$. Since X is linearly independent, it is a basis of V'. Let $x \in V \setminus V'$. Then $X \cup \{x\}$ is linearly independent. Suppose otherwise. Then if

$$d_1x_1 + \cdots + d_nx_n + dx = 0$$

where $d_i, d \in D$ and $x_i \in X$, we have

$$x = d^{-1}(d_1x_1 + \cdots + d_nx_n) \in V'.$$

But this is a contradiction since $x \notin V'$. This forces $d = 0$, so $d_1x_1 + \cdots + d_nx_n = 0$. In turn, this implies $d_1 = d_2 = \cdots = d_n = 0$ as well. This implies $X \cup \{x\}$ is linearly independent, but this contradicts the fact that X is a maximal linearly independent set. □

Theorem 9.1 (Zorn's lemma)**.** *Let $A \neq \emptyset$ be a partially ordered set, such that every chain has an upper bound in A. Then A contains a maximal element.*

Theorem 9.2. *Let V be a vector space over a division ring D. Then V has a basis, so V is a free D-module. Moreover, if Y is a linearly independent subset of V, then there exists a basis X of V such that $Y \subseteq X$.*

Proof. The first part follows from the second part, and clearly $\emptyset$ is (vacuously) linearly independent by default, so wle will prove the second part only. Let

$$A := \{X \subseteq V : X \text{ linearly independent and } Y \subseteq X\}.$$

Since $Y \in A$, $A \neq \emptyset$. A is partially ordered by inclusion. If $\mathcal{C}$ is a chain in A, define

$$\underline{X} := \bigcup_{X \in \mathcal{C}} X \in A.$$

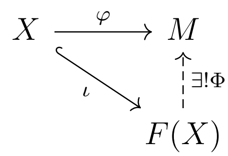
Then $\underline{X}$ is an upper bound of $\mathcal{C}$. By Zorn's lemma, A contains a maximal element B, so by Lemma 9.1, B is a basis of V. □

Theorem 9.3. *If V is a vector space over a division ring D, then every generating set of V contains a basis of V.*

Proof. If X is a generating set of V, let $A := \{Y \mid Y \subseteq X \text{ linearly independent}\}$, which is a partially ordered set under inclusion. Again, every chain has an upper bound by Zorn's lemma. Suppose that Y is a maximal element of A. Then $x \in \langle Y \rangle$ for all $x \in X$ (otherwise, we can add an element to Y, which contradicts the maximality of Y). Hence $V \subseteq \langle X \rangle \subseteq \langle Y \rangle$, so $V = \langle Y \rangle$. □

10. January 28 & 30

Theorem 10.1. *Let X be any set, and R a ring with unity. Then there exists a free R-module $F(X)$ on X satisfying the following universal property: for any R-module M and $\varphi : X \to M$ a function, there is a* unique *R-module homomorphism $\Phi : F(X) \to M$ such that $\Phi(x) = \varphi(x)$ for all $x \in X$. In other words, the following diagram commutes.*



Proof. Build $F(X)$. If $X = \emptyset$ then $F(X) = 0$. Otherwise, $F(X) = \{f : X \to R : f(x) = 0$ for all but finitely many $x \in X\}$. We will make $F(X)$ into an R-module. Let $f, g \in F(X)$ and $r \in R$, and let

$$(f+g)(x) := f(x) + g(x)$$
$$(rf)(x) := r.f(x)$$

for all $x \in X$. If $x \in X$ define $f_x \in F(X)$ as

$$f_x(y) := \begin{cases} 1 & y = x \\ 0 & \text{otherwise.} \end{cases}$$

So if $f \in F(X)$ then there are $x_1, \dots, x_n \in X$ such that

$$f = f(x_1)f_{x_1} + \cdots + f(x_n)f_{x_n}.$$

Note that $f(x_i) \in R$ and $f_{x_i} \in F(X)$ for all i. And we know this is unique, so $\{f_x : x \in X\}$ is a basis for $F(X)$. Thus $F(X)$ is a free R-module.

To check the universal property, suppose $\varphi : X \to M$. Define $\Phi : F(X) \to M$ so that

$$\Phi\left(\sum_{i=1}^{n} a_i f_{x_i}\right) = \sum_{i=1}^{n} a_i \varphi(x_i).$$

It is not hard to check if it is well-defined, is a homomorphism, and $\Phi|_X = \varphi$ (Exercise).

Every element of $F(X)$ has a unique presentation in the form of

$$\sum_{i=1}^{n} a_i f_{x_i}$$

for some $n \in \mathbb{Z}_+, a_i \in R$, and $x_i \in X$. Thus Φ is the unique extension of φ to $F(X)$ as needed. □

Proposition 10.1. *Every finitely generated R-module for R a ring with identity is the homomorphic image of a finitely generated free module.*

Proof. Let $X := \{x_1, \dots, x_n\}$, and $M = \langle X \rangle$ be a finitely generated R-module. By the universal property, there is a free R-module $F(X)$ and a homomorphism $\varphi : F(X) \to M$ satisfying $f_x \mapsto x$. □

Remark 10.1. In fact, $M \cong F(X)/\ker\varphi \cong R^n/\ker\varphi$.

10.1. **Free modules and ranks**

Suppose that F is a free module over a ring with 1. Do every two bases necessarily have the same cardinality? The answer is actually **no** in general, but it is true for commutative rings and division rings. Our main goal in this section is to prove this is indeed the case.

Definition 10.1. Let R be a commutative ring or a division ring, and let X be a basis of a free R-module F. Then the *rank* of F is the cardinality of X.

Theorem 10.2. *Let R be a ring with unity, and F a free module with basis X with $|X| = \infty$. Then every basis of X has the same cardinality as X. Therefore, if the basis is infinite, then the cardinality is unique* regardless of what the ring is.

Proof. Suppose Y is another basis of F whose basis is X. If Y is finite, suppose $Y = \{y_1, \ldots, y_n\}$. Then for all $y_i \in Y$ one can find $x_{i,1}, \ldots, x_{i,m_i} \in X$ and $r_{i,1}, \ldots, r_{i,m_i} \in R$ so that $y_i = r_{i,1}x_{i,1} + \cdots + r_{i,m_i}x_{i,m_i}$. Then $X' = \{x_{i,j} : 1 \le i \le n, 1 \le j \le m_i\}$ is a finite subset of X spanning F. Therefore X contains a finite-generating set for F, but this contradicts the fact that $|X| = \infty$. Therefore $|Y|$ is infinite.

Let $K(Y)$ be the set of finite subsets of Y, and define $f : X \to K(Y)$ so that $x \mapsto \{y_1, \ldots, y_n\}$ where $x = \sum_{i=1}^{n} r_i y_i$ is uniquely defined. (i.e., $r_1, r_2, \ldots, r_n \in R \setminus \{0\}$ are unique, and $y_1, \ldots, y_n \in Y$ are uniquely determined by x. Therefore f is well-defined. We make a few observations regarding f.

First, $\operatorname{im} f$ is an infinite set. Suppose otherwise, and let $X = \langle \bigcup_{A \in \operatorname{im} f} A \rangle$. Note that $A = f(x)$ for some x. Thus A is a finite set, and the finite union of finite sets is finite. Thus F is generated by a finite subset of Y, which is a contradiction. Second, for any $S \in \operatorname{im} f$ we have $|f^{-1}(S)| < \infty$. Let $x \in f^{-1}(S)$. Then $x \in \langle y : y \in S \rangle$ is a submodule of F. Hence $f^{-1}(S) \subseteq \langle y : y \in S \rangle$. Each y in S thus can be uniquely written as a sum of finite elements of X, and $|S| < \infty$. Hence $f^{-1}(S) \subseteq \langle X_S \rangle$, where X_S is a finite subset of X.

Now, if $x \in f^{-1}(S)$, then there are $x_1, \ldots, x_n \in X_S$ and $r_1, \ldots, r_n \in R$ such that $x = \sum R_i x_i$. Thus $f^{-1}(S) \subset X_S$. Therefore $|f^{-1}(S)| \le |X_S| < \infty$. Now let $s \in \operatorname{im}(f)$. Then, say, $f^{-1}(S) = \{x_1, \ldots, x_n\}$. Define $g_S : f^{-1}(S) \to \operatorname{im} f \times \mathbb{N}$ by $x_i \mapsto (S, i)$. Now we claim that the sets $f^{-1}(S)$ for $S \in \operatorname{im} f$ forms a partition of X. It is a relatively straightforward exercise to verify that

$$X = \bigcup_{S \in \operatorname{im} f} f^{-1}(S),$$

and if $x \in X$, there exists a unique $\{y_1, \ldots, y_n\} = S \subseteq Y$ such that $x \in \langle y_1, \ldots, y_n \rangle$.

Thus define $g : X \to \operatorname{im} f \times \mathbb{N}$ by $x \mapsto g_S(x)$ where $x \in f^{-1}(S)$. Note that g is well-defined and injective. Furthermore, $|X| \le |\operatorname{im} f| \times |\mathbb{N}| = |\operatorname{im} f| \aleph_0 = |\operatorname{im} f| \le |K(Y)| = |Y|$ (For more information, refer to Hungerford's I.8.13).

Now use the reverse argument to show that $|Y| \le |X|$, from which $|X| = |Y|$ follows. $\square$

Corollary 10.1. *Let V be a vector space over a division ring D, and X, Y two bases of V. Then $|X| = |Y|$.*

Now that we got the infinite case out of the way, we can move on to the finite basis case. Recall that we claimed that the rank of a free R-module is well-defined only when R is a division ring or a commutative ring.

Theorem 10.3. *Let V be a finite-dimensional vector space over a division ring D. Let X and Y be two bases of V. Then $|X| = |Y|$.*

Proof. Suppose that $X = \{x_1, \dots, x_n\}$ and $Y = \{y_1, \dots, y_m\}$. Without loss of generality, assume $n \le m$. Then there are $r_1, \dots, r_n \in D$ so that $y_m = r_1x_1 + \cdots + r_nx_n$. Let k be the smallest index with $r_k \neq 0$. Then

$$x_k = r_k^{-1}y_m - r_k^{-1}r_{k+1}x_{k+1} - \cdots - r_k^{-1}r_nx_n.$$

So $X_1 = \{x_1, \dots, x_{k-1}, x_{k+1}, \dots, x_n\} \cup \{y_m\}$ spans V. Now we do the same thing for y_{m-1} with X_1. Thus, we can find $a_i \in D$ and $b_m \in D$ so that

$$y_{m-1} = b_my_m + a_1x_1 + \cdots + a_{k-1}x_{k-1} + a_{k+1}x_{k+1} + \cdots + a_nx_n.$$

If all $a_i = 0$, then $y_{m-1} = b_my_m$, but this is a contradiction as Y will no longer be linearly independent. So there is a_i so that $a_i \neq 0$. Pick the smallest such index s so that $a_s \neq 0$. Using the same argument as we did on x_k, we see that $x_s \in \langle x_1, \dots, x_{k-1}, x_{k+1}, \cdots, x_{s-1}, x_{s+1}, \dots, x_n, y_m, y_{m-1}\rangle$. Hence $X \setminus \{x_s, x_k\} \cup \{y_m, y_{m-1}\}$ spans V. We can use this argument repeatedly (at each step i, throw out x_{k_i} from X, and add y_{m-i+1}) till we reach step $u = n-1$, where we have

$$X_u = X \setminus \{x_{k_1}, \dots, x_{k_{n-1}}\} \cup \{y_m, y_{m-1}, \dots, y_{m-u+1}\}$$

spans V. Hence $y_{m-u} \in \langle X_u\rangle$. This means we can throw out the last remaining x_i (specifically, x_{k_u}), so $X_u = \{y_m, \dots, y_{m-u}\}$ spans V. But this is possible only when $X_u = Y$. Hence $m - u = 1$, or $m = u + 1 = n - 1 + 1 = n$, as required. □

Definition 10.2. We say that R a ring with unity has the *invariant rank property* if for every free R-module F, any two bases have the same cardinality. In this case we call the cardinality of a basis (of F) the *rank* (or the *dimension*) of F.

Example. Any division ring has the invariant rank property. Any commutative ring has the invariant rank property.

11. February 6

Our goal in this section is to prove that the rank of a free module is well-defined if it is a module over a commutative ring with unity.

Lemma 11.1. *Let R be a ring with unity, and I a proper ideal of R. Suppose that F is a free R-module, X a basis of F, and $\Pi : F \to F/IF$ the canonical quotient map. Then F/IF is a free R/I-module with basis $\Pi(X)$ and $|\Pi(X)| = |X|$.*

Proof. If $y \in F/IF$, then evidently there is $x \in F$ such that $y = x + IF$. Let $r_1, \dots, r_n \in R$ satisfy $x = r_1x_1 + \cdots + r_nx_n$. (note that $r_1, \dots, r_n, x_1, \dots, x_n$ are unique by the linear independence of a basis). Thus $\Pi(x) = y = r_1(x_1 + IF) + \cdots + r_n(x_n + IF) = r_1\Pi(x_1) + \cdots + r_n\Pi(x_n)$. This means $\Pi(X)$ spans F/IF.

Let $\overline{r_1}\Pi(x_1) + \cdots + \overline{r_n}\Pi(x_n) = 0$ for some $r_i \in R$ and $x_i \in X$ (where $\overline{r_i} := r_i + I$). If $\Pi(r_1x_1 + \cdots + r_nx_n) = 0$, then $r_1x_1 + \cdots + r_nx_n \in IF$. Then we know there exist $y_1, \dots, y_m \in X$ and $s_1, \dots, s_m \in I$ such that

$$r_1x_1 + \cdots + r_nx_n = s_1y_1 + \cdots + s_my_m.$$

Then by the uniqueness of presentation of an element of F in terms of X, we have $m = n$ and $r_i = s_i \in I$, and $y_i = x_i$. So $r_1, \ldots, r_n \in I$, or $\overline{r_1} = \cdots = \overline{r_n} = 0$. Hence $\Pi(X)$ is linearly independent over R/I, meaning it is a basis of F/IF as an R/I-module.

As for the last part, we need to show that Π is one-to-one on X. If $\Pi(x) = \Pi(x')$, then $\Pi(x - x') = 0$. Thus $x - x' \in IF$, so $x - x' = s_1 y_1 + \cdots + s_m y_m$ for $s_i \in I$ and $y_j \in X$. By the uniqueness of presentation, indeed $m = 2$; and without loss of generality we may let $y_1 = x, y_2 = x', s_1 = 1$, and $s_2 = -1$. So $1 \in I$, so $I = R$. But this contradicts the fact that I is a proper ideal of R. Hence Π is one-to-one on X, from which $|\Pi(X)| = |X|$ follows. □

Definition 11.1. If M is an R-module, then M *has torsion* if there exist non-zero $r \in R$ and $m \in M$ such that $rm = 0$. M is said to be *torsion-free* if M has no torsion elements.

Proposition 11.1. *Suppose R is an integral domain, and M an R-module. If M is free, then M is torsion-free.*

Proof (sketch). Suppose m is a torsion-element. Then there is r such that $rm = 0$. Then there exist unique $x_1, \ldots, x_n$ basis elements and $r_1, r_2, \ldots, r_n \in R$ such that $m = r_1 x_1 + \cdots + r_n x_n$. So $rm = rr_1 x_1 + \cdots + rr_n x_n = 0$. Thus $rr_i = 0$ for all i, so $r = 0$, which contradicts the fact that r is non-zero. □

Remark 11.1. What happens if R is not an integral domain? Then there exist zero divisors in R, i.e., $r \neq 0, s \neq 0$, but $rs = 0$. Suppose that F is a free R-module with basis X, and $x \in X$. Since $s \neq 0$, indeed $sx \neq 0$. But $r(sx) = (rs)x = 0x = 0$, so we see that sx is a torsion element. So a free module may contain a torsion element in this case.

Proposition 11.2. *Suppose $f : R \to S$ is a surjective ring homomorphism (i.e., S is a homomorphic image of R) and that both R and S contain identity. If S has the invariant rank property, then R also has the invariant rank property.*

Proof. If $\ker f =: I$, then by the first isomorphism theorem, $S \cong R/I$. If F is a free R-module, and X and Y are both bases of F, we want to show that $|X| = |Y|$. But this follows from the first isomorphism theorem, Lemma 11.1, and the invariant rank property of $R/I \cong S$; therefore $|X| = |\Pi(X)| = |\Pi(Y)| = |Y|$. □

Theorem 11.1. *Every commutative ring with unity has the invariant rank property.*

Proof. R has a maximal ideal $\mathfrak{m}$ by Zorn's lemma, so $R/\mathfrak{m}$ is a field, and we have a surjective homomorphism $R \to R/\mathfrak{m}$. So by Proposition 11.2, R has the invariant rank property. Recall that $R/\mathfrak{m}$ is *a fortiori* a division ring, so $R/\mathfrak{m}$ has the invariant rank property. □

12. February 8

12.1. Dimension theory in division rings

Theorem 12.1. *Let D be a division ring, and V a vector space over D. Suppose that W is a subspace of V. Then*

(i) $\dim_D W \leq \dim_D V$.
(ii) If $\dim_D V < \infty$ *and* $\dim_D V = \dim_D W$, *then* $W = V$.
(iii) $\dim_D V = \dim_D W + \dim_D V/W$.

Proof. (i) A basis X of W can be extended to a basis Y of V. So $|X| \leq |Y|$, from which $\dim_D W \leq \dim_D V$ follows.

(ii) Let X be a basis of W, and we proved X can be extended to a basis Y of V, so $X \subseteq Y$. But then $|X| = |Y|$ so $X = Y$. Therefore $V = W$.

(iii) Pick a basis X for W and extend to a basis Y for V. So $X \subseteq Y$. Let $Z = \{y + W : y \in Y \setminus X\}$. We want to claim that Z is a basis of V/W. Clearly $Z \subseteq V/W$, and if $v + W \in V/W$ then there exist unique $y_1, \ldots, y_n \in Y$ and $a_1, \ldots, a_n \in D$ so that $v = a_1y_1 + \cdots + a_ny_n$. Then $v + W = a_1y_1 + \cdots + a_ny_n + W$. Without loss of generality, suppose $y_1, \ldots, y_s \notin X$ but $y_{s+1}, \ldots, y_n \in X$. This implies $v + W = a_1y_1 + \cdots + a_sy_s + W \in \langle Z \rangle$, so Z spans V/W.

We also need to prove linear independence. Suppose that $a_1(y_1+W)+\cdots+a_n(y_n+W) = 0$ fo some $a_1, \ldots, a_n \in D$ and $y_1 + W, \ldots, y_n + W \in Z$. Suppose that there are $b_1, \ldots, b_m \in D$ and $x_1, \ldots, x_m \in X$ such that $a_1y_1 + \cdots + a_ny_n = b_1x_1 + \cdots + b_mx_m$. But since Y is linearly independents, this forces $a_i = b_j = 0$ for all $1 \le i \le n, 1 \le j \le m$. So Z is a basis of V/W. Also $|Z| = |Y| - |X| = \dim_D V - \dim_D W$, from which the claim follows. □

Corollary 12.1. *Let V and V' be D-modules, where D is a division ring. Let $f : V \to V'$ be a linear transformation (or, equivalently, a D-module homomorphism). Then there exists a basis X of V such that $X \cap \ker f$ is a basis of* $\ker f$*, and $f(X) \setminus \{0\}$ is a basis of* $\operatorname{im} f$*. Furthermore,* $\dim_D V = \dim_D \ker f + \dim_D \operatorname{im} f$.

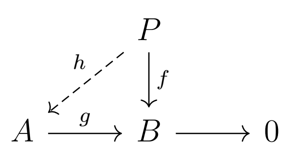
Proof. Apply the previous theorem (iii) with $W = \ker f$ which is a submodule of V. Recall that any D-module is free since D is a division ring, so W has a basis X' which can be extended to a basis X of V. Also, $V/W \cong V/\ker f \cong \operatorname{im} f$ by virtue of the first isomorphism theorem for modules. Therefore $f(X) \setminus \{0\}$ is a basis of $\operatorname{im} f$. □

Corollary 12.2. *Let V and W be vector spaces over division ring D, and that both V and W are finite-dimensional. Then* $\dim_D V + \dim_D W = \dim_D(V + W) + \dim_D(V \cap W)$.

Proof. Exercise. □

13. February 11: Projective and injective modules

Definition 13.1. A module P over a ring R is said to be *projective* if given any diagram of R-module homomorphisms whose bottom row is exact (i.e., g is an epimorphism),



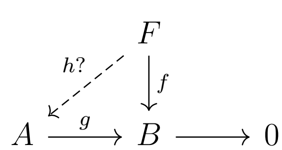
there exists an R-module homomorphism $h : P \to A$ that makes the above diagram commute ($gh = f$).

Now we shall take a look at some examples of projective modules.

Theorem 13.1. *Every free module F over a ring R* with unity *is projective.*

Remark 13.1. The theorem holds even without the unity assumption.

Proof. Consider



with the bottom row exact. Let X be a basis of F. Let $x \in X$. Since g is an epimorphism, there is $a_x \in A$ such that $g(a_x) = f(x)$. Define $h' = x \to A$ by $h'(x) = a_x$. Since F is free, the map h' induces an R-module homomorphism $h : F \to A$ defined by

$$h\left(\sum_{i=1}^{n} c_i x_i\right) = \sum_{i=1}^{n} c_i a_{x_i}.$$

Note that h is well-defined since F is free – F being free implies that $\sum c_i x_i$ is the unique representation of an element of F. Now it is not a hard exercise to check that h is a homomorphism. Now, we have $f(x) = g(a_x) = gh(x)$. By the uniqueness of presentation of elements of F (as F is free), we see that $f(u) = gh(u)$ for all $u \in F$. Therefore F is projective as required. □

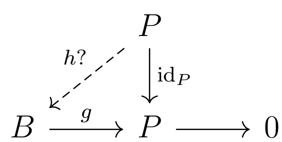
Theorem 13.2. *Let R be a ring with unity. The following conditions on an R-module P are equivalent:*

(i) P is projective.

(ii) Every short exact sequence $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} P \longrightarrow 0$ is split exact. Hence $B \cong A \oplus P$.

(iii) P is a direct summand of a free module F. In other words, $F \cong K \oplus P$ with F a free R-module and K an R-module.

Proof. ((i) ⇒ (ii)) Consider the diagram



Since P is projective, there exists an R-module homomorphism $h : P \to B$ so that $gh = \mathrm{id}_P$. Thus we have

$$0 \longrightarrow A \xrightarrow{f} B \underset{h}{\overset{g}{\rightleftarrows}} P \longrightarrow 0$$

Therefore the above sequence splits, so $B \cong A \oplus P$ as required.

((ii) ⇒ (iii)) Every R-module is a homomorphic image of a free module. So there exists a free module F such that

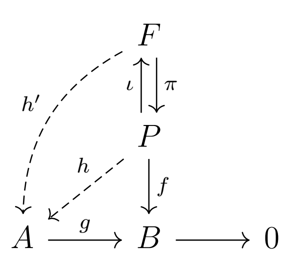
$$0 \longrightarrow \ker f \longrightarrow B \xrightarrow{f} P \longrightarrow 0$$

is exact. By hypothesis, the sequence splits so

$$F \cong \ker f \oplus P.$$

Now take $\ker f =: K$.

((iii) ⇒ (i)) Consider a diagram



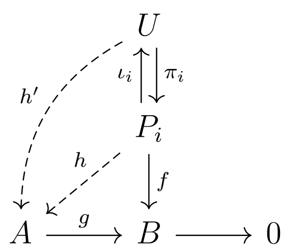
with $F \cong K \oplus P$. Since F is free, it is projective. So there exists an R-module homomorphism $h' : F \to A$ such that $gh' = f\pi$. Define $h : P \to A$ as $h = h'\iota$. Then $gh = gh'\iota = f\pi\iota = f \circ \mathrm{id}_P = f$. $\square$

Proposition 13.1. *Let R be a ring with unity, and let I be an index set . A direct sum of R-modules $\sum_{i\in I} P_i$ is projective if and only if each P_i is projective fo all $i \in I$.*

Proof. ($\Rightarrow$) Suppose that $\sum P_i$ is projective. Then

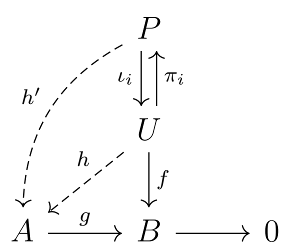
$$\underbrace{\sum_{i\in I} P_i}_{=:U} = P_i \oplus \underbrace{\sum_{\substack{j\in I\\ j\neq i}} P_j}_{=:V}$$

for a fixed $i \in I$. Now consider the diagram



Since U is projective, there exists an R-module homomorphism $h' : U \to A$ such that $gh' = f\pi_i$. Define $h : P_i \to A$ as $h = h'\iota_i$. Then $gh = gh'\iota_i = f\pi_i\iota_i = f\,\mathrm{id}_{P_i}$. So P_i is projective for all $i \in I$.

($\Leftarrow$) Suppose that P_i is projective for all $i \in I$. Consider the diagram



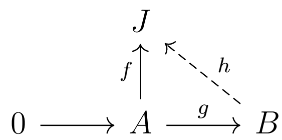
Since P_i is projective, there exists an R-module homomorphism $h'_i : P_i \to A$ such that $gh'_i = f\iota_i$. By the universal property of direct sums, there exists an R-module homomorphism $h : U \to A$ such that $h\iota_i = h'_i$. Then $gh\iota_i = gh'_i = f\iota_i$ for all $i \in I$. Therefore $gh = f$ as needed. So

$$U = \sum_{i\in I} P_i$$

is projective. $\square$

14. February 25 & 27

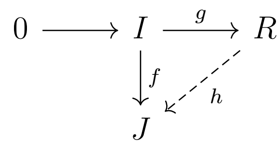
Definition 14.1. If R is a ring with identity, then an R-module J is called *injective* if for any diagram of R-modules and R-module homomorphisms



there is $h : B \to J$ such that the diagram commutes, i.e., $hg = f$.

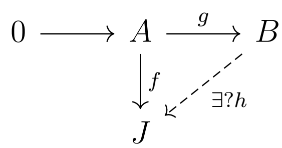
Lemma 14.1 (Baer's criterion)**.** *Suppose R is a ring with the identity, and J an R-module. Then J is injective if and only if for any left ideals I of R, any R-module homomorphism $I \to J$ can be extended to an R-module homomorphism from R to J.*

Proof. Let $f : I \to J$ and consider the diagram



which is exact. Since J is injective, there is $h : R \to J$ such that $hg = f$.

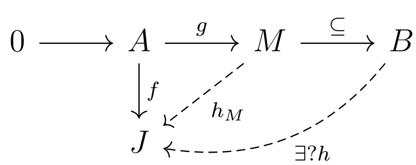
($\Leftarrow$) Suppose that we have the diagram of R-module homomorphisms



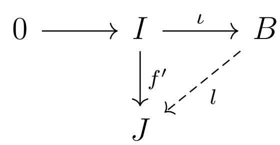
Consider the set $S := \{h_C : C \to J \mid \operatorname{im} g \subseteq C \subseteq B\}$. We claim that $S \neq \emptyset$ since $fg^{-1} : \operatorname{im} g \to J$ is in S. S is partially ordered by $\leq$ where $h_c \leq h_D \Leftrightarrow C \subseteq D$ and $h_D|_C = h_C$. Suppose that $\mathcal{C}$ is a chain in S. We shall show that $\mathcal{S}$ has an upper bound in S. Write

$$M_{\mathcal{C}} := \bigcup_{h_C \in \mathcal{C}} C.$$

Then note that $M_{\mathcal{C}}$ is a submodule of B containing $\operatorname{im} g$. $\operatorname{im} g \subseteq M_{\mathcal{C}} \subseteq B$, so we can define the homomorphism $h_{M_{\mathcal{C}}} : M_{\mathcal{C}} \to B$ defined by $h_{M_{\mathcal{C}}}(x) = h_C(x)$ when $x \in C$ and $h_C \in \mathcal{C}$. Thus $h_{M_{\mathcal{C}}} \in S$ and is an upper bound for $\mathcal{C}$. By Zorn's lemma, S has a maximal element; let this maximal element be M. So let $h_M : M \to J$.



So far, we know that there is h_M making the above diagram commute. But is it $M = B$? This is what we want. Suppose that $M \subsetneq B$. Then there is $b \in B \setminus M$. Construct $I = \{r \in R : rb \in M\}$. This is an ideal (proving this is left as an exercise); consider now $f' : I \to J$ defined by $r \mapsto h_M(rb)$. f' is a well-defined R-module homomorphism (exercise to prove that this is the case). Therefore, by assumption



there is $l : R \to J$ such that $l\iota = f'$. Now define $\overline{h} : M+Rb \to J$ where $a+rb \mapsto h_M(a)+rl(1)$. Suppose that $a, a' \in M$ and $r, r' \in R$ such that $a+rb = a'+r'b$. Then $(r'-r)b = a-a' \in M$. Thus $r-r' \in I$, so $rl(1)-r'l(1) = (r-r')l(1) = l((r-r')\cdot 1) = l(r-r') = h_M((r-r')b)$. Hence $h_M((r-r')b) = h_M(a'-a) = h_M(a')-h_M(a)$; it follows that $h_M(a)+rl(1) = h_M(a')+r'l(1)$. It is a straightforward verification to check whether $\overline{h}$ is an R-module homomorphism. This means that $\overline{h} = h_{M+Rb} \in S$, which contradicts the maximality of h_M. This forces $M = B$, so $h_M = h_B$ is indeed the homomorphism we were seeking. □

15. March 1

Definition 15.1. Let M be an R-module over domain R. If $m \in M$ and $r \in R$, we say that m is *divisible* by r if there is $m' \in M$ such that $m = rm'$. We say that M is a *divisible module* if every $m \in M$ is divisible by every non-zero $r \in R$.

Example. $\mathbb{Q}$ is divisible $\mathbb{Z}$-module. $\text{Frac}(R)$, the fraction field of R, is a divisible R-module, where R is a domain.

Proposition 15.1. *If R is a domain, and M an injective R-module, then M is divisible.*

Proof. Let $m \in M$ and $r \in R$ with $r \neq 0$; we need to find $x \in M$ such that $m = rx$. Let $f : (r) = Rr \to M$ so that $f(ar) = am$. f is well-defined since R is a domain, and f is an R-module homomorphism. Since M is injective, by Baer's criterion, there is $h : R \to M$ such that $h|_{(r)} = f$. Thus $m = f(r) = h(r) = h(r \cdot 1) = rh(1)$. Now let $x = h(1)$, so we have $m = rx$. The claim follows. □

Theorem 15.1. *Suppose R is a principal ideal domain, and M an R-module. Then M is injective if and only if M is divisible.*

Proof. ($\Leftarrow$) Suppose that M is divisible. By Baer's criterion, it suffices to show that for any ideal I of R and any $f : I \to M$ an R-module homomorphism, f can be extended to the entire R. Since R is a PID, there is a such that $I = (a)$. Since M is divisible, there is $m \in M$ such that $(a) = am \in M$. Let $h : R \to M$ be $h(r) = rm$. One can verify that h is an R-module homomorphism. If $r \in I$, then $h(r) = rm$; if $s \in R$ satisfies $r = sa$, then $h(r) = rm = sam = sf(a) = f(sa) = f(r)$. Thus h extends f, so M is injective.

($\Rightarrow$) This follows from Proposition 15.1. □

Corollary 15.1. *Let R be a PID. Suppose M an injective (hence also divisible) R-module, and N a submodule of M. Then M/N is injective (hence divisible) over R.*

Proof. If $m + N \in M/N$ and $r \neq 0 \in R$, then there exists $m' \in M$ such that $m = rm'$. Hence $m + N = rm' + N = r(m' + N)$. Therefore M/N is divisible. But then over a PID, any module is divisible if and only if it is injective, so the claim follows. $\square$

Corollary 15.2. *The homomorphic image of a divisible group (i.e., divisible $\mathbb{Z}$-module) is divisible.*

Proof. Let G' be a homomorphic image of a divisible group G. So there exists a homomorphism $\varphi : G \to G'$ such that φ is surjective. So by the first isomorphism theorem we have $G' \cong G/\ker\varphi$. $G/\ker\varphi$ is divisible by the previous corollary, so G' is also divisible. $\square$

16. March 6 & 8

Recall that if M and N are R-modules, then $\mathrm{Hom}_R(M, N)$ is the set of all R-module homomorphisms from M to N.

Proposition 16.1. *If J is a divisible abelian group, and R is a ring with identity, then $\mathrm{Hom}_{\mathbb{Z}}(R, J)$ is an injective R-module.*

Proof. We know $\mathrm{Hom}_{\mathbb{Z}}(R, J)$ is an R-module with action of R defined by $rf(x) := f(xr)$, where $r \in R$ and $f \in \mathrm{Hom}_{\mathbb{Z}}(R, J)$. Assume that I is a left ideal of R, and $f : I \to \mathrm{Hom}_{\mathbb{Z}}(R, J)$ is an R-module homomorphism. We would like to apply Baer's criterion: that is, find $\psi : R \to \mathrm{Hom}_{\mathbb{Z}}(R, J)$ such that ψ extends f.

Let $g : I \to J$ be $g(x) = f(x)(1)$. We need to verify if g is an R-module homomorphism. Let $x, y \in I$ and $r \in R$. Then $g(rx + y) = f(rx + y)(1) = (rf(x) + f(y))(1) = rf(x)(1) + f(y)(1) = rg(x) + g(y)$, as needed. So we have

$$\begin{array}{ccccc} 0 & \longrightarrow & I & \longrightarrow & R \\ & & \downarrow{\scriptstyle g} & \swarrow{\scriptstyle l} & \\ & & J & & \end{array}$$

with $0 \to I \to R$ being an exact sequence. Since J is a divisible $\mathbb{Z}$-module, so J is an injective $\mathbb{Z}$-module. Hence there exists $l : R \to J$ which is a $\mathbb{Z}$-module homomorphism such that $l|_I = g$ by Baer's criterion. Now define $h : R \to \mathrm{Hom}_{\mathbb{Z}}(R, J)$ by $r \mapsto h(r) : R \to J$, where $h(r)$ maps x to $l(xr)$.

(1) We need to verify if $h(r)$ is a group homomorphism for any $r \in R$. For any $x, y \in R$ we have

$$\begin{aligned} h(r)(x + y) &= l((x + y)r) \\ &= l(xr + yr) \\ &= l(xr) + l(yr) \quad \text{(because } l \text{ is a group homomorphism)} \\ &= h(r)(x) + h(r)(y). \end{aligned}$$

(2) h is well-defined. Let $r = r'$ where $r, r' \in R$. Then for any $x \in R$ we have $h(r)(x) = l(xr)$ and $h(r')(x) = l(xr')$. If $r = r'$ in R, then $xr = xr'$ in R, so $l(xr) = l(xr')$. Hence $h(r)(x) = h(r')(x)$, so h is well-defined.

(3) h is an R-module homomorphism. Consider $h(rx+y) : R \to J$. For any $u \in R$,

$$\begin{aligned} h(rx+y)(u) &= l(u(rx+y)) = l(urx+uy) \\ &= l(urx) + l(uy) \quad (\because l \text{ is a group homomorphism}) \\ &= h(x)(ur) + h(y)(u) = (rh(x))(u) + h(y)(u) \\ &= (rh(x) + h(y))(u), \end{aligned}$$

as required.

(4) Finally, we need $h|_I = f$. Suppose $r \in I$. Then $h(r) : R \to J$ maps $x \mapsto l(xr)$. But $xr \in I$ since I is a left ideal. Therefore

$$\begin{aligned} l(xr) = g(xr) &= f(xr)(1) \\ &= xf(r)(1) \\ &= f(r)(1 \cdot x) \quad (\text{since } f \text{ is an } R\text{-module homomorphism}) \\ &= f(r)(x). \end{aligned}$$

Therefore for any $r \in I$, we have $h(r)(x) = f(r)(x)$. Hence $h = f$ whenever $r \in I$, so $h|_I = f$ as desired. □

We want to prove that if R is a ring with identity and M an R-module, then $M \subseteq J$ for some injective R-module J.

First we want to prove this for the case $R = \mathbb{Z}$.

Lemma 16.1. *Every abelian group can be embedded in a divisible abelian group.*

Proof. Let G be an abelian group. Then G is a $\mathbb{Z}$-module, so there exists free $\mathbb{Z}$-module $F = \bigoplus \mathbb{Z}$ and an epimorphism $f : F \to G$. The first isomorphism theorem implies $G \cong F/\ker f$. Observe that $F = \bigoplus \mathbb{Z} \hookrightarrow D = \bigoplus \mathbb{Q}$. D is divisible since $\mathbb{Q}$ is divisible as a $\mathbb{Z}$-module. $\mathbb{Z}$ is a PID, so $\mathbb{Q}$ is injective as well as a $\mathbb{Z}$-module; any direct sum of injective modules is injective, so $\bigoplus \mathbb{Q} = D$ is injective as a $\mathbb{Z}$-module.

If h is the injection from F to D, then $F \cong h(F)$. Thus, $G \cong F/\ker f \cong h(F)/h(\ker f) \subseteq D/h(\ker f)$. So G is embedded in an injective $\mathbb{Z}$-module; note that any quotient of a divisible module is also divisible, making $D/h(\ker f)$ divisible also. □

Theorem 16.1. *Let R be a ring with identity, and M an R-module. Then M can be embedded into an injective R-module.*

Proof. Let M be an abelian group. By the previous lemma there exists a divisible group J (injective $\mathbb{Z}$-module) such that $f : M \hookrightarrow J$ is a group monomorphism. We want to build $\overline{f} : \operatorname{Hom}_{\mathbb{Z}}(R, M) \to \operatorname{Hom}_{\mathbb{Z}}(R, J)$ mapping $g \mapsto fg$. Previously, we showed that $\operatorname{Hom}_{\mathbb{Z}}(R, J)$ is an injective R-module. We will show that M can be embedded here.

We claim that $\overline{f}$ is an R-module homomorphism. That is, if $a \in R$ and $g_1, g_2 \in \operatorname{Hom}_{\mathbb{Z}}(R, M)$, then $\overline{f}(ag_1 + g_2) = f(ag_1 + g_2) = f(ag_1) + f(g_2)$ as f is a group homomorphism. Observe that for any $r \in R$,

$$f(ag_1)(r) = f((ag_1)(r)) = f(g_1(ra)) = fg_1(ra) = afg_1(r).$$

Therefore

$$\overline{f}(ag_1 + g_2) = f(ag_1) + f(g_2) = afg_1 + fg_2,$$

as required.

Now that we showed $\overline{f}$ is an R-module homomorphism, we now need to show that $\overline{f}$ is injective. Suppose $\overline{f}(g) = 0$. Then $fg = 0$, so in particular $fg(1) = 0$. Therefore $f(g(1)) = 0$; but since f is injective, we have $g(1) = 0$. Thus $g \equiv 0$ as desired. Thus $\overline{f}$ is an R-module monomorphism as needed, so $\operatorname{Hom}_R(R, M)$ is a submodule of $\operatorname{Hom}_{\mathbb{Z}}(R, M)$.

Let $\varphi : M \to \operatorname{Hom}_R(R, M)$ be $m \mapsto f_m$ where $f_m : R \to M$ maps r to rm. Then φ is an R-module monomorphism. Indeed, if $\varphi(m) = 0$, then $f_m(r) = 0$ for all $r \in R$, which implies $f_m(1) = 0$. Therefore $1m = m = 0$, as needed.

Now we have a chain of injections

$$M \overset{\varphi}{\hookrightarrow} \operatorname{Hom}_R(R, M) \overset{i}{\hookrightarrow} \operatorname{Hom}_{\mathbb{Z}}(R, M) \overset{\overline{f}}{\hookrightarrow} \operatorname{Hom}_{\mathbb{Z}}(R, J).$$

But then we previously proved that $\operatorname{Hom}_{\mathbb{Z}}(R, J)$ is injective, so M is embedded in an injective R-module as desired. $\square$

Theorem 16.2. *Let R be a ring with identity, and J an R-module. Then the following are equivalent:*

(i) J is injective.
(ii) Every short exact sequence $0 \to J \to B \to C \to 0$ is split exact. In particular, $B \cong J \oplus C$.
(iii) If J is a submodule of B, then J is a direct summand of B.

Proof. ((i) $\Rightarrow$ (ii)) This works similarly to the projective case. Indeed,

$$\begin{array}{ccccccccc} 0 & \longrightarrow & J & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & {\scriptstyle \mathrm{id}}\downarrow & \swarrow{\scriptstyle \exists h} & & & & & \\ & & J & & & & & & \end{array}$$

Since J is injective, there is h such that $hf = \mathrm{id}_J$. By definition this is a split exact sequence, so indeed $B \cong J \oplus C$.

((ii) $\Rightarrow$ (iii)) The exact sequence

$$0 \longrightarrow J \longrightarrow B \longrightarrow B/J \longrightarrow 0$$

is split exact by (ii), so $B \cong J \oplus B/J$.

((iii) $\Rightarrow$ (i)) By the previous theorem, $J \subseteq J'$ where J' is an injective R-module. By (iii) J is a direct summand of an injective module, so J is injective. Recall that a direct product of R-modules $\prod_{i \in I} J_i$ is injective if and only if J_i is injective for each $i \in I$. $\square$

17. March 11, 13 & 15

Recall that if A and B are R-modules then

$$\operatorname{Hom}_R(A, B) = \{f : A \to B : f \text{ is a } R\text{-module homomorphism}\}.$$

Theorem 17.1. *Let $\varphi : C \to A$ and $\psi : B \to D$ be R-module homomorphisms where R is a ring. Then*

$$\theta : \operatorname{Hom}_R(A, B) \to \operatorname{Hom}_R(C, D)$$

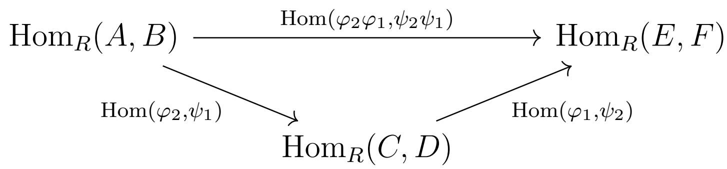
mapping $f \mapsto \psi f \varphi$ is a group homomorphism.

Proof. Note that θ is well-defined since it is just a composition of functions ($C \xrightarrow{\varphi} A \xrightarrow{f} B \xrightarrow{\psi} D$). θ is additive: for any $f, g \in \operatorname{Hom}_R(A, B)$, we have $\theta(f+g) = \psi(f+g)\varphi = \psi f \varphi + \psi g \varphi = \theta(f) + \theta(g)$. $\square$

Definition 17.1. We shall denote the θ in Theorem 17.1 by $\operatorname{Hom}(\varphi, \psi)$, and call it the *homomorphism induced by φ and ψ.*

Note that $\varphi_1 : E \to C, \varphi_2 : C \to A, \psi_1 : B \to D, \psi_2 : D \to F$. Then

$$\operatorname{Hom}(\varphi_1, \psi_2) \operatorname{Hom}(\varphi_2, \psi_1) = \operatorname{Hom}(\varphi_2\varphi_1, \psi_2\psi_1).$$



Proposition 17.1. *The following are equivalent:*

(a) $0 \longrightarrow A \xrightarrow{\varphi} B \xrightarrow{\psi} C$ *is an exact sequence of R-modules.*

(b) For every R-module D, $0 \longrightarrow \operatorname{Hom}_R(D, A) \xrightarrow{\overline{\varphi}} \operatorname{Hom}_R(D, B) \xrightarrow{\overline{\psi}} \operatorname{Hom}_R(D, C)$ *is an exact sequence of abelian groups, where* $\overline{\varphi} : f \mapsto \varphi f$ *and* $\overline{\psi} : g \mapsto \psi g$.

Proof. ($\Leftarrow$) Suppose $D = \ker \varphi$, and suppose $\iota : D \hookrightarrow A$ be the inclusion map. Note that $\iota \in \operatorname{Hom}_R(D, A)$. $\overline{\varphi}(\iota) = \varphi\iota = 0$: if $x \in D = \ker \varphi$, then $\varphi(\iota x) = \varphi(x) = 0$. Thus $\iota \in \ker \overline{\varphi}$; but since $\overline{\varphi}$ is injective by exactness, we have $\iota = 0$. Hence $D = \ker \varphi = 0$, so φ is injective.

Now pick $D = A$. Then $\operatorname{im} \overline{\varphi} = \ker \overline{\psi}$. So $\overline{\psi}\overline{\varphi}(\operatorname{id}_A) = 0$. So $\psi\varphi \operatorname{id}_A = 0$, hence $\psi\varphi = 0$. Therefore $\operatorname{im} \varphi \subseteq \ker \psi$.

For the other inclusion, we shall pick $D = \ker \psi$, and let $\iota : D \hookrightarrow B$. Indeed, $\overline{\psi}(\iota) = \psi\iota = 0$. Hence $\iota \in \ker \overline{\psi} = \operatorname{im} \overline{\varphi}$. Thus there exists $f \in \operatorname{Hom}_R(\ker \psi, A)$ so that $\iota = \overline{\varphi}(f)$. Hence $\iota(x) = \varphi(f(x)) \in \operatorname{im} \varphi$, so $\ker \psi \subseteq \operatorname{im} \varphi$. So $\ker \psi = \operatorname{im} \varphi$ as desired, thereby completing the proof.

($\Rightarrow$) Let D be an R-module. Suppose $f \in \ker \overline{\varphi}$. Then $\overline{\varphi}(f) = 0$. So $\varphi f = 0$. Hence for all $d \in D$ we have $\varphi(f(d)) = 0$. But φ is injective, so $f(d) = 0$ for all $d \in D$ which gives $f = 0$. Therefore $\overline{\varphi}$ is injective.

We still need to prove that $\operatorname{im} \overline{\varphi} = \ker \overline{\psi}$. Let $f \in \operatorname{im}(\overline{\varphi})$. Then $f = \varphi(g)$ for some $g \in \operatorname{Hom}_R(D, A)$. Thus $f(d) = \varphi g(d) = \varphi(g(d)) \in \operatorname{im} \varphi = \ker \varphi$. Hence $\overline{\psi}(f) = 0$ so $f \in \ker \overline{\psi}$. Hence $\operatorname{im} \overline{\varphi} \subseteq \ker \overline{\psi}$. Conversely, let $f \in \ker \overline{\psi}$. Then $\overline{\psi}(f) = \psi f = 0$. Therefore for all $d \in D$ we have $\psi f(d) = 0 = \psi(f(d))$. Thus $\operatorname{im} f \subseteq \ker \psi = \operatorname{im} \varphi$. φ is injective, so $\varphi : A \to \operatorname{im} \varphi$ is an isomorphism, by the first isomorphism theorem. Now we shall construct $h : D \xrightarrow{f} \operatorname{im} f \hookrightarrow \operatorname{im} \varphi \xrightarrow{\varphi^{-1}} A$ where $f \in \operatorname{Hom}_R(D, B)$. Then $h \in \operatorname{Hom}_R(D, A)$. Moreover, $f = \varphi h = \overline{\varphi}(h)$ by construction, so $f \in \operatorname{im} \overline{\varphi}$. Hence $\ker \overline{\psi} \subseteq \operatorname{im} \overline{\varphi}$, so indeed $\ker \overline{\psi} = \operatorname{im} \overline{\varphi}$, as needed. $\square$

We can prove the analogous result for $\operatorname{Hom}_R(\cdot, D)$ using a similar reasoning.

Theorem 17.2. *Let R be a ring. Then* $A \xrightarrow{\varphi} B \xrightarrow{\psi} C \to 0$ *is an exact sequence of R-modules if and only if* $0 \to \operatorname{Hom}_R(C, D) \xrightarrow{\overline{\psi}} \operatorname{Hom}_R(B, D) \xrightarrow{\overline{\varphi}} \operatorname{Hom}_R(A, D)$ *is an exact sequence of $\mathbb{Z}$-modules.*

In summary, $\mathrm{Hom}_R(D,\cdot)$ preserves left-exactness and the arrows; on the other hand, $\mathrm{Hom}_R(\cdot,D)$ flips arrows, and changes right-exactness to left-exactness.

Now we shall discuss some cases in which Hom is also right-exact.

Theorem 17.3. *Let R be a ring. Then the following are equivalent.*

(i) $0 \to A \overset{\varphi}{\to} B \overset{\psi}{\to} C \to 0$ *is a split exact sequence of R-modules*

(ii) $0 \to \mathrm{Hom}_R(D,A) \overset{\overline{\varphi}}{\to} \mathrm{Hom}_R(D,B) \overset{\overline{\psi}}{\to} \mathrm{Hom}_R(D,C) \to 0$ *is a split exact sequence of $\mathbb{Z}$-modules for every R-module D.*

(iii) $0 \to \mathrm{Hom}_R(C,D) \overset{\overline{\psi}}{\to} \mathrm{Hom}_R(B,D) \overset{\overline{\varphi}}{\to} \mathrm{Hom}_R(A,D) \to 0$ *is a split exact sequence of $\mathbb{Z}$-modules for every R-module D.*

Proof. ((i) ⇒ (iii)) $0 \to A \to B \to C \to 0$ is split exact, so there are $\psi_1 : C \to B$ such that $\psi\psi_1 = \mathrm{id}_C$. Consider $\overline{\psi_1} : \mathrm{Hom}_R(B,D) \to \mathrm{Hom}_R(C,D)$ defined the usual way ($f \mapsto f\psi_1$). Note that $\overline{\psi_1}\overline{\psi}f = \overline{\psi_1}(\overline{\psi}f) = \overline{\psi_1}(f\psi) = f\psi\psi_1 = f$ where $f \in \mathrm{Hom}_R(C,D)$. So the left-exactness of $\mathrm{Hom}_R(\cdot,D)$ gives us exactness everywhere but at $\overline{\varphi}$.

Now we need to show that $\overline{\varphi}$ is surjective. We already know that there is $\varphi_1 : B \to A$ such that $\varphi_1\varphi = \mathrm{id}_A$. Let $\overline{\varphi_1} : \mathrm{Hom}_R(A,D) \to \mathrm{Hom}_R(B,D)$ be the usual map, i.e., $f \mapsto f\varphi_1$. Observe that $\overline{\varphi}\overline{\varphi_1} = \mathrm{id}_{\mathrm{Hom}_R(A,D)}$. Therefore $\overline{\varphi}$ is surjective. Indeed, if $f \in \mathrm{Hom}_R(A,D)$, then $\overline{\varphi}\overline{\varphi_1}(f) = \overline{\varphi}(\overline{\varphi_1}(f)) = f$, so $f \in \mathrm{im}\,\overline{\varphi}$.

The remaining directions are left as exercises. □

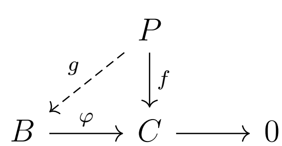
Theorem 17.4. *Let R be a ring, and let P be an R-module. The following are equivalent.*

(i) *P is projective.*

(ii) *If* $B \overset{\varphi}{\to} C \to 0$ *is an exact sequence of R-modules, then* $\mathrm{Hom}_R(P,B) \overset{\overline{\varphi}}{\to} \mathrm{Hom}_R(P,C) \to 0$ *is an exact sequence of $\mathbb{Z}$-modules.*

(iii) *If* $0 \to A \overset{\varphi}{\to} B \overset{\psi}{\to} C \to 0$ *is a short exact sequence of R-modules, then* $0 \to \mathrm{Hom}_R(P,A) \overset{\overline{\varphi}}{\to} \mathrm{Hom}_R(P,B) \overset{\overline{\psi}}{\to} \mathrm{Hom}_R(P,C) \to 0$ *is a short exact sequence of $\mathbb{Z}$-modules.*

Proof. ((i) ⇒ (ii)) Suppose $B \overset{\varphi}{\to} C \to 0$ is exact, and let $f \in \mathrm{Hom}_R(P,C)$. Since P is projective ,there is $g \in \mathrm{Hom}_R(P,B)$ such that $\varphi g = f$.



Thus for any f there is g such that $\overline{\varphi}(g) = f$, which shows that $\overline{\varphi}$ is surjective.

((ii) ⇒ (i)) Consider an exact sequence $B \overset{\varphi}{\to} C \to 0$ with surjective φ, and let $f : P \to C$ be an R-module homomorphism. But since $\overline{\varphi}$ is surjective, there is $g : P \to B$ such that $\overline{\varphi}(g) = f$. Hence $\varphi g = f$, so P is projective (see the commutative diagram above).

((ii) ⇒ (iii)) Suppose $0 \to A \overset{\varphi}{\to} B \overset{\psi}{\to} C \to 0$ is a short exact sequence. Then we know

$$0 \to \mathrm{Hom}_R(P,A) \overset{\overline{\varphi}}{\to} \mathrm{Hom}_R(P,B) \overset{\overline{\psi}}{\to} \mathrm{Hom}_R(P,C) \to 0$$

is exact for the first three arrows by the left exactness of Hom. The fourth arrow is also straightforward due to (ii).

((iii) ⇒ (ii)) Given $B \xrightarrow{\varphi} C \to 0$, we can build a short exact sequence $0 \to \ker\varphi \to B \to C \to 0$. By (iii),

$$0 \to \mathrm{Hom}_R(P, A) \xrightarrow{\overline{\varphi}} \mathrm{Hom}_R(P, B) \xrightarrow{\overline{\psi}} \mathrm{Hom}_R(P, C) \to 0$$

is exact, so hence $\mathrm{Hom}_R(P, B) \xrightarrow{\overline{\psi}} \mathrm{Hom}_R(P, C) \to 0$ is exact. □

The next theorem proves the injective counterpart.

Theorem 17.5. *Let R be a ring, and let J be an R-module. The following are equivalent.*

(i) J is injective.

(ii) If $0 \to A \xrightarrow{\varphi} B$ is an exact sequence of R-modules, then $\mathrm{Hom}_R(B, J) \xrightarrow{\overline{\varphi}} \mathrm{Hom}_R(A, J) \to 0$ is an exact sequence of $\mathbb{Z}$-modules.

(iii) If $0 \to A \xrightarrow{\varphi} B \xrightarrow{\psi} C \to 0$ is a short exact sequence of R-modules, then $0 \to \mathrm{Hom}_R(C, J) \xrightarrow{\overline{\psi}} \mathrm{Hom}_R(B, J) \xrightarrow{\overline{\varphi}} \mathrm{Hom}_R(A, J) \to 0$ is a short exact sequence of $\mathbb{Z}$-modules.

Proof. Similar to the projective case. □

18. March 18 & 20

Definition 18.1. Let M_R be a right R-module, and ${}_RN$ a left R-module, and let F be the free $\mathbb{Z}$-module on the set $M \times N$. That is, F has a basis $\{e_{(m,n)} : (m, n) \in M \times N\}$. For the simplicity of notation, write $(m, n) := e_{(m,n)}$. Then the *tensor product* of M and N is defined as the $\mathbb{Z}$-module

$$M \otimes_R N := F/Z,$$

where Z is the subgroup of F generated by the set

$$K := \{(m + m', n) - (m, n) - (m', n), (m, n + n') - (m, n) - (m, n'), \\ (mr, n) - (m, rn) \mid m, m' \in M, n, n' \in N, r \in R\}$$

For any $m \in M$ and $n \in N$, $m \otimes n := (m, n) + Z$.

Proposition 18.1 ("The three rules")**.** *Definition of tensor product implies the following properties:*

(i) $(m + m') \otimes n = m \otimes n + m' \otimes n$

(ii) $m \otimes (n + n') = m \otimes n + m \otimes n'$

(iii) $r(m \otimes n) = mr \otimes n = m \otimes rn$

Corollary 18.1. $m \otimes 0 = 0 \otimes n = 0$.

We shall see that $M \otimes_R N$ is a $\mathbb{Z}$-module for any ring R. If R is commutative, we will see that $M \otimes_R N$ is not just an abelian group, but is an R-module. We shall also see that $M \otimes_R N$ is generated by $\{m \otimes n : m \in M, n \in N\}$. Thus any typical element of $M \otimes_R N$ is of the form

$$\sum_{i=1}^{h} m_i \otimes n_i$$

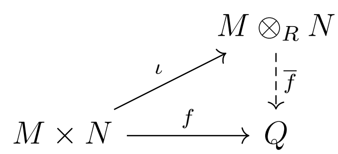
where $m_1, \ldots, m_h \in M, n_1, \ldots, n_h \in N$, and $h \in \mathbb{N}$.

Definition 18.2. Let M_R and ${}_RN$ be right and left R-modules respectively, and let Q be an abelian group. Then a function $f : M \times N \to Q$ is said to be *middle-linear* if for all $m, m' \in M, n, n' \in N$, and $r \in R$, f satisfies the following three conditions.

(i) $f(m + m', n) = f(m, n) + f(m', n)$
(ii) $f(m, n + n') = f(m, n) + f(m, n')$
(iii) $f(mr, n) = f(m, rn)$

In particular, the middle-linear map $\iota : M \times N \to M \otimes_R N$ defined by $\iota(m, n) = m \otimes n$ is said to be the *canonical middle-linear map.*

Proposition 18.2 (Universal property of tensor products)**.** *Let M_R be a right R-module and ${}_RN$ a left R-module; let Q be an abelian group. If $f : M \times N \to Q$ is a middle-linear map, then there exists a* unique *group homomorphism $\overline{f} : M \otimes_R N : Q$ such that the diagram below commutes.*

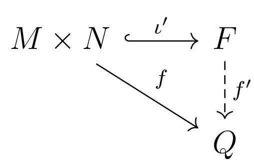


i.e., $f = \overline{f}\iota$. Moreover, $M \otimes_R N$ is the unique *abelian group with this property.*

Proof. As before, let F be a free $\mathbb{Z}$-module with on $M \times N$, and let

$$K := \langle (m + m', n) - (m, n) - (m', n), (m, n + n') - (m, n) - (m, n'),$$
$$(mr, n) - (m, rn) \mid m, m' \in M, n, n' \in N, r \in R \rangle.$$

Then $M \otimes_R N = F/K$ by definition. By the universal property of free modules, for the function $f : M \times N \to Q$, there exists a unique abelian group homomorphism $f' : F \to Q$ such that $f'\iota' = f$.



Now if $m, m' \in M, n, n' \in N$ and $r \in R$, we have $f'((m + m', n) - (m, n) - (m', n)) = 0$. Similarly, $f'(\alpha) = 0$ for all $\alpha \in K$. Hence $K \subseteq \ker f'$. Therefore f' induces an abelian group homomorphism $\overline{f} : F/K \to Q$ such that $\overline{f}(m \otimes n) = f'((m, n)) = f(m, n)$.

Suppose that g is another group homomorphism $g : M \otimes_R N \to Q$ such that $g\iota = f$. Then for any $(m, n) \in M \times N$, $g(m \otimes n) = g\iota(m, n) = f(m, n) = \overline{f}\iota(m, n) = \overline{f}(m \otimes n)$. Hence $g = \overline{f}$, which proves the uniqueness of $\overline{f}$. Finally, the uniqueness of $M \otimes_R N$ comes from the uniqueness of universal objects in categories. □

Definition 18.3. Suppose that R is a commutative ring, and A, B, C R-modules (note that since R is commutative, every module is is both a left R-module and a right R-module). A *bilinear map* $f : A \times B \to C$ is a function satisfying the following three conditions for all $a, a' \in A, b, b' \in B, r \in R$.

(i) $f(a + a', b) = f(a, b) + f(a', b)$
(ii) $f(a, b + b') = f(a, b) + f(a, b')$
(iii) $f(ra, b) = rf(a, b) = f(a, rb)$

Remark 18.1. The (iii) from the above definition gives us the R-module structure on $M \otimes_R N$ when R is commutative.

Remark 18.2. When A and B are R-modules for a commutative ring R, then $A \otimes_R B$ is an R-module, and the canonical middle-linear map $\iota : A \times B \to A \otimes_R B$ is in fact bilinear.

Recall that if R is a commutative ring, then M, N are left R-modules, then $M \otimes_R N$ is a left R-module with action on R defined as $r(m \otimes n) = rm \otimes n = mr \otimes n = m \otimes rn$ for $r \in R, m \in M, n \in N$.

Example. We claim that $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z} = 0$. Indeed, suppose that $a = 3a \in \mathbb{Z}/2\mathbb{Z}$ and $b \in \mathbb{Z}/3\mathbb{Z}$. Then $a \otimes b = 3a \otimes b = 3(a \otimes b) = a \otimes 3b = a \otimes 0 = a \otimes 0 = 0$.

The above example shows that the value of $x \otimes y$ depends very much on where x and y live. We present another example which illustrates this point.

Example. We will see what $2 \otimes 1$ is in $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$. We have $2 \otimes 1 = 2(1 \otimes 1) = 1 \otimes 2 = 1 \otimes 0 = 0$. But on the other hand, in $2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$, we have $2 \otimes 1 \neq 0$.

Proposition 18.3. *Let R be a commutative ring, and let M, M', N, N' R-modules. Suppose that $f : M \to M'$ and $g : N \to N'$ are R-module homomorphisms. Then there exists a unique R-module homomorphism $f \otimes g : M \otimes_R N \to M' \otimes_R N'$ where $(f \otimes g)(m \otimes n) := f(m) \otimes g(n)$.*

Proof. Define $h : M \times N \to M' \otimes_R N'$ by $h(m, n) = f(m) \oplus g(n)$. We need to show that h is well-defined, but this is straightforward since f and g are. We also need to show that h is bilinear. Let $m, m' \in M, n, n' \in N$, and $r \in R$.

$$\begin{aligned} h(m + m', n) &= f(m + m') \otimes g(n) = (f(m) + f(m')) \otimes g(n) \\ &= f(m) \otimes g(n) + f(m') \otimes g(n) = h(m, n) + h(m', n) \\ h(m, n + n') &= f(m) \otimes g(n + n') = f(m) \otimes (g(n) + g(n)') \\ &= f(m) \otimes g(n) + f(m) \otimes g(n') = h(m, n) + h(m, n') \\ h(rm, n) &= f(rm) \otimes g(n) = rf(m) \otimes g(n) = r(f(m) \otimes g(n)) = rh(m, n) \\ h(m, rn) &= f(m) \otimes g(rn) = f(m) \otimes rg(n) = r(f(m) \otimes g(n)) = rh(m, n). \end{aligned}$$

Hence h is bilinear map from $M \times N$ to $M' \otimes N'$. By the universality of tensor products, h extends to unique R-module homomorphism. ☐

Proposition 18.4 (Right-exactness of tensor)**.** *Suppose R is a commutative ring. Let $M \xrightarrow{f} N \xrightarrow{g} K \longrightarrow 0$ be an exact sequence of left R-modules. If D is any right R-module, then*

$$D \otimes_R M \xrightarrow{\mathrm{id}_D \otimes f} D \otimes_R N \xrightarrow{\mathrm{id}_D \otimes g} D \otimes_R K \longrightarrow 0$$

is also an exact sequence of R-modules.

Proof. We will prove it the direct way. First, we claim that $\mathrm{id}_D \otimes g$ is surjective. Note that $D \otimes_R K$ is generated by elements of the form $d \otimes k$, where $d \in D$ and $k \in K$. Since g is surjective, there exists $n \in N$ such that $g(n) = k$. Hence $d \otimes k = (\mathrm{id}_D \otimes g)(d \otimes n)$. Second, we need $\mathrm{im}(\mathrm{id}_D \otimes f) = \ker(\mathrm{id}_D \otimes g)$. $\mathrm{im}(\mathrm{id}_D \otimes f)$ is generated by $d \otimes n$ where $d \in D$ and $n \in \mathrm{im}\, f = \ker g$. Thus $(\mathrm{id}_D \otimes g)(d \otimes n) = d \otimes g(n) = d \otimes 0 = 0$. Hence $d \otimes n \in \ker(\mathrm{id}_D \otimes g)$. To prove the reverse inclusion, consider the canonical quotient map

$\pi : D \otimes_R N \to D \otimes_R N/\operatorname{im}(\mathrm{id}_D \otimes f)$. Since $\operatorname{im}(\mathrm{id}_D \otimes f) \subseteq \ker(\mathrm{id}_D \otimes g)$, there is a unique R-module homomorphism

$$\varphi : (D \otimes_R N)/\operatorname{im}(\mathrm{id}_D \otimes f) \to D \otimes_R K.$$

We show that φ is an isomorphism, which will show that $\ker(\mathrm{id}_D \otimes g) = \operatorname{im}(\mathrm{id}_D \otimes f)$. To do this we shall show that φ has an inverse, by showing that there is a bilinear map $\psi : D \times K \to (D \otimes N)/\operatorname{im}(\mathrm{id}_D \otimes f)$ defined by $(d, k) \mapsto d \otimes n + \operatorname{im}(1_D \otimes f)$ where $n \in N$ is such that $g(n) = k$. We show that ψ is well-defined bilinear map. Suppose that $n, n' \in N$ such that $g(n) = g(n') = k$. Then $\psi(d, k) = d \otimes n + \operatorname{im}(\mathrm{id}_D \otimes f)$ but also $\psi(d, k) = d \otimes n' + \operatorname{im}(\mathrm{id}_D \otimes f)$. Observe that $d \otimes n - d \otimes n' = d \otimes (n - n') \in \operatorname{im}(\mathrm{id}_D \otimes f)$. But then $g(n) = g(n') = k$, so $g(n - n') = 0$. Thus $n - n' \in \ker g = \operatorname{im} f$, so ψ is well-defined. Proving bilinearity is straightforward, so this will be left as an exercise. So by the universality of tensor, there exists $\overline{\psi} : D \otimes_R K \to (D \otimes_R N)/\operatorname{im}(\mathrm{id}_D \otimes f)$. Finally, observe $\psi\overline{\psi} = \overline{\psi}\psi = \mathrm{id}$, thereby proving that ψ is an isomorphism as desired. □

Remark 18.3. The above statement can also be proved using the exactness of Hom and the observation that $\operatorname{Hom}(M \otimes_R N, P) \cong \operatorname{Hom}(M, \operatorname{Hom}(N, P))$.

19. March 25

Definition 19.1. A *functor* F is a function from a caterogy to another category preserving morphisms. F is *covariant* if $F(f) : F(A) \to F(B)$ for $f : A \to B$. F is *contravariant* if $F(f) : B \to A$ where $f : A \to B$. F is *exact* if F takes short exact sequences to short exact sequences.

Example. Let R be a commutative ring, and D an R-module. Then $\operatorname{Hom}_R(D, \cdot)$ is a covariant functor which is exact if and only if D is projective. Similarly, $\operatorname{Hom}_R(\cdot, D)$ is a contravariant functor which is exact if and only if D is injective. The functor $\cdot \otimes_R D$ is a covariant functor which is exact if and only if D is a flat module.

Corollary 19.1. *Let R be a commutative ring, and M, M', N, N' all left R-modules. Also, let $f : M \to M'$ and $g : N \to N'$ surjective homomorphisms. Then $f \otimes g : M \otimes_R N \to M' \otimes_R N'$ is a surjective homomorphism of R-modules.*

Proof. Applying the functor $M \otimes_R \cdot$, we see that

$$M \otimes_R N \stackrel{\mathrm{id}_M \otimes g}{\longrightarrow} M \otimes_R N' \longrightarrow 0$$

is exact. Similarly, we can apply the functor $\cdot \otimes_R N'$ gives

$$M \otimes_R N' \stackrel{f \otimes \mathrm{id}_{N'}}{\longrightarrow} M' \otimes_R N' \longrightarrow 0$$

is exact. Note that if $m \in M$ and $n \in N$, then $(f \otimes g)(m \otimes n) = f(m) \otimes g(n) = (f \otimes \mathrm{id}_{N'})(m \otimes g(n))$. Therefore $f \otimes g = (f \otimes \mathrm{id}_{N'}) \circ (\mathrm{id}_M \otimes g) : M \otimes N \to M' \otimes N'$. Hence $f \otimes g$ is surjective since other two are. □

Theorem 19.1. *Let R be a commutative ring with unity. Suppose that A is a right R-module and B a left R-module. Then $A \otimes_R R \cong A$ and $R \otimes_R B \cong B$.*

Proof. Define $f : R \times B \to B$ by $f(r, b) = rb$. We show that f is bilinear.

$$f(r + r', b) = (r + r')b = rb + r'b = f(r, b) + f(r', b)$$

$$f(r, b+b') = r(b+b') = rb + rb' = f(r,b) + f(r,b')$$
$$f(sr, b) = (sr)b = s(rb) = sf(r,b) = (rs)b = r(sb) = f(r, sb).$$

By the universal property of tensor product, there is a R-module homomorphism $\overline{f} : R \otimes_R B \to B$ defined by $r \otimes b \mapsto rb$. We just need to show that $\overline{f}$ is bijective. f is surjective since for any $b \in B$, we have $b = 1 \cdot b = \overline{f}(1 \otimes b)$. As for injectivity, suppose that

$$\overline{f}\left(\sum_{i=1}^{n} r_i \otimes b_i\right) = 0$$

where $r_1, \ldots, r_n \in R$ and $b_1, \ldots, b_n \in B$. Then

$$\sum_{i=1}^{n} r_i b_i = 0$$

in B. Thus,

$$\sum_{i=1}^{n} r_i \otimes b_i = \sum_{i=1}^{n} r_i(1 \otimes b_i) = \sum_{i=1}^{n}(1 \otimes r_i b_i) = 1 \otimes \left(\sum_{i=1}^{n} r_i b_i\right) = 1 \otimes 0 = 0.$$

Thus $\overline{f}$ is an R-module isomorphism as required. □

20. March 27: Modules over principal ideal domains

Definition 20.1. Let R be a ring, and M a left R-module. M is a *Noetherian module* if M satisfies the ascending chain condition (ACC) of submodules, i.e., for any chain of submodules $M_1 \subseteq M_2 \subseteq \cdots \subseteq M_k \subseteq M_{k+1} \subseteq \cdots$, there exists N such that $M_n = M_{n+1} = \cdots$ for all $n \geq N$. Therefore every ascending chain of submodules stabilizes. In particular, R is a *Noetherian ring* if it satisfies the ascending chain condition on its ideals.

Theorem 20.1. *If R is a ring, and M a left R-module, then the following are equivalent.*

(1) M is Noetherian.
(2) Every non-empty set of submodules of M contains a maximal element under inclusion.
(3) Every submodule of M is finitely generated.

Proof. ((1) ⇒ (2)) Suppose that M is Noetherian, and Σ a non-empty set of submodules of M. Let $M_1 \in \Sigma$, and suppose that M_1 is not maximal. Then there exists $M_2 \in \Sigma$ with $M_1 \subseteq M_2$. If M_2 is not maximal, there exists M_3 such that $M_1 \subseteq M_2 \subseteq M_3$. Repeating this step, we can build an ascending chain of modules in Σ. But since M is Noetherian, there must exists N such that $M_n = M_{n+1} = \cdots$ for all $n \geq N$. Then M_k is a maximal element of Σ.

((2) ⇒ (3)) Let N be a submodule of M, and we want to show that N is finitely generated. Let

$$\Sigma = \{N' \mid N' \text{ finitely generated submodule of } N\}.$$

Clearly $0 \in \Sigma$ so $\Sigma \neq \emptyset$. Now let N' be a maximal element of Σ. If $N = N'$, we are done. If not, then $N' \subsetneq N$. So there exists $x \in N$ but $x \in N'$. But then $N' = \langle f_1, \ldots, f_s \rangle$ for some $f_1, \ldots, f_s \in N$ since N' is finitely generated. Define $N'' = \langle f_1, \ldots, f_s, x \rangle$. But $N'' \supsetneq N$, and clearly $N'' \in \Sigma$. But this contradicts the maximality of N'. Therefore $N = N'$, so N is finitely generated.

((3) $\Rightarrow$ (1)) Suppose that $M_1 \subseteq M_2 \subseteq \cdots$ is an ascending chain of submodules of M. Let

$$N := \bigcup_{i \geq 1} M_i,$$

so N is a submodule of M. Thus N is finitely generated, say $N = \langle f_1, \ldots, f_s \rangle$ for $f_1, \ldots, f_s \in M$. Thus there exists $M_{a_1}, \ldots, M_{a_s}$ such that $f_1 \in M_{a_1}, \ldots, f_s \in M_{a_s}$. Without loss of generality suppose that $a_1 \leq a_2 \leq \cdots \leq a_s$. Thus $M_{a_1} \subseteq M_{a_2} \subseteq \cdots \subseteq M_{a_s}$; note that $f_1, \ldots, f_s \in M_{a_s}$, so $M_{a_s} = N$. Therefore we have $M_n = M_{n+1}$ for any $n \geq a_s$, which is precisely the ascending chain condition we wanted to show. $\square$

Example. Any PIDs are Noetherian rings since every ideal is generated by one element.

Definition 20.2. If R is a domain, and M an R-module, then

$$\operatorname{tor}(M) = \{x \in M \mid rx = 0 \text{ for some } r \in R \setminus \{0\}\}$$

is called *the torsion submodule.*

Remark 20.1. The emphasis on the word "the" in the above definition is intended, to emphasize that $\operatorname{tor}(M)$ is the *unique maximal* torsion submodule of M. Observe that any submodule of $\operatorname{tor}(M)$ is also *a* torsion module.

Remark 20.2. If M is a free R-module, then $\operatorname{tor}(M) = 0$. Thus any free module is torsion-free.

Definition 20.3. The *annihilator* of M is

$$\operatorname{ann}(M) = \{r \in R : rn = 0 \text{ for all } n \in M\}.$$

Remark 20.3. Note that the following properties hold for $\operatorname{ann}(M)$:

(1) If N is not a torsion submodule of M, then $\operatorname{ann}(N) = (0)$.
(2) If $N \subseteq L$ both submodules of M, then $\operatorname{ann}(L) \subseteq \operatorname{ann}(N)$, since if $rL = 0$ then $rN = 0$.
(3) If, in addition to (2), R is a PID, then $\operatorname{ann}(L) = (a) \subseteq (b) = \operatorname{ann}(N)$, and so $b \mid a$. In particular, if $x \in M$ then $\operatorname{ann}(x) = (a) \supseteq \operatorname{ann}(M) = (b)$, so $a \mid b$.
(4) $\operatorname{ann}(M)$ is an ideal of R. Indeed, $0 \in \operatorname{ann}(M)$, so $\operatorname{ann}(M)$ is non-empty. If $a, b \in \operatorname{ann}(M)$, then $(a-b)x = ax - bx = 0 - 0 = 0$ for any $x \in M$, so $a - b \in \operatorname{ann}(M)$. Finally, for any $a \in \operatorname{ann}(M)$ and $r \in R$, we have $(ra)x = r(ax) = r0 = 0$ for any $x \in M$. Hence $ra \in \operatorname{ann}(M)$.

21. March 29

Theorem 21.1. *Let R be a PID, and M a free R-module of rank $n < \infty$. Suppose that N is a submodule of M. Then*

(1) N is free of rank m where $m \leq n$.
(2) There is a basis $y_1, \ldots, y_n$ of M such that $a_1 y_1, \ldots, a_m y_m$ is a basis of N where $a_1, \ldots, a_m \in R$ are such that $a_1 \mid a_2 \mid \cdots \mid a_m$.

Proof. The claims hold trivially for $N = 0$, so assume that $N \neq 0$. Thus for all $\varphi \in \mathrm{Hom}_R(M, R)$, $\varphi(N)$ is an ideal of R; and since R is a PID, we have $\varphi(N) = (a_\varphi)$ where $a_\varphi \in R$. Define

$$\Sigma = \{(a_\varphi) \mid \varphi \in \mathrm{Hom}_R(N, R)\}.$$

Clearly $0 \in \Sigma$ so Σ is non-empty. Since R is Noetherian and $\Sigma \neq \emptyset$, Σ has a maximal element, say (a_ν) for some $\nu \in \mathrm{Hom}_R(N, R)$. Therefore $\nu(N) = (a_\nu) \supset (a_\varphi) = \varphi(N)$ for all $\varphi \in \mathrm{Hom}_R(M, R)$. Let $a_1 := a_\nu$.

First, we prove that $a_1 \neq 0$. Let M be a free module with basis, say, $x_1, \ldots, x_n$, and projection homomorphisms $\pi_i : M \to R$ defined by $\sum c_j x_j \mapsto c_i$. Since $N \neq 0$, $\pi_i(N) \neq 0$ for some i. Hence there exists a non-zero element in Σ, which is enough to show that $a_1 \neq 0$, since (a_1) is a maximal element of Σ.

Second, we claim that if $y \in N$ such that $\nu(y) = a_\nu = a_1$, then $a_1 \mid \varphi(y)$ for all $\varphi \in \mathrm{Hom}_R(M, R)$. Fix $\varphi \in \mathrm{Hom}_R(M, R)$ and let $(\varphi(y), a_1) = (d)$. Indeed, if $\varphi(y) \in (d)$ and $a_1 \in (d)$, then $d \mid \varphi(y)$ and $d \mid a_1$. Conversely, if $d \in (\varphi(y), a_1)$ then $d = r_1 a_1 + r_2 \varphi(y)$ for some $r_1, r_2 \in R$.

Let $\psi : r_1\nu + r_2\varphi \in \mathrm{Hom}_R(M, R)$. Then $\psi(y) = r_1\nu(y) + r_2\varphi(y) = r_1 a_1 + r_2\varphi(y)$. So $d \in \psi(N)$; hence $(d) \subseteq \psi(N)$. Thus $(a_1) \subseteq (d) \subseteq \psi(N) \subseteq (a_1)$ since a_1 is a maximal element. Since $(a_1) = (d) = \varphi(N)$, $a_1 \mid d$ and $d \mid \varphi(y)$, so $a_1 \mid \varphi(y)$ as desired.

Let $\varphi = \pi_i$ be the projection onto the "i-th coordinate". Then $a_1 \mid \pi_i(y)$, which holds true for every i. So there exists $b_i \in R$ such that $\pi_i(y) = b_i a_1$ for each $i = 1, 2, \ldots, n$. Suppose that $y_1 = b_1 x_1 + \cdots + b_n x_n$. Then $a_1 y_1 = a_1 b_1 x_1 + \cdots + a_1 b_n x_n = \pi_1(y) x_1 + \cdots + \pi_n(y) x_n =$ y. Thus $a_1 = \nu(y) = \nu(a_1 y_1) = a_1 \nu(y_1)$. But since $a_1 \neq 0$, it follows $\nu(y_1) = 1$.

We claim that y_1 can be a basis element of M, and $a_1 y_1$ can be a basis elements of N. Note that it suffices to show instead that (a) $M = Ry_1 \oplus \ker \nu$ and (b) $N = Ra_1 y_1 \oplus (N \cap \ker \nu)$ – observe that the main claim follows from (a) and (b) by extending $\{y_1\}$ and $\{a_1 y_1\}$ to a basis.

We prove (a) first. Suppose that $x \in M$. Then $x = \nu(x) y_1 + (x - \nu(x) y_1) = \nu(x - \nu(x) y_1) = \nu(x) - \nu(x)\nu(y_1) = \nu(x) - \nu(x) \cdot 1 = 0$. So $x - \nu(x) y_1 \in \ker \nu$. Hence $M = Ry_1 + \ker \nu$. Now suppose that $Ry_1 \cap \ker \nu$ is non-trivial. Then there is $r \in R$ such that $ry_1 \in \ker \nu$. Since $\nu(ry_1) = r\nu(y_1) = 0$, it follows $r = 0$ since $\nu(y_1) = 1$. Hence $Ry_1 \cap \ker \nu$ is trivial, as required.

As for (b), we start by assuming that $x' \in N$ so that $\nu(x') \in (a_1) = \nu(N)$. Then $a_1 \mid \nu(x')$. Thus there exists $b \in R$ such that $\nu(x') = b a_1$. Now consider the decomposition $x' = \nu(x') y_1 + (x' - \nu(x') y_1)$. Clearly $\nu(x') y_1 = b a_1 y_1 \in R a_1 y_1$. Observe that

$$\nu(x' - \nu(x') y_1) = \nu(x') - \nu(x')\nu(y_1) = \nu(x') - \nu(x') = 0,$$

so $x' - \nu(x') y_1 \in \ker \nu \cap N$. Using the similar argument as used in part (a), we see that $Ra_1 y_1 \cap (\ker \nu \cap N) = 0$, so $N = Ra_1 y_1 \oplus (N \cap \ker \nu)$.

Now that all the ground work is complete, we shall go back to prove the two statements of the theorem. For (1), we will prove by induction on m, where m is the maximum number of linearly independent elements of N. If $m = 0$, then N is a torsion module, but this in turn implies $N = 0$. Indeed, since M is free over a PID, M is torsion-free, which in turn implies that the only torsion element of M (hence of N) is 0. If $m > 0$, then $N \cap \ker \nu$ has the maximum $m - 1$ linearly independent elements. By induction hypothesis, $N \cap \ker \nu$ is of rank $m - 1$. Therefore N is free of rank m, completing the proof of (1).

The proof of (2) is also by induction, this time on $n = \text{rank}(M)$. $\ker\nu$ is indeed a submodule of M by (1), and $\ker\nu$ is free. By part (a), $\text{rank}(\ker\nu) = n-1$. So by induction hypothesis applied to $\ker\nu$ and its submodule $N \cap \ker\nu$, there exists a basis $\{y_2, \dots, y_n\}$ of $\ker\nu$ such that $a_2y_2, \dots, a_my_m$ is a basis of $N \cap \ker\nu$, and $a_2 \mid a_3 \mid \cdots \mid a_m$. By (a) we see that $y_1, \dots, y_n$ is a basis of M; and by (b), $a_1y_1, \dots, a_my_m$ is a basis of N. Now it remains to show that $a_1 \mid a_2$. Let $\varphi \in \text{Hom}_R(M, R)$ be such that $\varphi(y_1) = \varphi(y_2) = 1$ but $\varphi(y_i) = 0$ for all $i > 2$. So $a_1 = \varphi(a_1y_1) \in \varphi(N)$. Since $(a_1) \subseteq \varphi(N) \in \Sigma$ and (a_1) is maximal in Σ, we have $\varphi(N) = (a_1)$. Similarly, $a_2 = \varphi(a_2y_2) \in \varphi(N)$, so $a_2 \in (a_1)$, which proves $a_1 \mid a_2$. □

22. April 1

Definition 22.1. An R-module M is *cyclic* if $M = \langle x \rangle$ for some $x \in M$.

Let $\pi : R \to M = \langle x \rangle$ such that $\pi(1) = x$ and hence $\pi(r) = rx$. Then π is surjective, so by the first isomorphism theorem we have $M \cong R/\ker\pi$. But if R is a PID, then there exists $a \in R$ such that $\ker\pi = (a)$. Thus $M \cong R/(a)$. Therefore, a cyclic module over a PID R is of this form. Particularly, $(a) = \text{ann}(M)$.

Theorem 22.1 (Fundamental theorem of finitely generated modules over a PID)**.** *Suppose R is a PID, and M is a finitely generated R-module. Then the following are true.*

(1) M is isomorphic to the direct sum of finitely many cyclic modules. That is, there exist $r \in \mathbb{N} \cup \{0\}$ and non-units $a_1, \dots, a_m \in R^*$ such that $a_1 \mid a_2 \mid \cdots \mid a_m$ such that

$$M \cong R^r \oplus R/(a_1) \oplus \cdots \oplus R/(a_m).$$

(2) From the above isomorphism, $R/(a_1) \oplus \cdots \oplus R/(a_m)$ is isomorphic to the torsion submodule of M. In particular, M is a torsion R-module if and only if $r = 0$, and in this case $\text{ann}(M) = (a_m)$.

(3) M is torsion-free if and only if M is free.

Proof. (1) M is finitely generated, so let $\{x_1, \dots, x_n\}$ be a generating set for M of minimal cardinality. Let R^n be the free R-module of rank n with basis $b_1, \dots, b_n$. Define $\pi : R^n \to M$ by $r(b_i) = x_i$, and extend by R-linearity to R^n. But π is surjective, so the first isomorphism theorem implies $M \cong R^n/\ker\pi$. $\ker(\pi)$ is a submodule of M, and M is free over R which is a PID, so $\ker(\pi)$ is free over R. Hence there exist a basis $y_1, \dots, y_n$ of R^n and $a_1, \dots, a_m \in R$ such that $a_1 \mid a_2 \mid \cdots \mid a_m$ and $a_1y_1, \dots, a_my_m$ is a basis of $\ker(\pi)$ by virtue of Theorem 21.1. Thus we have

$$M \cong R^n/\ker\pi = \frac{Ry_1 \oplus Ry_2 \oplus \cdots \oplus Ry_n}{Ra_1y_1 \oplus \cdots \oplus Ra_my_m}.$$

Define $\varphi : Ry_1 \oplus \cdots \oplus Ry_n \to R/(a_1) \oplus \cdots \oplus R(a_m) \oplus R^{n-m}$ by $\varphi(u_1y_1, \dots, u_ny_n) = (u_1 \bmod (a_1), \cdots, u_m \bmod (a_m), u_{m+1}, \dots, u_r)$. And so $\ker\varphi = Ra_1y_1 \oplus Ra2y_2 \oplus \cdots \oplus Ra_my_m \oplus 0^{n-m}$. Putting the isomorphisms together, we see

$$M \cong \frac{Ry_1 \oplus \cdots Ry_n}{Ra_1y_1 \oplus \cdots \oplus Ra_my_m} \cong R/(a_1) \oplus \cdots \oplus R/(a_m) \oplus R^{n-m}.$$

If any of the a_i is a unit, then $R/(a_i) = 0$ so we can drop that component from the direct sum. This means we can assume that any of the a_i's are non-units.

(2) This follows immediately, since $\text{ann}(R/(a_i)) = (a_i)$.

(3) Each $R/(a_i)$ is a torsion R-module, so R is torsion-free if and only if $M \cong R^r$. □

Definition 22.2. Suppose R is a PID, and M a finitely generated R-module. Then there are $r \in \mathbb{N} \cup \{0\}$ and $a_1 \,|\, a_2 \,|\, \cdots \,|\, a_m$ non-units such that

$$M \cong R^r \oplus R/(a_1) \oplus \cdots \oplus R/(a_m).$$

Then r is called the *free rank* or the *Betti number* of M. $a_1, \ldots, a_m$ are called the *invariant factors* of M, unique up to multiplication by units. Finally, we call such presentation the *invariant factor form.*

Remark 22.1. The r and the a_i from the above definition are all unique, though this is yet to be proved.

Any PID is a UFD, so R has unique factorization. So if $a \in R$, then $a = up_1^{\alpha_1} \cdots p_s^{\alpha_s}$ where the p_i's are primes, and u is a unit and $\alpha_i > 0$ for all $1 \leq i \leq s$. And hence the ideals $(p_i^{\alpha_i})$ are uniquely determined by a. It is also known that $(p_i^{\alpha_i}) + (p_j^{\alpha_j}) = R$ for any $i \neq j$ since $\gcd(p_i^{\alpha_i}, p_j^{\alpha_j}) = 1$ (i.e., $(p_i^{\alpha_i})$ and $(p_j^{\alpha_j})$ are comaximal). By the Chinese remainder theorem,

$$R/(a) \cong R/(p_1^{\alpha_1}) \oplus \cdots \oplus R/(p_s^{\alpha_s}).$$

Apply this to the invariant factor form of M to obtain the following theorem.

Theorem 22.2. *If M is a finitely generated R-module over a PID R, then M is the direct sum of finitely many cyclic R-modules whose annihilators are either* (0) *or generated by powers of primes in R, i.e.,*

$$M \cong R^r \oplus R/(p_1^{\alpha_1}) \oplus \cdots \oplus R/(p_t^{\alpha_t}),$$

where $r \geq 0, p_1^{\alpha_1}, \ldots, p_t^{\alpha_t}$ are powers of not necessarily distinct primes $p_1, \ldots, p_t \in R$.

Definition 22.3. The $p_1^{\alpha_1}, \ldots, p_t^{\alpha_t}$ in the above decomposition are called the *elementary divisors* of M, and the abote decomposition is called the *elementary divisor form.*

23. April 3

In this lecture we will prove the uniqueness of presentation of a finitely generated modules over a PID (i.e., the uniqueness of the Betti number, invariant factors, and elementary divisors).

Theorem 23.1 (Primary decomposition theorem)**.** *Let R be a PID, and M a non-zero torsion R-module (not necessarily finitely generated) with a non-zero annihilator a. Suppose that the factorization of a into distinct powers of primes in R is $a = up_1^{\alpha_1} \cdots p_n^{\alpha_n}$ where u is a unit, p_i primes, and $a_i \in \mathbb{Z}_+$. Also let $N_i = \{x \in M : p_i^{\alpha_i} x = 0\}$ for each $1 \leq i \leq n$. Then N_i is a submodule of M with annihilator $p_i^{\alpha_i}$ and is the submodule of M consisting of all elements annihilated by some power of p_i. We have*

$$M = N_1 \oplus N_2 \oplus \cdots \oplus N_n.$$

If M is finitely generated, then each N_i is a direct sum of finitely many cyclic modules whose annihilators are divisors of $p_i^{\alpha_i}$.

Proof. The result is known if M is finitely generated (just group together all factors $R/(p^\alpha)$, with the same p and varying α). In general, it is easy to prove that N_i is a submodule with annihilator $(p_i^{\alpha_i})$. If R is a PID, then $(p_i^{\alpha_i})$ and $(p_j^{\alpha_j})$ is comaximal if $i \neq j$. Therefore by the Chinese remainder theorem it follows $M = N_1 \oplus N_2 \oplus \cdots \oplus N_n$. $\square$

Lemma 23.1. *Let R be a PID, p a prime in R, and let $F = R/(p)$ which is a field. Then*

(1) If $M = R^r$, then $M/pM \cong F^r$.

(2) If $M = R/(a)$ and $a \neq 0$, then

$$M/pM \cong \begin{cases} F & (\textit{if } p \,|\, a \textit{ in } R) \\ 0 & (\textit{if } p \nmid a \textit{ in } R). \end{cases}$$

(3) $M = R/(a_1) \oplus \cdots \oplus R/(a_k)$ where $p \,|\, a_i$ for all i, then $M/pM \cong F^k$.

Proof. (1) Consider the map $\pi : R^r \to F^r = (R/(p))^r$ defined by $(\alpha_1, \ldots, \alpha_r) \mapsto (\overline{\alpha_1}, \ldots, \overline{\alpha_r})$ where $\overline{\alpha_i} = \alpha_i \bmod (p)$. π is a surjective R-module homomorphism and $\pi(\alpha_1, \ldots, \alpha_r) = 0$ if and only if $p \,|\, \alpha_i$ for all $i = 1, 2, \ldots, r$. Therefore $\ker \pi = pR^r = pR \oplus \cdots \oplus pR$. Hence $R^p/pR^r \cong F^r \cong M/pM$.

(2) Let $M = R/(a)$. Then $pM = pR/(a) = ((p) + (a))/(a)$. If $d = \gcd(p, a)$, then $(p) + (a) = (d)$. So putting the two things together, we have

$$M/pM \cong \frac{R/(a)}{((p) + (a))/(a)} \cong R/((p) + (a)).$$

Therefore if $p \,|\, a$, then $R/(p) = F$. If $p \nmid a$, then $\gcd(p, a) = d = 1$ so $(d) = R$. Therefore in this case $M/pM = 0$.

(3) If $M = R/(a_1) \oplus \cdots \oplus R/(a_k)$ such that $p \,|\, a_i$ for all i, then let $\pi : R/(a_1) \oplus \cdots \oplus R/(a_k) \to R/(p) \oplus \cdots \oplus R/(p)$ be $(u_1 + (a_1), \ldots, u_k + (a_k)) \to (u_1 + (p), \ldots, u_k + (p))$ where $u_1, \ldots, u_k \in R$. Note that $(u_1 + (a_1), dots, u_k + (a_k)) \in \ker \pi$ if and only if $p \,|\, u_i$ for each i; this is also equivalent to saying that $u_i + (a_i) \in pR/(a_i)$. This means that

$$\ker(\pi) = pR/(a_1) \oplus \cdots \oplus pR/(a_k) = pM.$$

Therefore $M/pM = M/\ker \pi \cong F^k$. □

24. April 5

Definition 24.1. If R is a ring, and M an R-module, then the *p-primary submodule* of M is the submodule of M consisting of elements annihilated by a power of p.

Theorem 24.1 (Fundamental theorem of finitely generated modules over a PID – uniqueness)**.** *Two finitely generated modules M_1 and M_2 over a PID R are isomorphic if and only if they have the same free rank and the same list of invariants. Also, two finitely generated modules M_1 and M_2 over a PID R are isomorphic if and only if they have the same free rank and the same set of elementary divisors.*

Proof. ($\Leftarrow$) This direction is evident (for both invariant factors and elementary divisors).

($\Rightarrow$) Suppose that $M_1 \cong M_2$, with an isomorphism $\varphi : M_1 \to M_2$. Note that then $\varphi(\operatorname{tor}(M_1)) = \varphi(\operatorname{tor}(M_2))$ since $am_1 = 0$ if and only if $a\varphi(m_1) = 0$. Hence

$$R^{r_1} \cong M_1/\operatorname{tor}(M_1) \cong M_2/\operatorname{tor}(M_2) \cong R^{r_2}.$$

So by the invariant rank property of free modules over a PID, we see $r_1 = r_2$. Hence we may assume that M_1 and M_2 are both torsion modules. Suppose p is a prime, $\alpha \in \mathbb{Z}^+$, and p^α an elementary divisor of M_1. Suppose that $M_1 \to M_2$ is an isomorphism. Then there exists $m_1 \in M_1$ such that $p^\alpha m_1 = 0$, so $p^\alpha \varphi(m_1) = 0$. Thus the p-primary submodule of M_1 is isomorphic to the p-primary submodule of M_2. Observe that the p-primary component of M_1 is a direct sum of $R/(p^\alpha)$ for various α, and the same goes for M_2.

So without loss of generality, we may assume that we have two modules M_1 and M_2 where $\operatorname{ann}(M_1)$ and $\operatorname{ann}(M_2)$ are both generated by a power of p – say $\operatorname{ann}(M_1) \cong \operatorname{ann}(M_2) = (p^k)$. We will prove by induction on k that M_1 and M_2 have the same list of elementary divisors.

If $k = 0$, then $M_1 = M_2 = 0$, so this completes the base case. Suppose $k > 0$. The. In M_1 and M_2 have elementary divisors $\underbrace{p, p, \ldots, p}_{m \text{ times}}, p^{\alpha_1}, \ldots, p^{\alpha_s}$. In other words,

$$M_1 \cong (R/(p))^m \oplus R/(p^{\alpha_1}) \oplus \cdots \oplus R/(p^{\alpha_s}),$$

where $2 \leq \alpha_1 \leq \alpha_2 \leq \cdots \leq \alpha_s$. Now the module pM has elementary divisors $p^{\alpha_1 - 1}, \ldots, p^{\alpha_s - 1}$. Therefore,

$$pM_1 \cong R^m \oplus R/(p^{\alpha_1 - 1}) \oplus \cdots \oplus R/(p^{\alpha_s - 1}).$$

Similarly, the elementary divisors of M_2 are $\underbrace{p, p, \ldots, p}_{n \text{ times}}, p^{\beta_1}, \ldots, p^{\beta_t}$ where $2 \leq \beta_1 \leq \cdots \leq \beta_t$, so the elementary divisors of pM_2 are $p^{\beta_1 - 1}, \ldots, p^{\beta_t - 1}$.

If $M_1 \cong M_2$, then $pM_1 \cong pM_2$. Furthermore, $\operatorname{ann}(pM_1) \cong \operatorname{ann}(pM_2) = (p^{k-1})$. By the induction hypothesis, we have $\beta_1 - 1 = \alpha_1 - 1, \ldots, \beta_{t-1} = \alpha_s - 1$. Hence $s = t$ and $\alpha_i = \beta_i$ for all $1 \leq i \leq s$.

Also, if $F := R/(p)$, we have $F^{t+m} \cong M_1/pM_1 \cong M_2/pM_2 \cong F^{t+n}$ by Lemma 23.1, so $t + m = t + n$, or $m = n$. Hence M_1 and M_2 have the same set of elementary divisors $\underbrace{p, p, \ldots, p}_{m \text{ times}}, p^{\alpha_1}, \ldots, p^{\alpha_t}$.

We shall now show that M_1 and M_2 have the same invariant factors. If $a_1 \,|\, a_2 \,|\cdots|\, a_m$ are invariant factors of M_1 and $b_1 \,|\, b_2 \,|\cdots|\, b_n$ those of M_2, then we can find elementary divisors of M_1 by factoring $a_1, \ldots, a_m$, and of M_2 by factoring $b_1, \ldots, b_n$. Since $a_1 \mid \cdots \mid a_m$, a_m contains the largest power of each prime appearing in $a_1, \ldots, a_{m-1}$. Similarly, a_{m-1} contains the largest power of each prime appearing in $a_1, \ldots, a_{m-2}$, and so forth.

In a similar fashion, we get elementary divisors of M_2 from $b_1, \ldots, b_n$. Since the list of elementary divisors of M_1 and M_2 are the same, a_m and b_n can only differ by a unit (i.e., $a_m = ub_n$ for some unit $u \in R$). This hold for a_{m-1} and b_{n-1}, and so on. Hence $m = n$ and $a_i = u_i b_i$ for all $1 \leq i \leq n$ where each u_i is a unit. □

Corollary 24.1. *Let R be a PID, and M a finitely generated R-module.*

(1) The elementary divisors of M are the prime power factors of the invariant factors of M.

(2) The largest invariant factor of M is the product of the largest of the distinct prime powers amongst the elementary divisors of M; the next largest invariant factor of M is the product of the largest of the remaining distinct prime powers, and so forth.

Corollary 24.2 (Fundamental theorem of finitely generated abelian groups)**.** *If G is a finitely generated abelian group, then*

(1) there exist $r, n_1, \ldots, n_s \in \mathbb{Z}$ satisfying $G \cong \mathbb{Z}^r \oplus \mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_s\mathbb{Z}$ such that:
  - *(a) $r \geq 0, n_j \geq 2$ for all j*
  - *(b) $n_1 \,|\, n_2 \,|\cdots|\, n_s$.*

(2) The expression in (1) is unique.

Department of Mathematics and Statistics, Dalhousie University, 6316 Coburg Rd, Halifax, NS, Canada B3H 4R2
E-mail address: hsyang@dal.ca