Lecture 1

Rings:

Definition 0.1. A ring R is an abelian group $(R, +)$ together with multiplication

$$\begin{aligned} R \times R &\mapsto R \\ (r, s) &\mapsto r \cdot s \end{aligned}$$

such that

1. $r_1 \cdot (r_2 \cdot r_3) = (r_1 \cdot r_2) \cdot r_3$ for all $r_1, r_2, r_3 \in R$. In other words, multiplication is *associative.*

2. $r_1 \cdot (r_2 + r_3) = r_1 \cdot r_2 + r_1 \cdot r_3$ for all $r_1, r_2, r_3 \in R$. That is, $\cdot$ *distributes* over $+$.

3. There is an element $1 \in R$ such that $1 \cdot r = r \cdot 1 = r$ for all $r \in R$. This is *multiplicative identity.*

Remark.

- The multiplication is *not* assumed to be commutative. If it is, we say R is a *commutative ring.*
- The above definition (including 3) is sometimes called *ring with identity.* An object which satisfies all of these except 3 is sometimes called a *rng* (pronounced "rung").

Example 0.1. **1.** The integers $\mathbb{Z}$ with the usual addition and multiplication.

2. For any $n \in \mathbb{N}, n \geq 1$, $\mathbb{Z}/n\mathbb{Z}$ is a ring under the operations

$$\begin{aligned} + : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} &\mapsto \mathbb{Z}/n\mathbb{Z} \\ (\overline{a}, \overline{b}) &\mapsto \overline{a+b} \\ \times : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} &\mapsto \mathbb{Z}/n\mathbb{Z} \\ (\overline{a}, \overline{b}) &\mapsto \overline{ab} \end{aligned}$$

3. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all rings (in fact they are fields).

4. The set of $n \times n$ matrices with entries in a ring R.

5. $R[x]$, the ring of all polynomials with coefficients in a ring R

6. Let G be an abelian group, and let

$$R = \{\text{all group homomorphisms } G \to G\}$$

Define, for all $\phi, \psi \in R$, for all $g \in G$,

$$(\phi + \psi)(g) = \phi(g) + \psi(g)$$
$$(\phi \cdot \psi(g) = \phi(\psi(g))$$

$1 = \mathrm{Id}_G$.

Exercise: Check that R is a ring.

7. Let X be any set, and let $R = \mathcal{P}(X)$, the power set of X. Define, for all $E, F \in R$,

$$E + F = E \triangle F$$
$$E \cdot F = E \cap F$$

$1 = X$ Exercise: Check R is a (commutative) ring.

Definition 0.2. Let R and S be rings. A ring homomorphism is a map $f : R \to S$ such that for all $r_1, r_2 \in R$,

$$f(r + s) = f(r) + f(s)$$
$$f(r \cdot s) = f(r) \cdot f(s)$$
$$f(1_R) = 1_S$$

Example 0.2. The quotient map $\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ given by $a \mapsto \overline{a}$ is a ring homomorphism.
Let R be a ring.

Definition 0.3. A subset $S \subseteq R$ is a subring if S is an additive subgroup of R, is closed under multiplication, and contains 1.

Definition 0.4. **1.** A subset $I \subseteq R$ is a left ideal of R if I is an additive subgroup of R such that $R \cdot I \subseteq I$, i.e. for all $r \in R, s \in I$, $rs \in I$.

A subset $I \subseteq R$ is a right ideal of R if I is an additive subgroup of R such that $I \cdot R \subseteq I$, i.e. for all $s \in I, r \in R$, $sr \in I$.

An ideal is both a left and right ideal (a "two-sided" ideal).

2. Suppose I is an ideal. Then the quotient

$$R/I \overset{\text{def}}{=} \{\overline{r} = r + I : r \in R\}$$

inherits an addition and multiplication from R :

$$(r+I) + (r'+I) = (r+r'+I)$$
$$(r+I) \cdot (r'+I) = (r \cdot r' + I)$$

making it a ring with identity $1+I$. This is called the quotient ring or residue class. Note that the quotient map

$$\pi : R \to R/I$$
$$r \mapsto \overline{r} = r + I$$

is a ring homomorphism.

Two Exercises:

1. ("Correspondence Theorem")

Let R be a ring, $I \subseteq R$ an ideal, and $\phi : R \to R/I$ the quotient map. Then there is a bijective orderpreserving correspondence between $\{J \subset R, J$ is an ideal, $I \subseteq J \subseteq R\}$ and ideals of R/I, which sends J to $\overline{J} = \phi(J) = (I+J)/I$.

2. ("First Isomorphism Theorem")

Let $\phi : R \to S$ be a ring homomorphism. Then

- $\ker(\phi) = \{r \in R : \phi(R) = 1_S\} \subset R$ is an ideal of R.
- $\mathrm{Im}(\phi) = \{s \in S : \exists r \in R s.t. s = \phi(r)\}$ is an ideal of S.
- ϕ induces a ring isomorphism (i.e. a bijective ring homomorphism whose inverse is also a ring homomorphism)

$$R/\ker(\phi) \to \mathrm{Im}(\phi)$$

given by

$$\overline{r} \mapsto \phi(r)$$

Lecture 2, 1/11/23

Definition 0.5. **1.** A zero divisor in a ring R is an element $x \in R$ such that there exists a $y \in R, y \neq 0$, such that $xy = yx = 0$.

Examples:

$\overline{2} \in \mathbb{Z}/6\mathbb{Z}$ is a zero divisor. 0 is always a zero divisor unless $R = \{0\}$.

2. A nonzero commutative ring R without nonzero zero divisors is called an integral domain.

Examples: $\mathbb{Z}$, all polynomial rings, $\mathbb{Z}/p\mathbb{Z}$ where p is prime are all integral domains.

3. An element $r \in R$ is nilpotent if $r^n = 0$ for some $n > 0$.

Note: r nilpotent $\implies$ r a zero divisor. The converse is false (e.g. $\overline{2} \in \mathbb{Z}/6\mathbb{Z}$)

4. An element $R \in R$ is a unit (or invertible) if there exists an $s \in R$ such that $rs = sr = 1$.

Examples: $\overline{5} \in \mathbb{Z}/6\mathbb{Z}$. A matrix $A \in M_{n\times n}(R)$ with entries in a ring R is a unit in the matrix ring if and only if $\det(A)$ is a unit in R.

Note that $R^\times$, denoting the units, is a multiplicative group.

5. Let $x \in R$ The multiples $r \cdot x$ (or $x \cdot r$) form a left (or right) ideal, denoted Rx (or xR). If R is commutative, we write (x) for $Rx = xR$.

6. A field is a nonzero commutative ring R in which every nonzero element is a unit.

Note: Since being a unit implies not being a zero divisor, all fields are integral domains. The converse does not hold, and $\mathbb{Z}$ is a witness to its failure.

Proposition 1. *Let R be a nonzero commutative ring. Then the following are equivalent:*

1. *R is a field.*

2. *The only ideals are $\{0\}$ and R.*

3. *Every ring homomorphism $R \to S$ with $S \neq \{0\}$ is injective*

Proof. $1 \to 2$ Suppose R is a field. Let I be a nonzero ideal. Then there exists $x \in I$ nonzero. Since R is a field, x is a unit. Thus $R = (x) \subseteq I$. So $I = R$.

$2 \to 3$ For $S \neq \{0\}$, let $\phi : R \to S$ be a ring homomorphism. Then $\ker(\phi) \subseteq R$ is a proper ideal (since $\phi(1) = 1 \neq 0$). By 2, $\ker(\phi) = \{0\}$, so ϕ is injective.

3 → 1 Let $x \in R$ be nonzero. We want to show that X is a unit. Consider the quotient map $\phi : R \to R/(x)$. Notice $\ker(\phi) = (x) \neq \{0\}$, i.e. ϕ is not injective. By 3, $R/(x) \cong \{0\}$, so $(x) = R$, i.e. $x \in R^\times$.

Definition 0.6. Let R be a commutative ring.

1. An ideal I is a prime ideal if it is a proper ideal and for all $r, s \in R$, $rs \in I$ if and only if $r \in I, s \in I$, or both.

Note $p \in \mathbb{N}$ is prime if and only if for all $a, b \in \mathbb{Z}$, $p \mid ab$ implies $p \mid a$, $p \mid b$, or both.

Equivalently, $ab \in (p)$ implies $a \in (p), b \in (p)$, or both.

2. An ideal $I \subset R$ is a maximal ideal if I is proper and, if J is an ideal such that $I \subset J \subset R$, then $J = I$ or $J = R$.

Proposition 2. *Let R be a commutatie ring and I a proper ideal. Then R/I is an integral domin if and only if I is a prime ideal.*

Proof. =>

Let $r, s \in R$ such that $rs \in I$. We want to show that $r \in I$ or $s \in I$. Then the elements $\overline{r}, \overline{s} \in R/I$ are such that $\overline{r} \cdot \overline{s} = \overline{rs} = \overline{0}$. Since R/I is an integral domain, either $\overline{r} = \overline{0}$ or $\overline{s} = \overline{0}$, or both. In other words, either $r \in I$, or $s \in I$.

<=

Since $I \neq R$, the ring R/I is nonzero. Choose $\overline{r}, \overline{s} \in R/I$ such that $\overline{r} \cdot \overline{s} = \overline{0}$. We want to show that either $\overline{r} = \overline{0}, \overline{s} = \overline{0}$, or both . Since $\overline{rs} = \overline{r} \cdot \overline{s} = \overline{0}$, $rs \in I$. Since I is a prime ideal, either $r \in I$ or $s \in I$, or both. So $\overline{r} = \overline{0}, \overline{s} = \overline{0}$, or both. Thus, R/I is an integral domain.

■

Lecture 3, 1/13/23

Proposition 3. *Let R be a nonzero commutative ring, and $I \subset R$ a proper ideal. Then R/I is a field if and only if I is a maximal ideal.*

Proof. =>

Suppose that $J \subset R$ is an ideal with $I \subset J \subset R$. Suppose that these inclusions are strict i.e. $I \subsetneq J \subsetneq R$. Let $X \in J \setminus I$, so $\underbrace{\overline{x}}_{\stackrel{\text{def}}{=} x+I} \neq \overline{0} \in R/I$. Then by assumption there exists $\overline{y} \in R/I$ such that $\underbrace{\overline{x} \cdot \overline{y}}_{=\overline{xy}} = \overline{1} \in R/I$. So, $1 - xy \in I \subset J$. But $x \in J$ and J is an ideal, so $xy \in J$. So, $1 \in J$, so $J = R$.

<=

Let $\overline{x} \neq \overline{0} \in R/I$ for some $x \notin I$. Consider $J = \underbrace{\{a + rx \mid a \in I, r \in R\}}_{I+(x)}$. Then we see that J is an ideal of R containing I, i.e. $I \subset J$. Further, $X \neq J$ because $x \in J \setminus I$. By maximality, we must conclude that $J = R$.
In particular, $1 = a + rx$ for some elements $a \in I, r \in R$. So in R/I, $\overline{1} = \overline{a + rx} = \overline{a} + \overline{rx}$. $a \in I$ though, so $\overline{1} = \overline{rx}$, so $\overline{x}$ is indeed a unit of R/I.

∎

Corollary 0.1. *In a nonzero commutative ring R, all maximal ideals are prime ideals.*

Proof. Fields are integral domains

∎

Remark. The converse is <u>not</u> true. $\mathbb{Z}$ is an integral domain with prime ideal (0), but this ideal is not maximal, as $\mathbb{Z}/(0) \cong \mathbb{Z}$ is not a field!
For another counterexample, let $R = \mathbb{Z}[x]$, and consider the ideal $I = \{$ all polynomials with constant term equal to $0\} = (x)$. This ideal is prime, since $R/I \cong \mathbb{Z}$ via $\overline{f(x)} \mapsto f(0)$ is an integral domain. But this ideal is not maximal, because $\mathbb{Z}$ is not a field.
Note: I is strictly contained in the ideal of polynomials with even constant term, which is a strict subset of $R = \mathbb{Z}[x]$.

<u>The existence of maximal ideals</u>

Definition 0.7. A <u>partial ordering</u> on a set A is a relation $\leq$ satisfying

1. $x \leq x$ for all $x \in A$

2. $x \leq y, y \leq x \implies x = y$ for all $x, y \in A$

3. If $x \leq y$ and $y \leq z$, then $x \leq z$.

Remark. This definition does <u>not</u> necessitate that all elements x, y are comparable.

Definition 0.8. Let $(A, \leq)$ be a partially ordered set.

- Let $B \subset A$ and $x \in A$. We say x is an <u>upper bound</u> for B if $y \leq x$ for all $y \in B$.

- A subset $B \subset A$ is called a chain if $\leq$ is a total ordering on B (that is, all elements of B are comparable to all other elements of B)

Lemma 1. *(Zorn's Lemma)*
Let A be a nonempty partially ordered set in which every chain has an upper bound. Then A has a maximal element, i.e. an element $x \in A$ such that for all $y \in A$, y cannot be compared to x, or $y \leq x$.

Proof. This is actually equivalent to the axiom of choice!

■

Theorem 0.2. *Let R be a nonzero commutative ring, and let $I \subset R$ be a proper ideal. Then there exists a maximal ideal $J \subset R$ containing I.*

Proof. Consider the poset (Partially Ordered SET) A consisting of all proper ideals containing I, partially ordered by inclusion.
Then:

- $A \neq \varnothing$, since $I \in A$
- If $a_{\lambda\lambda\in\Lambda}$ is a chain in A, then $\cup_{\lambda\in\Lambda} a_\lambda \in A$ gives an upper bound for the chain.

  Note: In general, the union of ideals is not an ideal. However, this is an increasing union of ideals, which does give an ideal.

By Zorn's lemma, there exists a maximal element of A, which will be a maximal ideal containing I.

■

Corollary 0.3. *Let R be a nonzero commutative ring. Then R contains some maximal ideal.*

Proof. Take $I = (0)$ in the previous proposition.

■

Lecture 4, 1/18/23

From now on:
All rings R will be assumed to be commutative with 1.

Definition 0.9. • Let $A_1, \dots, A_t \subset R$ be ideals, then their sum is the ideal

$$A_1 + \cdots + A_t \stackrel{\text{def}}{=} \{a_1 + \cdots + a_t \mid a_i \in A_i\}$$

This is the smallest ideal containing A_i for all i.

- If $x_1, \dots, x_t \in R$, the ideal generated by them

$$(x_1, \dots, x_t) \stackrel{\text{def}}{=} \{\sum_{i=1}^{t} r_i x_i \mid r_i \in R\}$$
$$= (x_1) + \cdots + (x_t)$$

- More generally, if $\{x_i\}_{i \in I} \subset R$ is some collection of elements of R, the ideal they generate is

$$\sum_{i \in I} (x_i) \stackrel{\text{def}}{=} \{\text{all finite linear combinations of elements of } \{x_i\}_{i \in I}\}$$

- If $A, B \subset R$ are ideals, then their product is the ideal

$$AB \stackrel{\text{def}}{=} \{\sum_{i}^{n} a_i b_i \mid a_i \in A, b_i \in B, n < \infty\}$$

this is the ideal generated by $\{ab \mid a \in A, b \in B\}$. Note $A \cap B \subsetneq AB$, with equality if $A + B = R$

Example 0.3. Let $R = \mathbb{Z}$. Then $(a) + (b) = (\gcd(a, b))$, $(a) \cap (b) = (\operatorname{lcm}(a, b))$. When a, b are coprime, then $(a) + (b) = (1) = \mathbb{Z}$, and $(a) \cap (b) = (ab)$.

Definition 0.10. A ring R with exactly 1 maximal ideal $\mathfrak{M}$ is called a local ring (often denoted $(R, \mathfrak{M})$).

Example 0.4.
- $(\mathbb{R}, \{0\})$ is a local ring (in fact any field is) with maximal ideal $\{0\}$
- $(\mathbb{Z}/(p^n), p\mathbb{Z}/(p^n))$ is a local ring for any prime p and $n > 0$

Lemma 2. Let R be a ring and $\mathfrak{M} \subsetneq R$ a proper ideal such that every $x \in R \setminus \mathfrak{M}$ is a unit. Then R $(R, \mathfrak{M})$ is a local ring.

Proof. We want to show that $\mathfrak{M}$ is a maximal ideal of R, and is the unique such maximal ideal.
Let $I \subsetneq R$ be a proper ideal. If it contained a unit, then $I = R$, which by hypothesis is not true. So, I contains no units. So, it must exist entirely within $\mathfrak{M}$. So, $\mathfrak{M}$ is a unique maximal ideal.

■

Proposition 4. Let R be a ring and $\mathfrak{M} \subset R$ a maximal ideal. Then $(R, \mathfrak{M})$ is a local ring if and only if every $x \in 1 + \mathfrak{M}$ is a unit in R.
Note: $1 + \mathfrak{M} = \{1 + y \mid y \in \mathfrak{M}\} \subset R$ is closed under multiplication.

Proof. =>

Suppose $(R, \mathfrak{M})$ is a local ring, and suppose for the sake of contradiction that $x \in 1+\mathfrak{M}$ is NOT a unit. Note $x = 1+y, y \in \mathfrak{M}$. By hypothesis, $(1+y)$ is a proper ideal in R, because $1+y$ is not a unit.
So $(1+y) \subset \mathfrak{M}$. In particular, $1+y \in \mathfrak{M}$. But $y \in \mathfrak{M}$, so $1 \in \mathfrak{M}$. Oopsy! Contradiction. So, we have proven one direction.

<=

Let $x \in R \setminus \mathfrak{M}$. Since $\mathcal{M}$ is maximal, $\mathfrak{M} + (x) = R$. So, $1 = y + rx$ for some $y \in \mathfrak{M}, r \in R$. Thus $rx = 1 - y \in \mathfrak{M}$, so rx is a unit by hypothesis, meaning there is a z such that $(rx)z = 1 = x(rz)$, so x is a unit.
By the lemma, this shows $(R, \mathfrak{M})$ is a local ring.

■

Definition 0.11. Let R be a ring. Then the nilradical is defined as

$$\mathcal{N} \stackrel{\text{def}}{=} \{\text{all nilpotent elements of } R\}$$

Proposition 5. *The nilradical is an ideal, and the quotient ring $R/\mathcal{N}$ has no nonzero nilpotent elements.*

Proof. If $x \in \mathcal{N}$, then clearly $rx \in \mathcal{N}$ for any $r \in R$. Suppose $x, y \in \mathcal{N}$. Then for some n, m, $x^n = y^m = 0$. Then, by the binomial theorem,

$$(x-y)^{n+m} = \sum_{i=0}^{n+m} x^i (-y)^{n+m-i} \binom{n+m}{i}$$

for all i, at least one of x^i, y^{n+m-i} is zero. So, this sum is zero, so $(x-y) \in \mathcal{N}$.
Now, suppose $\overline{x} \in R/\mathcal{M}$. We want to show that $\overline{x} = 0$. Then $\overline{x}^n = 0$ for some n, so $x^n \in \mathcal{N}$ for some n. But then x^n is nilpotent, so x is nilpotent. So, $\overline{x} = 0$.

■

Proposition 6. *The nilradical of R is the intersection of all prime ideals of R.*

Proof. Let $x \in \mathcal{N}$. Then $x^n = 0 \in \mathscr{P}$ for any prime ideal $\mathscr{P} \subset R$. So, $x \in \mathscr{P}$, so $\mathcal{N}$ is contained in the intersection. We will do the other inclusion next time.

■

Lecture 5, 1/20/23

We will continue the proof. Suppose $f \notin \mathscr{N}$. We wish to show that $f \notin \mathscr{P}$ for some prime ideal $\mathscr{P}$.
Let $\Sigma = \{\text{ideals } I \subset R \mid f^n \notin I \text{ for all } n > 0\}$.
Then $\Sigma \neq \varnothing$, as it contains 0 by hypothesis. Further, we can check that any chain has an upper bound (exercise).
By Zorn's Lemma, there exists a maximal $\mathscr{P} \in \Sigma$.
It remains to show $\mathscr{P}$ is a prime ideal.
Suppose that $x, y \notin \mathscr{P}$. Then $\mathscr{P} \subsetneq \mathscr{P} + (x)$ and $\mathscr{P} \subsetneq \mathscr{P} + (y)$. But by maximality of $\mathscr{P}$, $\mathscr{P} + (x), \mathscr{P} + (y) \notin \Sigma$. So, for some n, m, $f^n \in \mathscr{P} + (x)$, $f^m \in \mathscr{P} + (y)$.
So,

$$f^{n+m} \in (\mathscr{P} + (x))(\mathscr{P} + (y)) \subset \mathscr{P} + (xy)$$

Thus $\mathscr{P} + (xy) \notin \Sigma$. But $\mathscr{P} \in \Sigma$, so we are forced to conclude $(xy) \notin \Sigma$, so $xy \notin \mathscr{P}$. ■

Definition 0.12. We say that the ideals $I, J \subset R$ are coprime if $I + J = R$.

Example 0.5. $(m), (n) \in \mathbb{Z}$ are coprime iff $\gcd(m, n) = 1$, since $(m) + (n) = (d)$, where $d = \gcd(m, n)$.

Definition 0.13. Let $R_1, \ldots, R_m$ be rings. Their direct product is defined as

$$R_1 \times \cdots \times R_n = \{(x_1, \ldots, x_n) \mid x_i \in R\}$$

forms a ring with addition and multiplication defined component-wise.

Theorem 0.4. *(Chinese Remainder Theorem)*
Let $I_1, \ldots, I_n$ be ideals in a ring R, which are pairwise coprime.
Then

(i) $I_1 \cdots I_n = I_1 \cap \cdots \cap I_n$

(ii) The map $\phi : R \to R/I_n \times \cdots R/I_n$ given by

$$x \mapsto (x \pmod{I})_1, \ldots, x \pmod{I})_n)$$

induces a ring isomorphism

$$\frac{R}{I_1 \cdots I_m} \cong \frac{R}{I_1} \times \cdots \times \frac{R}{I_n}$$

Proof. (i) We will use induction on $n \geq 2$. For the base case, we know that $I_1 \cdot I_2 \subseteq I_1 \cap I_2$. Conversely, suppose $y \in I_1 \cap I_2$. Since $I_1 + I_2 = R$, we can write

$1 = x_1 + x_2$, with $x_i \in I_i$. So

$$\begin{aligned} y &= y \cdot 1 \\ &= y \cdot (x_1 + x_2) \\ &= \underbrace{y}_{\in I_2} \cdot \underbrace{x_1}_{\in I_1} + \underbrace{y}_{\in I_1} \cdot \underbrace{x_2}_{\in I_2} \\ &\in I_1 \cdot I_2 \end{aligned}$$

Now suppose $n > 2$ and we have $I_1 \cdots I_{n-1} = I_1 \cap \cdots \cap I_{n-1}$.

Let $J = I_1 \cdots I_n$. By hypothesis, for $i = 1, \ldots, n-1$, we have $I_i + I_n = R$, so $1 = \underbrace{x_i}_{\in I_i} + \underbrace{y_i}_{\in I_n}$

So $J \ni x_1 \cdots x_{n-1} = (1 - y_1) \cdots (1 - y_{n-1}) = (1 -$some element in $I_n) \equiv 1 \pmod{I}_n$

Notation: We write $x \equiv y \pmod{I}$ if $x - y \in I$ for some $x, y \in R$, $I \subset R$.

Thus we have $1 = ($ element of $J) + ($ element of $I_m)$, so $R = J + I_n$, so J and I_n are coprime.

By the base case, we have

$$\underbrace{J \cdot I_n}_{=I_1 \cdots I_{n-1} \cdot I_n} = \underbrace{J \cap I_n}_{=(I_1 \cap \cdots \cap I_{n-1}) \cap_n}$$

We have thus proven part (i).

(ii) $\phi : R \to \frac{R}{I_1} \times \cdots \times \frac{R}{I_m}$ is clearly a ring homomorphism, since every component of ϕ is.

To show ϕ is surjective, we will show that there exists some $x \in R$ such that $\phi(x) = (1, 0, \ldots, 0)$.

A similar argument would show that there exists $x_i \in R$ such that $\phi(x_i) = \overbrace{(0, \ldots, \underbrace{1}_{i\text{th slot}}, \ldots, 0)}^{\overset{\text{def}}{=} e_i}$ and then given any $r = (\overline{r}_1, \ldots, \overline{r}_m) \in \frac{R}{I_1} \times \cdots \times \frac{R}{I_n}$, we have

$$\phi\left(\sum_{i=1}^{n} r_i x_i\right) = \sum_{i=1}^{n} \overline{r}_i \phi(x_i) = \sum_{i=1}^{n} \overline{r}_i e_i = (\overline{r}_1, \ldots, \overline{r}_m) = r$$

So we will now show surjectivity. For $i = 2, \ldots, n$, we have $I_1 + I_i = R$, so $1 = \underbrace{u_i}_{\in I_1} + \underbrace{v_i}_{\in I_i}$.

Then

$$x \overset{\text{def}}{=} v_2 \cdots v_n = (1-u_2)\cdots(1-u_n) \equiv \begin{cases} 1 & \pmod{I}_1 \\ 0 & \pmod{I}_i, i \geq 2 \end{cases}$$

So $\phi(x) = (1, 0, \ldots, 0) \in \frac{R}{I_1} \times \cdots \times \frac{R}{I_n}$. Thus we have shown surjectivity of ϕ.

Finally,

$$\begin{aligned} \ker(\phi) &= \{x \in R \mid x \pmod{I}_i \equiv 0 \forall i\} \\ &= \{x \in R \mid x \in I_i \forall i\} \\ &= \cap_{i=1}^{n} I_i = I_1 \cdots I_n \end{aligned}$$

So by the first isomorphism theorem for rings (exercise), ϕ induces the claimed isomorphism.

This completes the proof.

■

Lecture 6, 1/23/23

Extension and contraction of ideals

Definition 0.14. Let $f : R \to S$ be a ring homomorphism, and $I \subset R$ and $J \subset S$ be ideals.

- The contraction of J is the ideal

$$J^c = f^{-1}(J) \subset R.$$

- The extension of I is the ideal generated by $f(I)$:

$$I^e = (f(I)) = \{\sum_{i=1}^{n} s_i f(x_i) \mid n \in \mathbb{N}, s_i \in S, x_i \in I\} \subset S$$

Remark. **1.** If $I \subset R$ is an ideal, then $f(I) \subset S$ is not necessarily an ideal. For example, consider the inclusion $f : \mathbb{Z} \hookrightarrow \mathbb{Q}$, then $f(\underbrace{(n)}_{\neq 0}) = (n) = n\mathbb{Z} \subset \mathbb{Q}$ is not an ideal.

2. If $J \subset S$ is a prime ideal, then so is $J^c \subset R$: indeed, the composition

$$R \xrightarrow{f} S \xrightarrow{\phi} S/J$$

has the kernel $f^{-1}(J) = J^c$, so it induces an injection

$$R/J^c \hookrightarrow S/J$$

S/J is an integral domain, so R/J^c must be as well

3. If $I \subset R$ is a prime ideal, then $I^e \subset J$ is <u>not</u> necessarily a prime ideal. For example, consider $f : \mathbb{Z} \hookrightarrow \mathbb{Q}$ and $I = (\underbrace{p}_{\text{prime}})$, we have $I^e = (p\mathbb{Z}) = \mathbb{Q}$, so is not prime.

4. Any ring homomorphism $f : R \to S$ can be factored as

$$R \xrightarrow{\phi} f(R) \xhookrightarrow{\iota} S$$

Note that by first isomorphism theorem, $f(R) \cong R/\ker(f)$.

- For ϕ, we know that there is a bijection between the prime ideals in R containing $\ker(f)$ and the prime ideals in $f(R)$ by the correspondence theorem.
- For the inclusion map, the situation is more complicated.

  Example 0.6. Consider $\mathbb{Z} \hookrightarrow \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$. Then a prime ideal $(p) \subset \mathbb{Z}$ may or may not stay prime in $\mathbb{Z}[i]$.

  (i) If $p \equiv 1 \pmod 4$, then $(p)^e$ is the product of two prime ideals in $\mathbb{Z}[i]$ (e.g $(5)^e = (2 + i)(2 - i)$).
  (ii) If $p \equiv 3 \pmod 4$, then $(p)^e$ is a prime ideal in $\mathbb{Z}[i]$.
  (iii) $(2)^e = (1 + i)^2$, the square of a prime ideal in $\mathbb{Z}[i]$.

Proposition 7. *Let $f : R \to S$ be a ring homomorphism, and $I \subset R, J \subset S$ ideals. Then:*

1. *$I \subset (I^e)^c$ and $J \supset (J^c)^e$.*

2. *$I^e = I^{ece}$ and similarly $J = J^{cec}$.*

3. *Let $C = \{$contracted ideals (from S) in $R\}$ and $E = \{$extended ideals (from R) in $S\}$. Then we have*

$$\begin{aligned} C &= \{I \subset R \mid I^{ec} = I\} \\ E &= \{J \subset S \mid J^{ce} = J\} \\ |C| &= |E| \end{aligned}$$

The last line says that C, E are in bijection, with $C \to E$ acting by $I \mapsto I^e$, and $E \to C$ acting by $J \mapsto J^c$.

Proof. **1.** We have $I \ni x \in f^{-1}(\overbrace{f(x)}^{\in I^e})$ so $I \subset I^{ec}$. On the other hand, let $y \in J^{ce}$. We can write $y = \sum_i s_i f(x_i)$, $s_i \in S, x_i \in J^c = f^{-1}(J)$. So $J^{ce} \subset J$.

2. Immediate from part (1): $I \subset I^{ec} \implies I^e \subset I^{ece} = (I^e)^{ce} \subset I^e$, so $I^e = I^{ece}$. A similar argument gives $J^c = J^{cec}$.

3. Suppose $I \in C$ is a contracted ideal. Then $I = J^c$ for some ideal $J \subset S$. Then $I^{ec} = J^{cec} = J^c = I$, so $C \subset \{I \subset R \mid I^{ec} = I\}$. Conversely, every ideal in $\{I \subset R \mid I^{ec} = I\}$ is a contracted ideal, so we get equality.

Similarly, we see that $E = \{J \subset S \mid J^{ec} = J\}$

■

Lecture 7, 1/25/23

Ring of fractions and localization

Motivation: Recall how we construct $\mathbb{Q}$ from $\mathbb{Z}$. We take all ordered pairs $(a, s), a, s \in \mathbb{Z}, s \neq 0$, and set up the equivalence relation $(a, s) \sim (b, t)$ if $at = sb$. Then $\mathbb{Q} \overset{\text{def}}{=} \{$ all such equivalence classes$\}$

Definition 0.15. Let R be a commutative ring with 1. A multiplicative set $S \subseteq R$ is a subset of R which contains 1 and is closed under multiplication. That is, $1 \in S$, and $s, t \in S \implies st \in S$.

Example 0.7.

1. If $\mathfrak{p} \subset R$ is a prime ideal, then $S = R \setminus \mathfrak{p}$ is a multiplicative sets.

2. If R is an integral domain then $S = R \setminus \{0\}$ is a multiplicative set.

3. For any $f \in R$, $S = \{1, f, f^2, \dots\}$ is a multiplicative set.

Let $S \subset R$ be a multiplicative set, and define the relation

$$(a, s) \sim (\ell, t) \iff (at - sb)u = 0$$

for some $u \in S$.
Exercise: Show that this is indeed an equivalence relation.

Definition 0.16. Let $\frac{a}{s}$ denote the equivalence class of $(a, s) \in R \times S$. Then

$$S^{-1}R \overset{\text{def}}{=} \{\frac{a}{s} \mid (a, b) \in R \times S\}$$

with addition and multiplication defined by

$$\frac{a}{s} + \frac{\ell}{t} \stackrel{\text{def}}{=} \frac{at + s\ell}{st}$$
$$\frac{a}{s} \cdot \frac{\ell}{t} \stackrel{\text{def}}{=} \frac{a\ell}{st}$$

We say that $S^{-1}R$ is the ring of fractions of R with respect to S, or alternatively the localization of R at S.

Note: We have a ring homomorphism $f : R \to S^{-1}R$ acting by

$$r \mapsto \frac{r}{1}$$

such that $f(s)$ is a unit in $S^{-1}R$ for all $s \in S$, since $\frac{1}{s} \in S^{-1}R$, and $\frac{1}{s}\frac{s}{1} = 1$.

Proposition 8. (Universal property of $S^{-1}R$)
Let $g : R \to R'$ be a ring homomorphism such that $g(s)$ is a unit in R' for all $s \in S$. Then there exists a unique ring homomorphism $h : S^{-1}R \to R'$ such that the diagram

$$\begin{tikzcd} R \arrow[r, "g"] \arrow[d, "f"'] & R' \\ S^{-1}R \arrow[ur, dotted, "\exists! h"'] & \end{tikzcd}$$

commutes.

Proof. Suppose first that such h exists. Then for any $r \in R$,

$$h(\frac{r}{1}) = h(f(r)) = g(r)$$

so for any $s \in S$,

$$h(\frac{1}{s}) = h((\frac{s}{1})^{-1}) = h(\frac{s}{1})^{-1} = h(f(s))^{-1} = g(s)^{-1}$$

So for $\frac{r}{s} \in S^{-1}R$, we must have

$$h(\frac{r}{s}) = h)(\frac{r}{1})h(\frac{1}{s}) = g(r)g(s)^{-1}$$

To prove the existence of h, set $h(\frac{r}{s}) \stackrel{\text{def}}{=} g(r)g(s)^{-1}$. Then h will be a ring homomorphism satisfying $g = h \circ f$, so long as h is well-defined, so we will check that now.

Suppose $\frac{r}{s} = \frac{r'}{s'}$. Then by definition $(rs' - r's)u = 0$ for some $u \in S$. So $(g(r)g(s') - g(r')g(s))g(u) = g(0) = 0$. $g(u) \in (R')^\times$, so is not a zero divisor, so $g(r)g(s') - g(r')g(s) = 0$, so $g(r)g(s)^{-1} = g(r')g(s')^{-1}$.

■

Example 0.8. Let $\mathfrak{p} \subset R$ be a prime ideal, and $S = R \setminus \mathfrak{p}$ (a multiplicative set). Then we write $R_\mathfrak{p}$ for $S^{-1}R$, and call it the localization of R at $\mathfrak{p}$.

<u>Note:</u> The set ${}_\mathfrak{p}R_\mathfrak{p} \overset{\text{def}}{=} \{\frac{a}{s} \mid a \in \mathfrak{p}, s \in S\} \subset R_\mathfrak{p}$ is a proper ideal in $R_\mathfrak{p}$, and

$$\frac{a}{s} \notin_\mathfrak{p} R_\mathfrak{p} \implies a \notin \mathfrak{p}$$

So $\frac{s}{a} \in R_\mathfrak{p}$, so $\frac{a}{s}$ is a unit in $R_\mathfrak{p}$.

So $R_\mathfrak{p}$ is a local ring, with ${}_\mathfrak{p}R_\mathfrak{p}$ the unique maximal ideal by a lemma from lecture 4.

Example 0.9. If $R = \mathbb{Z}$, $\mathfrak{p} = (p)$ with p a prime, then $\mathbb{Z}_{(p)} = \{\frac{a}{s} \mid p \nmid s\} \subset \mathbb{Q}$

8, 1/27/23

Proposition 9. *Let $S \subset R$ be a multiplicative subset of a ring R, and $f : R \to S^{-1}R$ the corresponding localization, sending r to $\frac{1}{r}$. Then*

(i) Every ideal in $S^{-1}R$ is extended.

(ii) An ideal $I \subset R$ is contracted iff for all $s \in S$, $\overline{s} \in \frac{R}{I}$ is NOT a zero divisor.

(iii) We have a bijection between the prime ideals in $S^{-1}R$ and the prime ideals of R which are disjoint from S. This bijection is given by extension and contraction.

Proof. (i) Let $J \subset S^{-1}R$ be an ideal. We want to show that J is extended, so it is enough to show $J \subset J^{ce}$.

Pick $\frac{r}{s} \in J$. Then $\frac{r}{1} = \frac{s}{1} \cdot \frac{r}{s} \in J$, so $r \in f^{-1}(J) = J^c$. We can then write $\frac{r}{s} = \frac{1}{s} \cdot \frac{r}{1} \in J^{ce}$.

(ii) Let $I \subset R$ be an ideal. It is enough to show

$$(I^{ec} \subset I) \iff \forall s \in S, \overline{s} \in \frac{R}{I} \text{ is not a zero divisor}$$

Let $x \in I^{ec} = f^{-1}(I^e)$. Then

$$\begin{aligned} f(x) \in I^e &= \{\text{all finite linear combinations } \sum_i \frac{r_i}{s_i} \overbrace{f(x_i)}^{=\frac{x_i}{1}} \mid r_i \in R, s_i \in S, x_i \in I\} \\ &= \{\frac{r}{s} \mid r \in I, s \in S\} \\ &\stackrel{\text{def}}{=} S^{-1}I \end{aligned}$$

So $\frac{x}{1} = \frac{r}{s}$ for some $r \in I, s \in S$, so $(xs - r)u = 0$ for some $u \in S$, so $x \underbrace{su}_{\in S} = \underbrace{ru}_{\in I}$. So $\overline{x} \cdot \overline{su} = \overline{0} \in \frac{R}{I}$.

Note: If $su \in I$, then $\frac{su}{1}$ is a unit in I^e. So $I^e = S^{-1}R$, so $I^{ec} = R$.

If $\overline{su} \neq \overline{0} \in \frac{R}{I}$ (i.e. $su \notin I$) then by hypothesis on elements in S, $\overline{x} = 0 \in \frac{R}{I}$, i.e. $x \in I$, so $I^{ec} \subset I$.

Now for the converse.

Suppose there exists $s \in S$ such that $\overline{s} \in \frac{R}{I}$ is a zero divisor. We want to show that I is not contracted, i.e. there exists an $x \in I^{ec} \setminus I$.

By hypothesis, there exists $\overline{x} \neq \overline{0} \in \frac{R}{I}$ (i.e. $x \notin I$) such that $\overline{x} \cdot \overline{s} = \overline{0} \in \frac{R}{I}$. So $xs = y$ for some $y \in I$, so $\frac{x}{1} = \frac{y}{s} \in S^{-1}I = I^e$. So $x \in f^{-1}(I^e) = I^{ec}$.

(iii) Suppose $\mathfrak{q} \subset S^{-1}R$ is a prime ideal. Then, by part (i), $\mathfrak{q} = S^{-1}\mathfrak{p} = \mathfrak{p}^e$ for some ideal $\mathfrak{p} \subset R$. So $\mathfrak{q}^c = \mathfrak{p}^{ec} \supset \mathfrak{p}$.

Claim. $\mathfrak{p}^{ec} \subset \mathfrak{p}$.

Proof. Indeed, we have $\mathfrak{p} \cap S = \varnothing$, since $s \in \mathfrak{p} \cap S$ implies $1 = \frac{s}{s} \in S^{-1}\mathfrak{p} = \mathfrak{q}$, so $s \notin \mathfrak{p}$ for all $s \in S$. So, $\overline{s} \neq \overline{0} \in \frac{R}{\mathfrak{p}}$ for all $s \in S$.

So $\overline{s}$ is not a zero divisor in $\frac{R}{\mathfrak{p}}$ (because it's an integral domain), so $\mathfrak{p}^{ec} \subset \mathfrak{p}$, as shown in proof of part (ii).

■

Thus $\mathfrak{q} = S^{-1}\mathfrak{p}, \mathfrak{p} = \mathfrak{q}^c$, and $\mathfrak{p} \cap S = \varnothing$, so we get an injection

$$\{\text{prime ideals } \mathfrak{p} \subset R \text{ with } \mathfrak{p} \cap S = \varnothing\} \hookleftarrow \{\text{prime ideals in } S^{-1}R\}$$

given by

$$\mathfrak{q} = S^{-1}\mathfrak{p} \mapsto \mathfrak{q}^c = \mathfrak{p}$$

Conversely, let $\mathfrak{p} \subset R$ be a prime ideal with $\mathfrak{p} \cap S = \varnothing$ (we want to show that $\mathfrak{p}^e = S^{-1}\mathfrak{p}$ is a prime ideal in $S^{-1}R$).

Let $\overline{S} = \{\overline{s} \in \frac{R}{\mathfrak{p}} \mid s \in S\} \subset \frac{R}{\mathfrak{p}}$. This is a multiplicative subset. Then the ring homomorphism $S^{-1}R \to \overline{S}^{-1}(\frac{R}{\mathfrak{P}})$ given by $\frac{r}{s} \mapsto \frac{\overline{r}}{\overline{s}}$ induces an isomorphism

$$\frac{S^{-1}R}{S^{-1}\mathfrak{p}} \to \overline{S}^{-1}(\frac{R}{\mathfrak{p}})$$

So we are done if we can show that $\overline{S}^{-1}(\frac{R}{\mathfrak{p}})$ is an integral domain.

But this follows from

- $\mathfrak{p} \cap S = \varnothing$, so $S^{-1}\mathfrak{p} \subsetneq S^{-1}R$, so $\overline{S}^{-1}(\frac{R}{\mathfrak{p}}) \neq (0)$
- $\overline{S}^{-1}(\frac{R}{\mathfrak{p}}) \hookrightarrow$ field of fractions of the integral domain $\frac{R}{\mathfrak{p}}$ (see next remark).

This concludes the proof.

■

Remark. Suppose R is an integral domain. Then $S = R \setminus \{0\}$ is a multiplicative set. We call $S^{-1}R$ the field of fractions of R.

1. $S^{-1}R$ is a field, since $\frac{r}{s} \neq 0 \in S^{-1}R$, so $r \neq 0$, i.e. $r \in S$, so $\frac{s}{r} \in S^{-1}R$,so $\frac{r}{s}$ is a unit in $S^{-1}R$.

2. The map $f : R \to S^{-1}R$, $r \mapsto \frac{r}{1}$, is injective.

Lecture 9, 1/30/23

Definition 0.17. Let R be a commutative ring with identity. An Abelian group M is called an R-module if there is a function $R : M \times M \to M$, with $(r, m) \mapsto r \cdot m$, such that, for all $r_1, r_2, r \in R, m_1, m_2, m \in M$,

1. $r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2$

2. $(r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m$

3. $(r_1 r_2) \cdot m = r_1 \cdot (r_2 \cdot m)$

4. $1 \cdot m = m$.

Example 0.10. Let R be as above.

1. R is an R-module via the map given by multiplication.

2. Let I be an ideal. I is an R-module, again via multiplication.

3. If V is a vector space over a field F, then V is an F-module.

4. Let G be an Abelian group. Then G is a $\mathbb{Z}$-module via the multiplication

$$n \cdot g = \begin{cases} g + \cdots + g \, (n \text{ times}) & n > 0 \\ e & n = 0 \\ (-g) + \cdots + (-g) \, (|n| \text{ times}) & n < 0 \end{cases}$$

5. let V be a vector space over a field F and let $\theta : V \to V$ be an F-linear map. Then we can regard V as an $F[x]$-module via $F[x] \times V \to V$, where

$$(\sum a_i x_i, v) \mapsto \sum_i a_i \theta^i(v)$$

Proposition 10. *Let M be an R-module. Then*

1. $0 \cdot m = 0 = r \cdot 0$

2. $-r \cdot m = r \cdot (-m) = -(r \cdot m)$.

Proof. Immediate ∎

Remark. If M is an R-module, then $\operatorname{Ann}_R(M) = \{r \in R \mid r \cdot m = 0 \forall m \in M\} \subset R$ is an ideal of R, called the annihilator of M, and M is naturall an $R/\operatorname{Ann}_R(M)$-module via $R/\operatorname{Ann}_R(M) \times M \to M$ by $(\overline{r}, m) \mapsto r \cdot m$.

Definition 0.18. Let M be an R-module. A subgroup N of the additive group of M is called a submodule if for all $r \in R, n \in N$, we have $r \cdot n \in N$.

Proposition 11. *A subset $N \subseteq M$ is a submodule if it satisfies*

1. $N \neq \varnothing$

2. $n_1, n_2 \in N \implies n_1 + n_2 \in N$

3. *For all $r \in R, n \in N, r \cdot n \in N$*

Proof. Exercise ∎

Example 0.11. **1.** If R is a commutatie ringr egarded as an R-module, then $\{R$-submodules of $R\} = \{\text{ideals of } R\}$.

2. If V is a vector space over a field F, then $\{$ submodules of $V\} = \{$subspaces of $V\}$.

3. If G is an Abelian group regarded as a $\mathbb{Z}$-module, then $\{\mathbb{Z}$-submodules of $G\} = \{$subgroups of $G\}$.

4. If V is a vector space over a field F with endomorphism $\theta : V \to V$ (i.e. V is an $F[x]$-module), then $\{F[x]$-submodule of $V = \{\theta$-invariant subspace $W \subseteq V\}$

Definition 0.19. Let M, N be R-modules. A group homomorphism $\theta : M \to N$ is called a module homomorphism (or R-homomorphism) if $\theta(r \cdot m) = r \cdot \theta(m)$ for all $r \in R, m \in M$.
Notation: $\mathrm{Hom}_R(M, N) = \{$ All R-homomorphisms $\theta : M \to N\}$.
$\mathrm{Hom}_R(M, N)$ is an R-module, where $R \times \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M, N)$ is defined by

$$(r, \theta) \mapsto \{r \cdot \theta : m \to r[\theta(m)]\}$$

Example 0.12.

1. If V, W are F-vector spaces, then $\{F$-homomorphisms $\theta : V \to W\} = \{F$-linear maps $V \to W\}$.

2. If G, H are groups, then $\{\mathbb{Z}$-homomorphisms $\theta : G \to H\} = \{$group homomorphisms $\theta : G \to H\}$.

Proposition 12. *If $\theta : M \to N$ is an R-homomorphism, then*

1. $\mathrm{Im}(\theta) = \theta(M) \subseteq N$ *is an R-module.*

2. $\ker(\theta) = \theta^{-1}(\{0\}) \subseteq M$ *is an R-module*

Proof. Immediate.

■

Definition 0.20. If $N \subseteq M$ is a submodule, then the quotient Abelian group $M/N = \{\overline{m} = m + N \mid m \in M\}$ can be made into an R-module via $R \times M/N \to M/N$ defined by $(r, \overline{m}) \to \overline{r \cdot m}$. We say M/N is a quotient module. The quotient map $\theta : M \to M/N$ where $\theta(m) = \overline{m}$ is then an R-homomorphism.

Theorem 0.5. *(1st isomorphism theorem)*
If $\theta : M \to N$ is an R-module homomorphism, then θ induces an R-module isomorphism $M/\ker(\theta) \cong \mathrm{Im}(\theta)$.

Proof. Exercise

■

Lecture 10, 2/1/23

Definition 0.21. Let M be an R-module an $A \subseteq M$ then the smallest submodule of M generated by A is $\langle A \rangle = \cap_{A \subseteq N \subseteq M} N \equiv_{\text{exercise}} \{$all finite linear combinations $\sum_i \lambda_i a_i \mid \lambda_i \in R, a_i \in A\}$.

Definition 0.22. An R-module M is finitely generated if it's of the forem $M = \langle A \rangle$ for some finite $A \subseteq M$.

Definition 0.23. An R-module M is free with basis $A \subseteq M$ is

1. $M = \langle A \rangle$

2. $\sum_i \lambda_i a_i = 0$ with distinct $\lambda_i \in R, a_i \in A \implies \lambda_i = 0$ for all i (linearly independent). In other words, every $m \in N$ can be uniquely written in the form $m = \sum_i \lambda_i a_i$ with $\lambda_i \in R, a_i \in A$ distinct.

Example 0.13.

1. R is a free R-module with basis $\{1\}$.

2. Similarly, R^n is a free R-module with basis $\{e_i \mid 1 \leq i \leq n\}$, where e_i is the standard vector with a 1 in the ith spot.

3. More generally, for any set A, the module $R^{(A)} = \{$all functions $f : A \to R$ with $f(a) = 0$ for all but finitely many $a\}$ is free with basis $\{\delta_a\}_{a \in A}$, where $\delta_a : A \to R$ is defined by $\delta_a(m) = \begin{cases} 1 & m = a \\ 0 & \text{otherwise} \end{cases}$

Remark. An R-module M is free with basis A if aned only if $M \cong R^{(A)}$.

Example 0.14.

1. If F is a field, then every finitely generated F-module is free.

2. $\mathbb{Z}_2$ is not a free $\mathbb{Z}$-modulek since $\mathbb{Z}_2$ is generated by 1, but we have $1 = 1 \cdot 1 = 3 \cdot 1 \in \mathbb{Z}_2$.

Remark. Suppose M is a free R-module with basis $A \subseteq M$. Let N be another R-module. Then any function $f : A \to N$ extends uniquely to an R-homomorphism $\varphi : M \to N$ where $f\varphi(\sum_i \lambda_i a_i) = \sum_i \lambda_i f(a_i)$. Note $\varphi(a) = f(a)$ for all $a \in A$.

Proposition 13. *Suppose we have the diagram of R-modules and R-homomorphisms θ, ϕ, where free R-module and ϕ is surjective. Then there exists an R-homomorphism*

$\psi : L \to N$ such that $\theta = \phi \circ \psi$. In other words, there is a ψ making this diagram commute:

$$\begin{tikzcd} & L \arrow[dl, dotted, "\exists\psi"'] \arrow[d, "\theta"] \\ N \arrow[r, "\phi"] & N \end{tikzcd}$$

Proof. Let A be a basis for L. Since ϕ is injective, for $a \in A$, there exists $n_a \in N$ such that $\phi(n_a) = \theta(a)$. Then by the preceeding remark, $f : A \to N$ defined by $f(a) = n_a$ can be extended uniquely to an R-homomorphism $\psi : L \to N$ by $\sum_i \lambda_i a_i \mapsto \sum_i \lambda_i n_{a_i}$.
By construction, for any $m = \sum_i \lambda_i a_i \in L$,

$$\begin{aligned} \theta(m) &= \theta(\sum_i \lambda_i a_i) \\ &= \sum_i \lambda_i \theta(a_i) \\ &= \sum_i \lambda_i \phi(n_{a_i}) \\ &= \sum_i \lambda_i (\phi \circ \psi)(a_i) \\ &= (\phi \circ \psi)(\sum_i \lambda_i a_i) \\ &= (\phi \circ \psi(m)) \end{aligned}$$

Thus $\phi \circ \psi = \theta$.

■

Remark. The result of prop 1 doesn't necessarily hold if L is not free, e.g. consider the following $\mathbb{Z}$-modules

$$\begin{tikzcd} & \mathbb{Z}_2 \arrow[dl, "\exists\psi?"'] \arrow[d, "\theta=\mathrm{Id}"] \\ \mathbb{Z} \arrow[r, "n\to\overline{n}"'] & \mathbb{Z}_2 \end{tikzcd}$$

Suppose $\psi : \mathbb{Z}_2 \to \mathbb{Z}$ is a $\mathbb{Z}$-linear map. Let $n = \psi(1) \in \mathbb{Z}$. Then $2n = 2\psi(1) = \psi(2 \cdot 1) = \psi(\overline{0}) = 0 \in \mathbb{Z} \implies n = 0$. Thus $\psi = 0$, so $\phi \circ \psi \neq \mathrm{Id}$.

Proposition 14. *Let M be an R-module. Then there exists a free L-module L such that $M \cong L/K$ for some submodule $K \subseteq L$. In other words, every module is a quotient of a free module.*

Proof. Take $A \subseteq M$ to be a generating set for M, i.e. $M = \langle A \rangle$. Consider the free R-module $R^{(A)}$ and let $\theta : L \to M$ be the unique R-linear extension of the inclusion $A \hookrightarrow M$. Then θ is surjective, since A generates M. By the 1st isomorphism theorem, $L/\ker(\theta) \cong M$. ∎

Lecture 11, 2/3/23

Definition 0.24. A sequence of R-modules and R-homomorphisms

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

is called <u>exact at M_i</u> if $\mathrm{Im}(f_{i-1}) = \ker(f_i)$, and called exact if it's exact at M_i for all i. In particular,

1. $(0) \longrightarrow M' \xrightarrow{f} M$ is exact $\iff$ f injective.

2. $M \xrightarrow{g} M' \longrightarrow 0$ is exact $\iff$ g surjective.

3. $0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ is exact iff

   (i) f injective
   (ii) g surjective
   (iii) $\mathrm{Im}(f) = \ker(g)$

   Such an exact sequence is called a short exact sequence.

Example 0.15. If $f : M \to N$ is an R-homomorphism, then

$$0 \longrightarrow \ker(f) \xhookrightarrow{\iota} M \xrightarrow{f} \mathrm{Im}(f) \longrightarrow 0$$

is a short exact sequence.

Remark. Any exact sequence $\cdots \longrightarrow M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \longrightarrow \cdots$ can be decomposed into short exact sequences

$$\begin{tikzcd}
 & & (\mathrm{Im}(f_i) = \ker(f_{i+1})) \arrow[dr] & & & & \\
\cdots \arrow[r] & M_{i-1} \arrow[rr, "f_{i-1}"] \arrow[ur] & & M_i \arrow[rr, "f_i"] \arrow[dr] & & M_{i+1} \arrow[r] & \cdots \\
0 \to \ker(f_i) \arrow[ur] & & & & \mathrm{Im}(f_{i+1} = \ker(f_{i+2})) \arrow[r] & 0 &
\end{tikzcd}$$

Proposition 15. *Let* Hom *be a left-exact functor.*

1. *Let* $0 \longrightarrow N' \xrightarrow{f} N \xrightarrow{g} N'' \longrightarrow 0$ *be an exact sequence. Then for any R-module M, the sequence*

$$0 \longrightarrow N' \xrightarrow{f} N \xrightarrow{g} N''$$

is exact, with $\overline{f}(\phi) = f \circ \phi, \overline{g}(\psi) = g \circ \psi$.

2. *Let* $M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ *be an exact sequence. Then for any R-module N, the sequence*

$$0 \longrightarrow \mathrm{Hom}_R(M'', N) \xrightarrow{\overline{g}} \mathrm{Hom}_R(M, N) \xrightarrow{\overline{f}} \mathrm{Hom}_R(M, N'')$$

is also exact.

Proof. We will prove 1.

Suppose $0 \longrightarrow N' \xrightarrow{f} N \xrightarrow{g} N''$ is exact.
We first show $\overline{f}$ is injective. Suppose $\phi \in$ Hom)$R(M, N')$ such that $f \circ \phi = \overline{f}(\phi) = 0$.
Then $\mathrm{Im}(\phi) \subseteq \ker(f) = 0$, so $\theta = 0$.
We now show $\mathrm{Im}(f) = \ker(g)$. Let $\phi \in \mathrm{Hom}_R(M, N')$. Then $(\overline{f} \circ \overline{g})(\phi) = g \circ f \circ \phi = 0 \circ \phi = 0$ (because $\ker(g) \subseteq \mathrm{Im}(f)$, so $\overline{g} \circ \overline{f} = 0$, i.e. $\mathrm{Im}(\overline{f}) \subseteq \ker(\overline{g})$.
Conversely, let $\psi \in \ker(\overline{g})$. Then $g \circ \psi = 0$, so $\mathrm{Im}(\psi) \subseteq \ker(g) = \mathrm{Im}(f)$ by exactness.

$$\begin{tikzcd}
 & M \ni m \arrow[dl, dotted, "\exists\phi"'] \arrow[d, "\psi"] \\
N' \arrow[r, "f"] & N \ni \psi(m) = f(n')
\end{tikzcd}$$

There exists a unique n' such that $f(n') = \psi(m)$ by exactness.
Now define $\phi : M \to N'$ by $\phi(m) = n'$. Then

- ϕ is well-defined
- ϕ is R-linear, since so are ψ and f
- ϕ satisfies $f \circ \phi = \psi$ by construction

Thus $\psi = \overline{f}(\phi)$, i.e. $\psi \in \operatorname{Im}(\overline{f})$. This concludes the proof of 1. The proof of 2 is similar.

■

Remark. In the context of part 1 of the proposition, suppose $0 \longrightarrow N' \xrightarrow{f} N \xrightarrow{g} N''$ is exact, as well as that g is surjective. Then for general R-modules M we (obviously) have

$$0 \longrightarrow \operatorname{Hom}_R(M, N') \xrightarrow{\overline{f}} N \xrightarrow{g} N'' \longrightarrow 0$$

is exact, but $\overline{g}$ is not necessarily surjective.

Example 0.16. For $M = \mathbb{Z}_2$ and $\left(N \xrightarrow{g} N'' \right) = \left(\substack{\mathbb{Z} \to \mathbb{Z}_2 \\ n \mapsto \overline{n}} \right)$, last time we say that $(\mathrm{Id} : \mathbb{Z}_2 \to \mathbb{Z}_2) \notin \operatorname{Im}(\overline{g})$.

$$\begin{tikzcd} & \mathbb{Z}_2 \arrow[d, "\mathrm{Id}"] \\ \mathbb{Z} \arrow[r, "g"] & \mathbb{Z}_2 \end{tikzcd}$$

Similarly, in the context of part 2 of the proposition,
$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ exact does not imply $\overline{f} : \operatorname{Hom}_R(M, N) \to \operatorname{Hom}_R(M', N)$ surjective for general R-modules.

Lecture 12, 2/6/23

Lecture 13, 2/8/23

On $\operatorname{Hom}_R(-, N)$

Recall: If N is an R-module and

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

is an exact sequence, then the sequence

$$\operatorname{Hom}_R(M'', N) \xrightarrow{\overline{g}} \operatorname{Hom}_R(M, N) \xrightarrow{\overline{f}} \operatorname{Hom}_R(M', N)$$

is exact. However, f injective does not imply $\overline{f}$ is surjective for general N.

Definition 0.25. An R-module is called injective if it satisfies any of the three equivalent (we prove they are equivalent next) conditions:

(i) For every such diagram of R-modules and R-homs,

$$\begin{tikzcd} 0 \arrow[r] & M' \arrow[r, "f"] \arrow[d, "\phi"] & M \\ & Q & \end{tikzcd}$$

with f injective, there is a $\psi : M \to Q$, that makes the following diagram commute

$$\begin{tikzcd} 0 \arrow[r] & M' \arrow[r, "f"] \arrow[d, "\phi"] & M \arrow[dl, dotted, "\exists\psi"] \\ & Q & \end{tikzcd}$$

(ii) For every injective R-homomorphism $f : M' \to M$, the induced map $\overline{f}$: $\mathrm{Hom}_R(M, Q) \to \mathrm{Hom}_R(M', Q)$, $\psi \mapsto \psi \circ f$ is surjective.

(iii) Every short exact sequence

$$0 \longrightarrow Q \xrightarrow{\alpha} M \longrightarrow N \longrightarrow 0$$

splits on the left. That is, there is a $\beta : M \to A$ such that $\beta \circ \alpha = \mathrm{Id}_Q$ (So $M \cong Q \oplus N$)

Theorem 0.6. *These three conditions are indeed equivalent.*

Proof. Exercise ■

Lemma 3. *(Baer's Criterion)*
Let Q be an R-module. If for all ideals $I \subset R$ every R-homomorphism $\phi : I \to Q$ extends to an R-homomorphism $\psi : R \to Q$,

$$\begin{tikzcd} I \arrow[r, hook, "\iota"] \arrow[d, "\phi"'] & R \arrow[dl, dotted, "\psi"] \\ Q & \end{tikzcd}$$

Then Q is an injective R-module.

Proof. Consider a diagram of R-modules and R-homomorphisms

$$\begin{tikzcd} 0 \arrow[r] & M' \arrow[r, "f"] \arrow[d, "\phi"'] & M \\ & Q & \end{tikzcd}$$

If f is an injection, then $M' \cong f(M')$. We want to show that there exists $\psi : M \to Q$ such that $\phi = \psi \circ f$. Without loss of generality, assume $M' \subseteq M$ and $f = \iota$.
Consider the set $\mathcal{A} = \{$all R-submodules N of M with $M' \subset N \subset M$, such that there exists an R-homomorphism $\phi_N : N \to Q$ with $\phi_N|_{M'} = \phi\}$.
We order the set as follows. We say $N_1 \leq N_2$ if $N_1 \subset N_2$ and $\phi_{N_2}|_{N_1} = \phi_{N_1}$. Because $M' \in \mathcal{A}, \mathcal{A} \neq \varnothing$. Further, it is clear that every chain in $\mathcal{A}$ has an upper bound.
By Zorn's lemma, there exists some maximal element N in $\mathcal{A}$. If $N = M$, we're done.
So for the sake of contradiction, suppose $N \subsetneq M$ is a proper submodule. Let $m \in M \setminus N$, and consider the ideal $I = \{r \in R \mid rm \in N\} \subset R$.
By hypothesis, the R-homomorphism $\phi_M : I \to Q$, $r \mapsto \phi_N(rm)$ extends to an R-homomorphism $\psi_m : R \to Q$:

$$\begin{tikzcd} I \arrow[r, hook, "\iota"] \arrow[d, "\phi_m"'] & R \arrow[dl, dotted, "\exists \psi_m"] \\ Q & \end{tikzcd}$$

Note that $\mathrm{Ann}_R(m) = \{r \in R \mid rm = 0\} \subset \ker \phi_m \subset \ker \psi_m$. So ψ_m factors as

$$\begin{tikzcd} & R \arrow[r, two heads] \arrow[dl, "\psi_m"'] & R/\mathrm{Ann}_R(m) & \cong Rm \arrow[dlll, dotted, "\psi'_m"] \\ Q & & & \end{tikzcd}$$

and we have $\psi'_m|_{Rm \cap N} = \phi_N|_{Rm \cap N}$ by definition.
So we can extend ϕ_N to

$$\begin{aligned} \phi_{N'} : N' &\overset{\text{def}}{=} N + Rm \to Q \\ n + r &\mapsto \phi_N(n) + \psi'_m(rm) \end{aligned}$$

but $N' \supsetneq N$, contradicting maximality of N.

■

Definition 0.26. Let G be an Abelian group. G is said to be divisible if for any $n \in \mathbb{Z} \setminus \{0\}$, the map $g \mapsto ng$ is surjective.

Proposition 16. *Let G be an Abelian group ($= \mathbb{Z}$-module). Then G is an injective $\mathbb{Z}$-module if and only if G is divisible.*

Proof. Suppose G is an injective $\mathbb{Z}$-module. Let $n \in \mathbb{Z} \setminus \{0\}, g \in G$, and consider

$$\begin{tikzcd} \mathbb{Z} \arrow[r, "g \mapsto n \cdot g"] \arrow[d, "1 \mapsto g"'] & \mathbb{Z} \arrow[dl, dotted, "\psi"] \\ G & \end{tikzcd}$$

Then there exists $\psi : \mathbb{Z} \to G$ such that $\phi = \psi \circ f$. So

$$\begin{aligned} g &= \phi(1) \\ &= \psi(f(1)) \\ &= \psi(n) \\ &= n \cdot \underbrace{\psi(1)}_{\in G} \end{aligned}$$

Now suppose G is divisible. By Baer's lemma, to check G is injective in $\mathbb{Z}$-mod, it is enough to show that for all ideals $I = (n) \subset \mathbb{Z}$ and $\phi : I \to G$, the map ϕ extends to $\mathbb{Z}$:

$$\begin{tikzcd} I = (n) \arrow[r, hook, "\iota"] \arrow[d, "\phi"'] & \mathbb{Z} \arrow[dl, dotted] \\ G & \end{tikzcd}$$

The case $n = 0$ is trivial. So suppose $n \neq 0$. Let $g = \phi(n)$. Then $g = n \cdot g'$ for some $g' \in G$.
The $\mathbb{Z}$-linear map $\psi : \mathbb{Z} \to G$ defined by $1 \mapsto g'$ extends phi.

■

Example 0.17. $\mathbb{R}, \mathbb{Q}, \mathbb{Q}/\mathbb{Z}$ are all injective $\mathbb{Z}$-modules since they are divisible.

Lecture 14, 2/10/23

Localization of modules

Let R be a commutative ring with 1, $S \subset R$ a multiplicative subset, and M an R-module.
Define the relation $\sim$ on $M \times S$ by $(m, s) \sim (m', s') \iff t(s'm - sm') = 0$ for some $t \in S$, and let $\frac{m}{s}$ =equivalence class of (m, s).
Then $S^{-1}M = \{\frac{m}{s} \mid m \in M, s \in S\}$ becomes an $S^{-1}R$-module via

$$\frac{m}{s} + \frac{m'}{s'} \stackrel{\text{def}}{=} \frac{s'm + sm'}{ss'}$$
$$\frac{r}{t} \cdot \frac{m}{s} \stackrel{\text{def}}{=} \frac{rm}{st}$$

If $f : M \to N$ is an R-homomorphism, then $S^{-1}f : S^{-1}M \to S^{-1}N$ given by $\frac{m}{s} \mapsto \frac{f(m)}{s}$ is a $S^{-1}R$ homomorphism.

Proposition 17. *If* $M' \xrightarrow{f} M \xrightarrow{g} M''$ *is a R-mod exact sequence, then*

$$S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M$$

is an $S^{-1}R$*-mod exact sequence. That is, localization is an exact functor.*

Proof. We need to show $\text{Im}(S^{-1}f) = \ker(S^{-1}g)$. We have $\text{Im}(f) = \ker(g)$, so $g \circ f = 0$. So $\underbrace{S^{-1}(g \circ f)}_{=(S^{-1}g)\circ(S^{-1}f)} = 0$. So $\text{Im}(S^{-1}f) \subseteq \ker(S^{-1}g)$. Conversely, let $\frac{m}{s} \in \ker(S^{-1}g)$. So $\frac{g(m)}{s} = 0 \in S^{-1}M''$.

So for some $t \in S$, $\overbrace{t \cdot g(m)}^{g(tm)} = 0 \in M''$. So $tm \in \ker(g) = \text{im}(f)$, so $tm = f(m')$ for some $m' \in M'$.
Therefore $\frac{m}{s} = \frac{tm}{ts} = \frac{f(m')}{ts} \in \text{Im}(S^{-1}f)$.

■

Corollary 0.7. *If* $N \subset M$ *is an* R*-submodule, then* $S^{-1}N \subset S^{-1}M$ *is an* $S^{-1}R$*-submodule, and* $\frac{(S^{-1}M)}{(S^{-1}N)} \cong S^{-1}(\frac{M}{N})$

Proof. Apply the proposition to the short exact sequence

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$$

Indeed, this tells us

$$0 \longrightarrow S^{-1}N \longrightarrow S^{-1}M \longrightarrow S^{-1}\frac{M}{N} \longrightarrow 0$$

is exact.

■

Notation: If $S = R \setminus \mathfrak{p}$ with $\mathfrak{p} \subset R$ a prime ideal, we often use $f_\mathfrak{p}, M_\mathfrak{p}$ to denote $S^{-1}f, S^{-1}M$.

Proposition 18. *Let M be an R-module. Then the following are equivalent:*

(i) $M = 0$.

(ii) $M_\mathfrak{p} = 0$ *for all prime ideals* $\mathfrak{p} \subset R$.

(iii) $M_\mathfrak{m} = 0$ *for all maximal ideals* $\mathfrak{m} \subset R$,

Proof. Clearly $(i) \implies (ii)$, and $(ii) \implies (iii)$, as maximal ideals are prime. The only thing to check is $(iii) \implies (i)$.
Suppose (iii) holds, and for the sake of contradiction that $M \neq 0$. Let $x \neq 0 \in M$. Then $I = \mathrm{Ann}_R(x) \overset{\text{def}}{=} \{r \in R \mid rx = 0\} \subset R$ is a proper ideal, so $I \subset \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$.
Then $\frac{x}{1} = 0 \in M_\mathfrak{m} \implies t \cdot x = 0$ for some $t \in R \setminus \mathfrak{m} \subset R \setminus I$.
But this means that $t \in I$!! Contradiction.

■

Corollary 0.8. *Let $f : M \to N$ be an isomorphism. Then the following are equivalent:*

(i) f *is injective.*

(ii) $f_\mathfrak{p} : M_\mathfrak{p} \to N_\mathfrak{p}$ *is injective for all prime ideals* $\mathfrak{p} \subset R$.

(iii) $f_\mathfrak{m} : M_\mathfrak{m} \to N_\mathfrak{m}$ *is injective for all maximal ideals* $\mathfrak{m} \subset R$.

Moreover, the same holds with "injective" replaced by "surjective" everywhere.

Proof. $(i) \implies (ii)$

If f is injective, then the sequence

$$0 \longrightarrow M \xrightarrow{f} N$$

is exact, so by the proposition, the sequence

$$0 \longrightarrow M_\mathfrak{p} \xrightarrow{f_\mathfrak{p}} N_\mathfrak{p}$$

is exact for all prime ideals $\mathfrak{p} \subset R$. So $f_\mathfrak{p}$ is injective.

$(ii) \implies (iii)$

Maximal ideals are prime.

$(iii) \implies (i)$

Suppose (iii) holds, and let $K = \ker(f)$. So we have the exact sequence

$$0 \longrightarrow K \longrightarrow M \xrightarrow{f} N$$

Then by the proposition, we have an exact sequence

$$0 \longrightarrow K_\mathfrak{m} \longrightarrow M_\mathfrak{m} \xrightarrow{f_\mathfrak{m}} N_\mathfrak{m}$$

So $K_\mathfrak{m} \cong \underbrace{\ker(f_\mathfrak{m})}_{0 \text{ by } (iii)}$

So by a previous proposition, $K = 0$, so f is injective.

∎

Motivation for next topic

Recall: An R-module M is finitely generated (fg) if there exist $f_1, \dots, f_r \in M$ such that

$$M = (f_1, \dots, f_r) = \{\sum_{i=1}^{r} a_i f_i \mid a_i \in R\}$$

Note: For general rings R, a submodule of a finitely generated module need not be finitely generated itself.
For instance, let $R = \mathbb{Z}[x_1, x_2, x_3, \dots]$ be the polynomial ring in countably-many variable seen as an R-module. This is finitely generated (e.g. by 1), but the ideal $I = (x_1, x_2, x_3, \dots)$ is not finitely generated.

Lecture 15, 2/13/23

Definition 0.27. Let R be a commutative ring with 1.

- An R-module M is a Noetherian R-module if every submodule M is finitely generated.
- We say R is a Noetherian ring if R is Noetherian as an R-module (iff every ideal is finitely generated).

Example 0.18. **1.** If F is a field, then F is a Noetherian ring and an F-module V is Noetherian iff $\dim_F V < \infty$.

2. If R is a PID, then R is a Noetherian ring and an R-module M is Noetherian iff it's finitely generated.

Proposition 19. *If an R-module M is Noetherian, then any submodule and any quotient of M is Noetherian.*

Proof. For submodules, this is clear by definition.
For quotients, let M/N be a quotient of M and $L \subset M/N$ a submodule.
Let $\phi : M \to M/N$ by $\phi(m) = m + N$.
Since M is Noetherian, we can write $\phi^{-1}(L) = (a_1, \ldots, a_r)$ for some $a_1, \ldots, a_r \in M$.
We claim $(\phi(a_1), \ldots, \phi(a_r))$ generated L.
Indeed, $\phi(a_i) = a_i + N$, since $\phi(\phi^{-1}(L)) \subset L$.
Thus $\{\overline{a_1}, \ldots, \overline{a_r}\} \subset L$.
Conversely, let $\lambda \in L$.
Then $\lambda = \overline{a} = a + N$ for some $a \in \phi^{-1}(L)$.
Thus $a = \sum_{i=1}^{r} r_i \phi(a_i)$.
Thus $L \subset (\phi(a_i), \ldots, \phi(a_r))$.

Definition 0.28. We say that an R-module M satisfies the ascending chain condition (ACC) if any ascending chain of submodules of M $N_1 \subset N_2 \subset N_3 \subset \cdots$ stabilizes, i.e. there exists $r \geq 1$ such that $N_r = N_{r+1} = \cdots$.

Theorem 0.9. *M is a Noetherian R-module iff M satisfies the ACC.*

Proof. =>

Let $N_1 \subset N_2 \subset \cdots$ be a chain of submodules of M.
Let $N = \cup_{i \geq 1} N_I$, and notes that N is a submodule of M. Then N is finitely generated, i.e. $N = (a_1, \ldots, a_k)$ for some k. Then for some r sufficiently large, $a_i \in N_r$ for $1 \leq i \leq k$. This implies that $(a_1, \ldots, a_k) \subset N_r \subset N$, so after the rth step, N_i stabilizes.

<=

Let $N \subset M$ be a submodule.
Without loss of generality, assume N is infinite. Choose a sequence of distinct points $(a_i) \in N$.
Note $(a_1) \subset (a_1, a_2) \subset (a_1, a_2, a_3) \subset \cdots$.
By the ACC, there exists r such that $(a_1, \ldots, a_r) = (a_1, \ldots, a_r, a_{r+1}) = (a_1, \ldots, a_r, a_{r+1}, a_{r+2})$ $\cdots$. So $(a_1, \ldots, a_r)$ generates N.

∎

Proposition 20. *Let M be an R-module and $N \subset M$ a submodule. If N and M/N are Noetherian R-modules, then so is M.*

Proof. Let $L_1 \subset L_2 \subset \cdots$ be an ascending chain of submodules of M.
Then $L_1 \cap N \subset L_2 \cap N \subset \cdots$ is an ascending chain of submodules of N and $\phi(L_1) \subset \phi(L_2) \subset \cdots$ is an ascending chain of submodules of M/N, where ϕ is the canonical projection.
Since $N, M/N$ are Notherian, by previous proposition we have r such that $L_1 \cap N = L_{r+1} \cap N = \cdots$ and $\phi(L_r) = \phi(L_{r=1}) = \cdots$.
We claim that $L_r = L_{r+1} = \cdots$.
It is enough to show $L_{r+1} \subset L_r$. Choose $m \in L_{r+1}$.
Then $\phi(m) \in \phi(L_{r+1}) = \phi(L_r)$.
So $m + N \in \phi(L_r)$.
Thus $m + N = y + N$ for some $y \in L_r = L_{r+1}$.
This implies that $m = y + n$ for some $n \in N$.
Note $n = m - y \in N \cap L_{r+1} = N + L_r$.
Thus $m = n + y \in L_r$.

■

Corollary 0.10. *If M and N are Noetherian modules, then so is their direct sum $M \oplus N$.*

Proof. Clear from previous, since M is a submodule of $M \oplus N$ and N is a quotient of $M \oplus N$.

■

Proposition 21. *If R is a Noetherian ring and M is a finitely generated R-module, then M is a Noetherian R-module.*

Proof. Suppose $M = (a_1, \ldots, a_n)$.
Then $\phi : R^n \to M$ by $\phi(c_i) = a_i$ is a sufjective R-homomorphism inducing $R^n / \ker(\phi) \cong M$. Then R^n is a Noetherian R-module by previous proposition.

■

Lecture 16, 2/22/23

Existence and uniqueness of tensor products.
Given R-modules M and N, we define their tensor produc t to be a pair $(M \otimes_R N, g)$, with $M \otimes_R N$ an R-module, and $g : M \times N \to M \otimes_R N$ an R-bilinear map, satisfying the universal property:
For any R-module P and R-bilinear $f : M \times N \to P$, there exists a unique R-linear map $f' : M \otimes_R N \to P$ such that $f = f \circ g$. That is, there is an f' making the

following diagram commute:

$$\begin{tikzcd} M \times N \arrow[r, "f"] \arrow[d, "g"'] & P \\ M \otimes_R N \arrow[ur, dotted, "\exists! f'"'] & \end{tikzcd}$$

Last time:
We constructed $M \otimes_R N = R^{(M\times N)}/\langle A\rangle$, where A is the submodule generated by all R-bilinear relations in $R^{(M\times N)}$.
Then $q : R^{(M\times N)} \to M \otimes_R N$ is the projection.

Remark. $M \otimes_R N$ is generated by the elements of the form $m \otimes n$, $(m \in M, n \in N)$, subject to the relations

$$\begin{aligned} (m_1 + m_2) \otimes n &= m_1 \otimes n + m_2 \otimes n \\ m \otimes (n_1 + n_2) &= m \otimes n_1 + m \otimes n_2 \\ (rm) \otimes n &= m \otimes (rn) = r(m \otimes n) \end{aligned}$$

It can be easily checked that indeed $g = q$ are bilinear, and indeed $(M \otimes_R N, g)$ satisfies the universal property.

Example 0.19.

1. $(\mathbb{Z}/3\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/2\mathbb{Z}) = 0$. It is enough to show $a \otimes b = 0$ for all $a \in \mathbb{Z}/3\mathbb{Z}, b \in \mathbb{Z}/2\mathbb{Z}$, and this follows from

$$\begin{aligned} a \otimes b &= 3(a \otimes b) - 2(a \otimes b) \\ &= \underbrace{(3a)}_{=0} \otimes b - a \otimes \underbrace{(2b)}_{=0} \\ &= 0 \end{aligned}$$

2. Let $I, J \subset R$ be ideals. Then

$$(R/I) \otimes_R (R/J) = R/(I + J)$$

In particular, $(\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/n\mathbb{Z}) = \mathbb{Z}/d\mathbb{Z}$, where $d = \gcd(m, n)$.

We check this by showing that $R/(I + J)$ along with the map β (given below) satisfies the same universal property as $(R/I) \otimes (R/J)$.

Define the map $\beta : R/I \times R/J \to R/(I + J)$ by $(r + I, s + J) \mapsto rs + I + J$. This is certainly R-bilinear.

Given any R-module P and R-bilinear $f : R/I \times R/J \to P$, we need an R-linear $f' : R/(I+J) \to P$ such that

$$\begin{tikzcd} R/I \times R/J \arrow[r, "f"] \arrow[d, "\beta"'] & P \\ R/(I+J) \arrow[ur, dotted, "f'"'] & \end{tikzcd}$$

commutes. We have $f(r+I, s+J) = rsf(1+I, 1+J)$ by R-bilinearity, and $\beta(r+I, s+J) = rs + I + J = rs(1+I+J)$.

Any such f' must send $1+I+J$ to $f(1+I, 1+J)$, and thiss uniquely determines the R-linear map $f' : R/(I+J) \to P$, $t + I + J \mapsto tf(1+I, 1+J)$, so $f = f' \circ \beta$.

Properties of the tensor product:

Proposition 22. *Let* L, M, N, M_1, M_2 *be* R*-modules. Then:*

(a) $R \otimes_R M \cong M$

(b) $M \otimes_R N \cong N \otimes_R M$

(c) $(L \otimes_R M) \otimes_R N \cong L \otimes_R (M \otimes_R N)$

(d) $(M_1 \oplus M_2) \otimes_R N \cong (M_1 \otimes_R N) \oplus (M_2 \otimes_R N)$

Proof. All these are shown using the universal property. We will prove (a). We want to produce an R-bilinear map from $R \times M \to M$. The map given by the ring action, $\beta(r, m) = r \cdot m$ is R-bilinear, and given any R-bilinear map $R \times M \to P$,

$$\begin{tikzcd} R \times M \arrow[r, "f"] \arrow[d, "\beta"'] & P \\ M \arrow[ur, "f'"] & \end{tikzcd}$$

$f(r, m) = rf(1, m)$, and $\beta(r, m) = r \cdot m$. So if we define $f' : M \to P$ by $m \mapsto f(1, m)$, this is the unique R-linear map satisfying $f = f' \circ \beta$.
So $R \otimes_R M \cong M$. ■

Lecture 12, 2/27/23

If $f : M \to N$ and $g : M' \to N'$ are R-homs, we define $f \otimes g : M \otimes M' \to N \otimes N$ by $\sum_i x_i \otimes y_i \mapsto \sum_i f(x_i) \otimes g(y_i)$.

Proposition 23. *($\otimes$ is a right exact functor)*

Suppose $M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ *be an R-module exact sequence. Then for any R-module N, the sequence*

$$M' \otimes N \xrightarrow{f \otimes \mathrm{Id}_n} M \otimes N \xrightarrow{g \otimes \mathrm{Id}_N} M'' \otimes N \longrightarrow 0$$

is also exact.

Claim. There is a natural R-module isomorphism

$$\mathrm{Hom}_R(M \otimes_R N, P) \cong \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P))$$

Proof. Indeed, for a map $f : M \otimes_R N \to P$, consider the map defined by $m \mapsto (n \mapsto f(m,n))$. The naturality of this is a classical exercise, and I did it for 236 homework. ■

We will now prove the proposition.

Proof. Let P be any R-module. By left-exactness of Hom, if

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

is exact, then

$$0 \longrightarrow \mathrm{Hom}_R(M'', \mathrm{Hom}_R(N, P)) \xrightarrow{\overline{g}} \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P)) \xrightarrow{\overline{f}} \mathrm{Hom}_R(M', \mathrm{Hom}_R(N$$

is exact. By the claim,

$$0 \longrightarrow \mathrm{Hom}_R(M'' \otimes_R, P) \xrightarrow{\overline{g \otimes \mathrm{Id}_N}} \mathrm{Hom}_R(M \otimes N, P) \xrightarrow{\overline{f \otimes \mathrm{Id}_N}} \mathrm{Hom}_R(M' \otimes N, P)$$

Note that above we really are using the fact that the correspondence between $\mathrm{Hom}_R(M \otimes_R N, P)$ and $\mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P))$ is not just a set isomorphism, but is indeed natural.

Remark.

1. The natural iso for any R-modules M, N, P,

$$\operatorname{Hom}_R(M \otimes N, P) \cong \operatorname{Hom}_R(M, \operatorname{Hom}_R(N, P))$$

means that $\otimes$ and Hom are <u>adjoint functors</u>.

2. If

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

is exact, then for an arbitrary R-module N, the sequence

$$0 \longrightarrow M' \otimes N \xrightarrow{f \otimes \mathrm{Id}_N} M \otimes N \xrightarrow{g \otimes \mathrm{Id}_N} M'' \otimes N \longrightarrow 0$$

is <u>not</u> necessarily exact (the problem is $f \otimes \mathrm{Id}_N$ is not necessarily injective).

Example 0.20. Consider the following $\mathbb{Z}$-module exact sequence:

$$0 \longrightarrow \mathbb{Z} \xrightarrow{f} \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

where f is given by $n \mapsto 2n$, and take $N = \mathbb{Z}/2\mathbb{Z}$. Then applying $- \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$ we get

$$0 \longrightarrow \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \xrightarrow{f \otimes 1} \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

But $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$, so this is the sequence

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \xrightarrow{f \otimes 1} \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

where $f \otimes \mathrm{Id}$ is <u>not</u> injective, as $f : \overline{n} \mapsto 2\overline{n} = \overline{2n} = 0$.

Definition 0.29. We say that an R-module M is <u>flat</u> (over R) if for any R-module exact sequence

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

the sequence

$$\cdots \longrightarrow M_{i-1} \otimes_R N \xrightarrow{f_{i-1} \otimes \mathrm{Id}_N} M_i \otimes_R N \xrightarrow{f_i \otimes \mathrm{Id}_n} M_{i+1} \otimes_R N \longrightarrow \cdots$$

is also exact.

Proposition 24. *Let N be an R-module. Then the following are equivalent:*

1. *N is flat over R.*

2. *If* $0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ *is a short exact sequence, then so is* $0 \longrightarrow M' \otimes_R N \xrightarrow{f \otimes_R \mathrm{Id}_N} M \otimes_R N \xrightarrow{g \otimes_R \mathrm{Id}_N} M'' \otimes_R N \longrightarrow 0$ *.*

3. *If* $f : M' \to M$ *is an injective* R*-homomorphism (with* M, M' *arbitrary* R*-modules), then* $f \otimes_R \mathrm{Id}_N : M' \otimes_R N \to M \otimes_R N$ *is also injective.*

4. *If* $f : M' \to M$ *is an injective* R*-homomorphism, with* M', M *finitely generated, then* $f \otimes_R \mathrm{Id}_N : M' \otimes_R N \to M \otimes_R N$ *is also injective.*

Proof.

(1) $\implies$ (2)

This is clear.

(2) $\implies$ (1)

Any exact sequence can be split into short exact ones.

(2) $\iff$ (3)

Previous proposition.

(3) $\implies$ (4)

Clear.

(4) $\implies$ (3)

Suppose $f : M' \to M$ is injective R-homomorphism with M, M' arbitrary, and let $u \in \ker(f \otimes \mathrm{Id}_N)$. We want to show $u = 0$.
Write $n = \sum_{i=1}^{r} x_i \otimes y_i$, with $x_i \in M', y_i \in N$, and consider the restrictions

$$\begin{tikzcd} M' \arrow[r, hook, "f"] & M \\ M'_0 \arrow[u, hook] \arrow[r, hook, "f_0"] & M_0 \arrow[u, hook] \end{tikzcd}$$

With $M'_0 \stackrel{\text{def}}{=} (x_1, \ldots, x_r)$, $M_0 \stackrel{\text{def}}{=} (f(x_1), \ldots, f(x_n))$.

Then f_0 is an injection between finitely generated R-modules, so by (4), $f_0 \otimes_R \mathrm{Id} : M_0' \otimes_R N \to M_0 \otimes_R N$ is injective.
Since $0 = (f \otimes \mathrm{Id})(u) = \sum_{i=1}^r f(x_i) \otimes y_i = \sum_{i=1}^r f_0(x_i) \otimes y_i$, since $x_i \in M_0'$. So this equals $(f_0 \otimes \mathrm{Id})(u)$. This shows $u = 0$, so $f \otimes \mathrm{Id}$ is injective.

■

Lecture 13, 3/1/23

Recall: An R-module N is flat over R if for any injective R-homomorphism $g : M' \hookrightarrow M$, the map $g \otimes_R \mathrm{Id} : M' \otimes_R N \to M \otimes_R N$ is also injective.

Example 0.21. Any free R-module is R-flat.
Indeed, if $N \cong R^n$ (the case of infinite is similar) and $g : M' \hookrightarrow M$ is an injective R-homomorphism, then

$$g \otimes_R \mathrm{Id} : \underbrace{M' \otimes_R M}_{\cong \bigoplus_{i=1}^n (M' \otimes_R R) \cong M' \oplus \cdots \oplus M'} \to M \otimes_R N$$

Similarly, $M \otimes_R N \cong M \oplus \cdots \oplus M$. As an exercise, verify $(g, \ldots, g) : M' \oplus \cdots \oplus M' \to M \oplus \cdots \oplus M$ is also injective.

Restriction and extension of scalars

Definition 0.30.
Let $f : R \to R'$ be a ring homomorphism.

1. If N is an R'-homomorphism, then N becomes an R-module via $R \times N \to N$ given by $(r, n) \mapsto f(r)m$. This is called the restriction of scalars of N (from R to R').

2. If M is an R-module, then define $M_{R'} \overset{\text{def}}{=} M \otimes_R R'$, viewing R' as an R-module via f. This is an R-module via $R' \times M_{R'} \to M_{R'}$, defined by $(a, m \otimes r') \mapsto m \otimes (ar')$. This is called the extension of scalars of N (from R' to R).

Proposition 25. *Let $f : R \to R'$ be a ring homomorphism, M an R-module, and N, P R'-modules.*
Then $M \otimes_R (N \otimes_{R'} P) \cong (M \otimes_R N) \otimes_{R'} P$ as R-module, and also as R'-modules.

Proof. Exercise (cf proof of "associativity" of $\otimes$ in lecture 17)

■

Corollary 0.11. *Let $f : R \to R'$ be a ring homomorphism, and M an R-module. Then if M is R-flat, then $M_{R'}$ is R'-flat.*

Proof. Let $g : N' \hookrightarrow N$ be an injective R'-homomorphism. Then it is an injective R-homomorphism. Because M is R-flat, $g \otimes_R \mathrm{Id} : N' \otimes_R M \to N \otimes_R M$ is also injective. Now, we write $N' \otimes_R M = (N' \otimes_{R'} R') \otimes_R M = N' \otimes_{R'} M_{R'}$, and $N \otimes_R M = (N \otimes_{R'} R') \otimes_R M = N \otimes_{R'} M_{R'}$.
So $M_{R'}$ is R'-flat.
In other words, flatness is preserved by extension of scalars. ∎

Note: For arbitrary ring homomorphism $f : R \to R'$, $M_{R'}$ is R'-flat DOES NOT imply that M is R-flat.

Example 0.22. Take $f : \underbrace{\mathbb{Z}}_{=R} \to \overbrace{\mathbb{Z}/2\mathbb{Z}}^{=R'}$, $n \mapsto \overline{n}$ the projection, and $M = \mathbb{Z}/2\mathbb{Z}$ viewed as a $\mathbb{Z}$-module. Then $M_{R'} = (\mathbb{Z}/2\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$, which is flat over R' because it is free over R'. But the original module is not flat over $\mathbb{Z}$, as we saw last time.

Flatness and localization

Proposition 26. *Let $S \subset R$ be a multiplicative subset and M an R-module. Then $(S^{-1}R) \otimes_R M \cong S^{-1}M$ as $S^{-1}R$-modules.*

Proof. Consider the following R-bilinear map $\beta : S^{-1}R \times M \to S^{-1}M$, $(\frac{a}{s}, m) \to \frac{am}{s}$. If $f : S^{-1}R \times M \to N$ is any R-bilinear map, with N any R-module, then by bilinearity, $f(\frac{a}{s}, m) = a(\frac{1}{s}, m)$. We want to find a map f' making the diagram commute:

$$\begin{tikzcd} S^{-1}R \times M \arrow[r, "f"] \arrow[d, "\beta"'] & N \\ S^{-1}M \arrow[ur, dotted, "\exists f'?"'] & \end{tikzcd}$$

Indeed, $f' : \frac{m}{s} \mapsto f(\frac{1}{s}, m)$ is the unique R-linear map making the diagram commute. By the universal property of $S^{-1}R \otimes_R M$, this implies $(S^{-1}R) \otimes_R M \cong S^{-1}M$, $\frac{a}{s} \otimes m \mapsto \frac{am}{s}$, and the isomorphism is clearly $S^{-1}R$-linear. ∎

Corollary 0.12. *("Localizations are flat")*
For any multiplicative set $S \subset R$, $S^{-1}R$ is a flat R-module, (viewing $S^{-1}R$ as an R-module via $f : R \to S^{-1}R, r \mapsto \frac{r}{1}$).

Proof. If $N \subset M$ is any R-submodule, then $S^{-1}N \subset S^{-1}M$ is an $S^{-1}R$-submodule. By previous proposition, $S^{-1}N = (S^{-1}R) \otimes_R N$, and $S^{-1}M = (S^{-1}R) \otimes_R M$.
So $S^{-1}R$ is a flat R-module. ∎

Proposition 27. *("Flatness is a local property").*
Let M be an R-module. Then the following are equivalent:

1. *M is R-flat*

2. *$M_{\mathfrak{p}}$ is flat for all prime ideals $\mathfrak{p} \subset R$*

3. *$M_{\mathfrak{m}}$ is $R_{\mathfrak{m}}$-flat for all maximal ideals $\mathfrak{m} \subset R$*

Lecture 14, 3/8/23

Next: Structure theorem for finitely generated modules over a PID.

- *Recall that an integral domain R is a principal ideal domain if every ideal in R is principle, i.e. $I = (a)$ for some $a \in R$.*
- *An integral domain R is a Euclidean domain if there is a function $N : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ such that for all $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ such that $q = qb + r$, with either $r = 0$ or $N(r) < N(b)$.*

Example 0.23. $\mathbb{Z}, F[t]$, with F a field, are PIDs, even Euclidean domains.

Lemma 4. *If R is a Euclidean domain, then R is a PID.*

Proof. Exercise

■

We'll give the proof of the structure theorem only for finitely generated modules over a Euclidean domain.

Lemma 5. *Let R be a Noetherian ring, and M a finitely generated R-module. Then there exists an R-module exact sequence*

$$R^n \xrightarrow{f} R^m \xrightarrow{g} M \longrightarrow 0$$

for some $m, n \geq 0$. In particular, $M \cong \frac{R^m}{f(R^n)}$

Proof. Let $\{v_1, \ldots, v_m\}$ be a generating set for M, and define the R-linear map $g : R^m \to M$ by $\begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} \mapsto \sum_{j=1}^m x_j v_j$.

Then $\mathrm{Im}(g) = M$, so the sequence $R^m \xrightarrow{g} M \longrightarrow 0$ is exact.

Let $K \overset{\text{def}}{=} \ker(g) \subset R^m$. Since R^m is a Noetherian R-module, K is finitely generated.

Let $\{w_1, \ldots, w_n\}$ be a generating set for K, and define the R-linear map $f : R^n \to R^m$ $f : R^n \to K \subset R^m$ by $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \sum_{i=1}^m y_i w_i$.

Them $\operatorname{Im}(f) = K (= \ker g)$, so

$$R^n \xrightarrow{f} R^m \xrightarrow{g} M \longrightarrow 0$$

is exact.

Remark.

1. A description of M as in Lemma 1 is called a presentation of M. It corresponds to a choice of:

  (i) A set of generators $\{v_1, \ldots, v_m\}$ of M

  (ii) A set of generators $\{w_1, \ldots, w_n\}$ of the set of all linear relations among the v_j's.

2. The map $f : R^n \to R^m$ corresponds to left multiplication by an $m \times n$ matrix $A \in M_{m\times n}(r)$, called a presentation matrix for M.

A has: a row for every generator v_j, and a column for every chosen generator of the relations among the v_j's.

An important fact (to be exploited) is that the same modules can have different presentation matrices.

Lemma 6. *Suppose $A \in M_{m\times n}(R)$ is a presentation matrix for M (so in particular $M \cong \frac{R^m}{Ar^n}$, and let A' be obtained from A by any of the following:*

(i) $A' = QAP^{-1}$, with $Q \in \mathrm{GL}_m(R)$, $P \in \mathrm{GL}_n(R)$.

(ii) $A' = ($A with a column $\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$ deleted)

(iii) Suppose A has a jth column equal to $\begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$, with 1 in the ith spot.

Then $A' = ($A with ith row and jth column deleted)

Then A' (of size $p \times q$, say) is also a presentation matrix for M, and $M \cong R^p/A'R^q$

Proof.

(i) From Linear Algebra, we know that that $A' = QAP^{-1}$ corresponds to a change of bases, so $M \cong R^m/AR^n \cong R^m/A'R^n$

(ii) A column $\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \in R^m$ in A corresponds to the relation $0v_1 + \cdots + 0v_m = 0$, so it can be omitted from A.

(iii) A column $\begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$ with a 1 in the ith row corresponds to the relation $0v_1 + \cdots + 1v_i + \cdots + 0v_n = 0$, which says $v_i = 0$, so it can be omitted from the generating set.

$\blacksquare$

Example 0.24.

- Suppose $M \cong \mathbb{Z}^2 / \begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix} \mathbb{Z}^2$, so M is generated by two elements, v_1, v_2, with relations $v_1 + 2v_2 = 0$ and $2v_1 - v_2 = 0$.

  Then by (1) $\dfrac{\mathbb{Z}}{\begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix} \mathbb{Z}^2} \cong \dfrac{\mathbb{Z}^2}{\begin{pmatrix} 1 & 2 \\ 0 & -5 \end{pmatrix} \mathbb{Z}^2}$. This says M is generated by v_1', v_2', with $v_1' + 0v_2' = 0$, $2v_1' - fv_2' = 0$ So $5v_2' = 0$.

  By (3), this module is isomorphic to $\dfrac{\mathbb{Z}}{5\mathbb{Z}}$

- Similarly, if $N \cong \dfrac{\mathbb{Z}^2}{\begin{pmatrix} 2 & 4 \\ 4 & 8 \end{pmatrix} \mathbb{Z}^2}$ then $\dfrac{\mathbb{Z}^2}{\begin{pmatrix} 2 & 4 \\ 4 & 8 \end{pmatrix} \mathbb{Z}^2} \cong \dfrac{\mathbb{Z}^2}{\begin{pmatrix} 2 & 4 \\ 0 & 0 \end{pmatrix} \mathbb{Z}^2} \cong \dfrac{\mathbb{Z}^2}{\begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} \mathbb{Z}^2}$, so N is generated by v_1, v_2, with relations $2v_1 + 0v_2 = 0, 0v_1 + 0v_2 = 0$, so is isomorphic by (2) to $\dfrac{\mathbb{Z}^2}{\begin{pmatrix} 2 \\ 0 \end{pmatrix} \mathbb{Z}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}$