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 :

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

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

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

is a ring homomorphism.

Two Exercises:

1. ("Correspondence Theorem")

Let R be a ring, $I \subseteq R$ an ideal, and $\phi : R \to R/I$ 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.
- $\operatorname{Im}(\phi) = \{s \in S : \exists r \in Rs.t.s = \phi(r)\}$ is an ideal of S.
- ϕ induces a ring isomorphism (i.e. a bijective ring homomorphism whose inverse is also a ring homomorphism)

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

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 $\underbrace{\overline{x}}_{\stackrel{\text{def}}{=} x+I} \neq \overline{0} \in R/I$. 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 $A_1, \ldots, A_t \subset R$ be ideals, then their sum is the ideal

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

  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 $(a) + (b) = (\gcd(a, b))$, $(a) \cap (b) = (\operatorname{lcm}(a, b))$. 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

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

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

∎