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

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

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.

$3 \to 1$ 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 $\underbrace{\overline{x}}_{\overset{\text{def}}{=} x+I} \neq \overline{0} \in R/I$. 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 $A_1, \ldots, A_t \subset R$ 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 $x_1, \ldots, x_t \in R$, the ideal generated by them

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

- 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

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

this is the ideal generated by $\{ab \mid a \in A, b \in B\}$. Note $A \cap B \subseteq AB$, 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 $(R, \mathfrak{M})$ 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 $R_1, \dots, R_m$ be rings. Their direct product is defined as

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

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

Theorem 0.4. *(Chinese Remainder Theorem)*
Let $I_1, \dots, I_n$ 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

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

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

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 $1 = (\text{ element of } J) + (\text{ element of } I_m)$, 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*

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

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

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

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 $h(\frac{r}{s}) \overset{\text{def}}{=} g(r)g(s)^{-1}$. 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 $f : R \to S^{-1}R$ 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

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

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

<u>Note:</u> 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.