Lecture 1

Rings:

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

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

such that

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

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

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

Remark.

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

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

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

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

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

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

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

6. Let G be an abelian group, and let

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

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

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

$1 = \mathrm{Id}_G$.

Exercise: Check that R is a ring.

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

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

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

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

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

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

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

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

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

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

2. Suppose I is an ideal. Then the quotient

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

inherits an addition and multiplication from R :

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

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

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

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.

∎