

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

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

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

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

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

$$\begin{aligned}(\phi + \psi)(g) &= \phi(g) + \psi(g) \\ (\phi \cdot \psi)(g) &= \phi(\psi(g))\end{aligned}$$

$$1 = \text{Id}_G.$$

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 $E, F \in R$,

$$\begin{aligned}E + F &= E \triangle F \\ E \cdot F &= E \cap F\end{aligned}$$

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

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

$$\begin{aligned}f(r + s) &= f(r) + f(s) \\ f(r \cdot s) &= f(r) \cdot f(s) \\ f(1_R) &= 1_S\end{aligned}$$

Example 0.2. The quotient map $\phi : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ given by $a \mapsto \bar{a}$ 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

$$R/I \stackrel{\text{def}}{=} \{\bar{r} = r + I : r \in R\}$$

inherits an addition and multiplication from R :

$$\begin{aligned}(r + I) + (r' + I) &= (r + r' + I) \\ (r + I) \cdot (r' + I) &= (r \cdot r' + I)\end{aligned}$$

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

$$\begin{aligned}\pi : R &\rightarrow R/I \\ r &\mapsto \bar{r} = r + I\end{aligned}$$

is a ring homomorphism.

Two Exercises:

1. (“Correspondence Theorem”)

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

2. (“First Isomorphism Theorem”)

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

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

$$R/\ker(\phi) \rightarrow \text{Im}(\phi)$$

given by

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

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:

$\bar{2} \in \mathbb{Z}/6\mathbb{Z}$ 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. $\bar{2} \in \mathbb{Z}/6\mathbb{Z}$)

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

Examples: $\bar{5} \in \mathbb{Z}/6\mathbb{Z}$. 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 \underline{Rx} (or \underline{xR}). If R is commutative, we write $\underline{(x)}$ 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 $R \rightarrow S$ with $S \neq \{0\}$ is injective

Proof. $1 \rightarrow 2$ 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 $I = R$.

$2 \rightarrow 3$ For $S \neq \{0\}$, let $\phi : R \rightarrow S$ 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 \rightarrow 1 Let $x \in R$ be nonzero. We want to show that X is a unit. Consider the quotient map $\phi : R \rightarrow R/(x)$. 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 commutative ring and I a proper ideal. Then R/I is an integral domain if and only if I is a prime ideal.

Proof. \Rightarrow

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 $\bar{r}, \bar{s} \in R/I$ are such that $\bar{r} \cdot \bar{s} = \overline{rs} = \bar{0}$. Since R/I is an integral domain, either $\bar{r} = \bar{0}$ or $\bar{s} = \bar{0}$, or both. In other words, either $r \in I$, or $s \in I$.

\Leftarrow

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

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 $\underbrace{\bar{X}}_{\stackrel{\text{def}}{=} x+I} \neq \bar{0} \in R/I$. Then by assumption there

exists $\bar{y} \in R/I$ such that $\underbrace{\bar{x} \cdot \bar{y}}_{= \bar{xy}} = \bar{1} \in R/I$. 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 $J = R$.

\leq

Let $\bar{x} \neq \bar{0} \in R/I$ 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, $J \neq R$ 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 , $\bar{1} = \overline{a + rx} = \bar{a} + \bar{r}\bar{x}$. $a \in I$ though, so $\bar{1} = \bar{r}\bar{x}$, so \bar{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 not 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 $I = \{\text{all polynomials with constant term equal to } 0\} = (x)$. 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 $R = \mathbb{Z}[x]$.

The existence of maximal ideals

Definition 0.7. A partial ordering 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 not 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 upper bound 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:

- $A \neq \emptyset$, since $I \in A$
- If $a_{\lambda \in \Lambda}$ 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

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

This is the smallest ideal containing A_i for all i .

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

$$\begin{aligned}(x_1, \dots, x_t) &\stackrel{\text{def}}{=} \left\{ \sum_{i=1}^t r_i x_i \mid r_i \in R \right\} \\ &= (x_1) + \dots + (x_t)\end{aligned}$$

- 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

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

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

Example 0.3. Let $R = \mathbb{Z}$. Then $(a) + (b) = (\gcd(a, b))$, $(a) \cap (b) = (\text{lcm}(a, b))$. 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, \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. \Rightarrow

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.

\Leftarrow

Let $x \in R \setminus \mathfrak{M}$. Since \mathfrak{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 $\bar{x} \in R/\mathcal{M}$. We want to show that $\bar{x} = 0$. Then $\bar{x}^n = 0$ for some n , so $x^n \in \mathcal{N}$ for some n . But then x^n is nilpotent, so x is nilpotent. So, $\bar{x} = 0$. ■

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

Proof. Let $x \in \mathcal{N}$. Then $x^n = 0 \in \mathcal{P}$ for any prime ideal $\mathcal{P} \subset R$. So, $x \in \mathcal{P}$, 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 $f \notin \mathcal{N}$. We wish to show that $f \notin \mathcal{P}$ for some prime ideal \mathcal{P} .

Let $\Sigma = \{\text{ideals } I \subset R \mid f^n \notin I \text{ for all } n > 0\}$.

Then $\Sigma \neq \emptyset$, 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 $\mathcal{P} \in \Sigma$.

It remains to show \mathcal{P} is a prime ideal.

Suppose that $x, y \notin \mathcal{P}$. Then $\mathcal{P} \subsetneq \mathcal{P} + (x)$ and $\mathcal{P} \subsetneq \mathcal{P} + (y)$. But by maximality of \mathcal{P} , $\mathcal{P} + (x), \mathcal{P} + (y) \notin \Sigma$. So, for some n, m , $f^n \in \mathcal{P} + (x)$, $f^m \in \mathcal{P} + (y)$.

So,

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

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

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, \dots, R_m be rings. Their direct product is defined as

$$R_1 \times \cdots \times R_m = \{(x_1, \dots, x_m) \mid x_i \in R_i\}$$

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

Theorem 0.4. (Chinese Remainder Theorem)

Let I_1, \dots, I_n be ideals in a ring R , which are pairwise coprime.

Then

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

(ii) The map $\phi: R \rightarrow R/I_1 \times \cdots \times R/I_n$ given by

$$x \mapsto (x \pmod{I_1}, \dots, x \pmod{I_n})$$

induces a ring isomorphism

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

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 $i = 1, \dots, n-1$, we have $I_i + I_n = R$, so $1 = \underbrace{x_i}_{\in I_i} + \underbrace{y_i}_{\in I_n}$

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

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 $1 = (\text{element of } J) + (\text{element of } I_n)$, so $R = J + I_n$, so J and I_n are coprime.

By the base case, we have

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

We have thus proven part (i).

- (ii) $\phi : R \rightarrow \frac{R}{I_1} \times \cdots \times \frac{R}{I_m}$ 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 $\phi(x) = (1, 0, \dots, 0)$.

A similar argument would show that there exists $x_i \in R$ such that $\phi(x_i) =$

$(0, \dots, \overbrace{1}^{\text{def } e_i}, \dots, 0)$ and then given any $r = (\bar{r}_1, \dots, \bar{r}_m) \in \frac{R}{I_1} \times \cdots \times \frac{R}{I_n}$, we have

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

So we will now show surjectivity. For $i = 2, \dots, n$, we have $I_1 + I_i = R$, so

$$1 = \underbrace{u_i}_{\in I_1} + \underbrace{v_i}_{\in I_i}.$$

Then

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

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

Finally,

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

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 $f : R \rightarrow S$ 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 $f(I)$:

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

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 not 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 $f : R \rightarrow S$ 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 $f : R \rightarrow S$ 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 $C = \{\text{contracted ideals (from } S) \text{ in } R\}$ and $E = \{\text{extended ideals (from } R) \text{ in } S\}$. 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 $C \rightarrow E$ acting by $I \mapsto I^e$, and $E \rightarrow C$ 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 $\mathbb{Q} \stackrel{\text{def}}{=} \{\text{all such equivalence classes}\}$

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

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

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 $f : R \rightarrow S^{-1}R$ 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 $g : R \rightarrow R'$ 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 $h : S^{-1}R \rightarrow R'$ such that the diagram

$$\begin{array}{ccc} R & \xrightarrow{g} & R' \\ f \downarrow & \nearrow \exists! h & \\ S^{-1}R & & \end{array}$$

commutes.

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

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

so for any $s \in S$,

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

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

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

To prove the existence of h , set $h\left(\frac{r}{s}\right) \stackrel{\text{def}}{=} g(r)g(s)^{-1}$. 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} .

Note: The set ${}_{\mathfrak{p}}R_{\mathfrak{p}} \stackrel{\text{def}}{=} \{\frac{a}{s} \mid a \in \mathfrak{p}, s \in S\} \subset R_{\mathfrak{p}}$ 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 $f : R \rightarrow S^{-1}R$ the corresponding localization, sending r to $\frac{r}{1}$. Then

- (i) Every ideal in $S^{-1}R$ is extended.
- (ii) An ideal $I \subset R$ is contracted iff for all $s \in S$, $\bar{s} \in \frac{R}{I}$ 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

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

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

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

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 $\bar{x} \cdot \overline{su} = \bar{0} \in \frac{R}{I}$.

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

Now for the converse.

Suppose there exists $s \in S$ such that $\bar{s} \in \frac{R}{I}$ 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 $\bar{x} \neq \bar{0} \in \frac{R}{I}$ (i.e. $x \notin I$) such that $\bar{x} \cdot \bar{s} = \bar{0} \in \frac{R}{I}$. 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 $\mathfrak{p} \cap S = \emptyset$, 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, $\bar{s} \neq \bar{0} \in \frac{R}{\mathfrak{p}}$ for all $s \in S$.

So \bar{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 $\mathfrak{p} \cap S = \emptyset$, so we get an injection

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

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 $\mathfrak{p} \cap S = \emptyset$ (we want to show that $\mathfrak{p}^e = S^{-1}\mathfrak{p}$ is a prime ideal in $S^{-1}R$).

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

$$\frac{S^{-1}R}{S^{-1}\mathfrak{p}} \rightarrow \bar{S}^{-1}(\frac{R}{\mathfrak{p}})$$

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

But this follows from

- $\mathfrak{p} \cap S = \emptyset$, so $S^{-1}\mathfrak{p} \subsetneq S^{-1}R$, so $\bar{S}^{-1}(\frac{R}{\mathfrak{p}}) \neq (0)$
- $\bar{S}^{-1}(\frac{R}{\mathfrak{p}}) \hookrightarrow$ 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 $f : R \rightarrow S^{-1}R$, $r \mapsto \frac{r}{1}$, 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 $R \times M \rightarrow M$, 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

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

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

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

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 $\text{Ann}_R(M) = \{r \in R \mid r \cdot m = 0 \forall m \in M\} \subset R$ is an ideal of R , called the annihilator of M , and M is naturally an $R/\text{Ann}_R(M)$ -module via $R/\text{Ann}_R(M) \times M \rightarrow M$ by $(\bar{r}, m) \mapsto r \cdot m$.

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. $N \neq \emptyset$
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 commutative ring regarded as an R -module, then $\{R\text{-submodules of } R\} = \{\text{ideals of } R\}$.

2. If V is a vector space over a field F , then $\{\text{submodules of } V\} = \{\text{subspaces of } V\}$.
3. If G is an Abelian group regarded as a \mathbb{Z} -module, then $\{\mathbb{Z}\text{-submodules of } G\} = \{\text{subgroups of } G\}$.
4. If V is a vector space over a field F with endomorphism $\theta : V \rightarrow V$ (i.e. V is an $F[x]$ -module), then $\{F[x]\text{-submodule of } V = \{\theta\text{-invariant subspace } W \subseteq V\}$

Definition 0.19. Let M, N be R -modules. A group homomorphism $\theta : M \rightarrow N$ 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: $\text{Hom}_R(M, N) = \{\text{All } R\text{-homomorphisms } \theta : M \rightarrow N\}$.

$\text{Hom}_R(M, N)$ is an R -module, where $R \times \text{Hom}_R(M, N) \rightarrow \text{Hom}_R(M, N)$ is defined by

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

Example 0.12.

1. If V, W are F -vector spaces, then $\{F\text{-homomorphisms } \theta : V \rightarrow W\} = \{F\text{-linear maps } V \rightarrow W\}$.
2. If G, H are groups, then $\{\mathbb{Z}\text{-homomorphisms } \theta : G \rightarrow H\} = \{\text{group homomorphisms } \theta : G \rightarrow H\}$.

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

1. $\text{Im}(\theta) = \theta(M) \subseteq N$ 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 $R \times M/N \rightarrow M/N$ defined by $(r, \overline{m}) \rightarrow \overline{r \cdot m}$. We say M/N is a quotient module. The quotient map $\theta : M \rightarrow M/N$ where $\theta(m) = \overline{m}$ is then an R -homomorphism.

Theorem 0.5. (1st isomorphism theorem)

If $\theta : M \rightarrow N$ is an R -module homomorphism, then θ induces an R -module isomorphism $M/\ker(\theta) \cong \text{Im}(\theta)$.

Proof. Exercise ■

Lecture 10, 2/1/23

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

Definition 0.22. An R -module M is finitely generated if it's of the form $M = \langle A \rangle$ 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 $m \in M$ 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 i th spot.
3. More generally, for any set A , the module $R^{(A)} = \{ \text{all functions } f : A \rightarrow R \text{ with } f(a) = 0 \text{ for all but finitely many } a \}$ is free with basis $\{\delta_a\}_{a \in A}$, where $\delta_a : A \rightarrow R$ 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 and 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} -module 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 $f : A \rightarrow N$ extends uniquely to an R -homomorphism $\varphi : M \rightarrow N$ 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 θ is free R -module and ϕ is surjective. Then there exists an R -homomorphism

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

$$\begin{array}{ccc} & & L \\ & \swarrow \exists \psi & \downarrow \theta \\ N & \xrightarrow{\phi} & N \end{array}$$

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 preceding remark, $f : A \rightarrow N$ defined by $f(a) = n_a$ can be extended uniquely to an R -homomorphism $\psi : L \rightarrow N$ by $\sum_i \lambda_i a_i \mapsto \sum_i \lambda_i n_{a_i}$.

By construction, for any $m = \sum_i \lambda_i a_i \in L$,

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

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

$$\begin{array}{ccc} & & \mathbb{Z}_2 \\ & \swarrow \exists \psi? & \downarrow \theta = \text{Id} \\ \mathbb{Z} & \xrightarrow{n \mapsto \bar{n}} & \mathbb{Z}_2 \end{array}$$

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

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 $\theta : L \rightarrow M$ 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 exact at M_i if $\text{Im}(f_{i-1}) = \ker(f_i)$, 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) $\text{Im}(f) = \ker(g)$

Such an exact sequence is called a short exact sequence.

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

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

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

$$\begin{array}{ccccccc}
 & & & \textcolor{red}{(\text{Im}(f_i) = \ker(f_{i+1}))} & & & \\
 & & \textcolor{red}{\nearrow} & & \textcolor{red}{\searrow} & & \\
 \cdots & \longrightarrow & M_{i-1} & \xrightarrow{f_{i-1}} & M_i & \xrightarrow{f_i} & M_{i+1} \longrightarrow \cdots \\
 & \textcolor{red}{\nearrow} & & & & & \\
 \textcolor{red}{0 \rightarrow \ker(f_i)} & & & & & & \textcolor{red}{\text{Im}(f_{i+1} = \ker(f_{i+2})) \rightarrow 0}
 \end{array}$$

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 $\bar{f}(\phi) = f \circ \phi$, $\bar{g}(\psi) = g \circ \psi$.

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

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

is also exact.

Proof. We will prove 1.

Suppose $0 \longrightarrow N' \xrightarrow{f} N \xrightarrow{g} N''$ is exact.

We first show \bar{f} is injective. Suppose $\phi \in \text{Hom}_R(M, N')$ such that $f \circ \phi = \bar{f}(\phi) = 0$. Then $\text{Im}(\phi) \subseteq \ker(f) = 0$, so $\phi = 0$.

We now show $\text{Im}(\bar{f}) = \ker(\bar{g})$. Let $\phi \in \text{Hom}_R(M, N')$. Then $(\bar{f} \circ \bar{g})(\phi) = g \circ f \circ \phi = 0 \circ \phi = 0$ (because $\ker(g) \subseteq \text{Im}(f)$, so $\bar{g} \circ \bar{f} = 0$, i.e. $\text{Im}(\bar{f}) \subseteq \ker(\bar{g})$).

Conversely, let $\psi \in \ker(\bar{g})$. Then $g \circ \psi = 0$, so $\text{Im}(\psi) \subseteq \ker(g) = \text{Im}(f)$ by exactness.

$$\begin{array}{ccc}
 & M \ni m & \\
 & \downarrow \psi & \\
 N' & \xrightarrow{f} & N \ni \psi(m) = f(n')
 \end{array}$$

There exists a unique n' such that $f(n') = \psi(m)$ by exactness.

Now define $\phi : M \rightarrow N'$ 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 $\psi = \bar{f}(\phi)$, i.e. $\psi \in \text{Im}(\bar{f})$. 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

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

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

Example 0.16. For $M = \mathbb{Z}_2$ and $(N \xrightarrow{g} N'') = \left(\begin{smallmatrix} \mathbb{Z} \rightarrow \mathbb{Z}_2 \\ n \mapsto \bar{n} \end{smallmatrix} \right)$, last time we say that $(\text{Id} : \mathbb{Z}_2 \rightarrow \mathbb{Z}_2) \notin \text{Im}(\bar{g})$.

$$\begin{array}{ccc} & \mathbb{Z}_2 & \\ & \downarrow \text{Id} & \\ \mathbb{Z} & \xrightarrow{g} & \mathbb{Z}_2 \end{array}$$

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 $\bar{f} : \text{Hom}_R(M, N) \rightarrow \text{Hom}_R(M', N)$ surjective for general R -modules.

Lecture 12, 2/6/23

Lecture 13, 2/8/23

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

Recall: If N is an R -module and

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

is an exact sequence, then the sequence

$$\text{Hom}_R(M'', N) \xrightarrow{\bar{g}} \text{Hom}_R(M, N) \xrightarrow{\bar{f}} \text{Hom}_R(M', N)$$

is exact. However, f injective does not imply \bar{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,

$$\begin{array}{ccccc} 0 & \longrightarrow & M' & \xrightarrow{f} & M \\ & & \downarrow \phi & & \\ & & Q & & \end{array}$$

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

$$\begin{array}{ccccc} 0 & \longrightarrow & M' & \xrightarrow{f} & M \\ & & \downarrow \phi & \nearrow \exists \psi & \\ & & Q & & \end{array}$$

- (ii) For every injective R -homomorphism $f : M' \rightarrow M$, the induced map $\bar{f} : \text{Hom}_R(M, Q) \rightarrow \text{Hom}_R(M', Q)$, $\psi \mapsto \psi \circ f$ 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 $\beta : M \rightarrow Q$ such that $\beta \circ \alpha = \text{Id}_Q$ (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 $\phi : I \rightarrow Q$ extends to an R -homomorphism $\psi : R \rightarrow Q$,

$$\begin{array}{ccc} I & \xhookrightarrow{\iota} & R \\ \phi \downarrow & \nearrow \psi & \\ Q & & \end{array}$$

Then Q is an injective R -module.

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

$$\begin{array}{ccccc} 0 & \longrightarrow & M' & \xrightarrow{f} & M \\ & & \downarrow \phi & & \\ & & Q & & \end{array}$$

If f is an injection, then $M' \cong f(M')$. We want to show that there exists $\psi : M \rightarrow Q$ such that $\phi = \psi \circ f$. Without loss of generality, assume $M' \subseteq M$ and $f = \iota$.

Consider the set $\mathcal{A} = \{\text{all } R\text{-submodules } N \text{ of } M \text{ with } M' \subset N \subset M, \text{ such that there exists an } R\text{-homomorphism } \phi_N : N \rightarrow Q \text{ with } \phi_N|_{M'} = \phi\}$.

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 $M' \in \mathcal{A}$, $\mathcal{A} \neq \emptyset$. 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 $\phi_M : I \rightarrow Q$, $r \mapsto \phi_N(rm)$ extends to an R -homomorphism $\psi_m : R \rightarrow Q$:

$$\begin{array}{ccc} I & \xhookrightarrow{\iota} & R \\ \phi_m \downarrow & \nearrow \exists \psi_m & \\ Q & & \end{array}$$

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

$$\begin{array}{ccccc} & R & \twoheadrightarrow & R/\text{Ann}_R(m) & \cong Rm \\ & \searrow \psi_m & & \nearrow \psi'_m & \\ Q & \hookleftarrow & & & \end{array}$$

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

So we can extend ϕ_N to

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

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

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{g \mapsto n \cdot g} & \mathbb{Z} \\ 1 \mapsto g \downarrow & \nearrow \psi & \\ G & & \end{array}$$

Then there exists $\psi : \mathbb{Z} \rightarrow G$ 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 $\phi : I \rightarrow G$, the map ϕ extends to \mathbb{Z} :

$$\begin{array}{ccc} I = (n) & \xhookrightarrow{\iota} & \mathbb{Z} \\ \phi \downarrow & \nearrow & \\ G & & \end{array}$$

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 $\psi : \mathbb{Z} \rightarrow G$ defined by $1 \mapsto g'$ extends ϕ . ■

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