Rings \( (R, +, \cdot) \)

1. \((R, +)\) abelian group, \(0, (-a) + a = 0\)
2. \(\cdot\) is associative, has identity \(1\), \(1 \cdot a = a \cdot 1 = a\) (unital rings)
3. Distributivity \((a+b) \cdot c = ac + bc\), \(a(b+c) = ab + ac\)

\(\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, M_n(R), \mathbb{Z}[\frac{1}{n}], \mathbb{Z}/n\)

Matrices \(M_n(R)\) are rings under matrix addition and multiplication.

Residues \(\mathbb{Z}/n\) under addition.

Commutative rings: \(ab = ba\) for all \(a, b \in R\)

\(M_n(R)\) is a commutative ring.

Ring of polynomials \(R[x]\)

\[ R[x] = \{ \sum_{i=0}^{n} a_i x^i | a_i \in R \} \]

- \(a_0\) constants
- \(a_0 + a_1 x\) linear
- \(a_0 + a_1 x + a_2 x^2\) quadratic
- \(a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \ldots\)
- \(a_0 + a_1 x + \ldots + a_n x^n\) degree \(n\) if \(a_n \neq 0\)

How to turn \(R[x]\) into a ring?

Need addition, multiplication of polynomials

Addition should be term-wise

\[ f(x) = a_0 + a_1 x + a_2 x^2 \]
\[ g(x) = b_0 + b_1 x + b_2 x^2 + b_3 x^3 \]

\[ f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1) x + (a_2 + b_2) x^2 + (a_3 + b_3) x^3 \]

Exercise:

\[ \deg(f(x) + g(x)) \leq \max(\deg(f(x)), \deg(g(x))) \]

In this example:

\[ \deg f = 2, \quad \deg g = 3 \]

\[ \deg(f + g) = 3 \]

If \(\deg f \neq \deg g\) then \(\deg(f + g) = \max(\deg f, \deg g)\) is \(\deg f\) or \(\deg g\) bigger than the other?

What if \(\deg f = \deg g\)?

Convenient to pad \(f(x), g(x)\) by zeros for uniform definition.
\[ f(x) = a_0 + a_1 x + a_2 x^2 \rightarrow \hat{f} = (a_0, a_1, a_2, 0, 0, 0, \ldots) \]

append in finitely many zeros

\[ g(x) = b_0 + b_1 x + b_2 x^2 + b_3 x^3 \rightarrow \hat{g} = (b_0, b_1, b_2, b_3, 0, 0, \ldots) \]

\[ f(x) = a_0 + a_1 x + \ldots + a_n x^n \rightarrow \hat{f} = (a_0, a_1, \ldots, a_n, 0, 0, 0, \ldots) \]

\[ g = (b_0, b_1, \ldots, b_m, 0, 0, \ldots) \]

\[ f + g = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots, 0, 0, \ldots) \]

\[ \text{Eventually all zeros} \]

\[ f(x) = \sum_{i=0}^{n} a_i x^i , \quad g(x) = \sum_{j=0}^{m} b_j x^j \]

\[ f(x) + g(x) = \sum_{i=0}^{\max(n,m)} (a_i + b_i^*) x^i \]

Eventually all zeros at either a's or b's.

**Addition**

Addition turns \( R[x] \) into an abelian group.

\[ f(x) = 0 \quad \text{additive identity}, \quad 0 + g(x) = g(x) \]

**Term-wise addition**

**How to multiply?**

Should have \( x^n \cdot x^m = x^{n+m} \)

Then extend using distributive laws

\[ (a_0 + a_3 x^3) x^2 = a_0 x^2 + a_3 x^5 \quad \text{example} \]

\[ (a_0 + a_1 x + a_n x^n) (b_0 + b_1 x + b_m x^m) = a_0 b_0 + a_0 b_1 x + a_0 b_m x^m + a_1 b_0 x + a_1 b_m x^m + a_n b_m x^{n+m} \]

\[ a_n x^n \text{ - a monomial.} \]
\[
\left( \sum_{i=0}^{n} a_i x^i \right) \left( \sum_{j=0}^{m} b_j x^j \right) = \sum_{i=0}^{n} \sum_{j=0}^{m} a_i b_j x^{i+j} =
\]
\[\delta(x) \quad g(x)\]

\[
= \sum_{k=0}^{n+m} \left( \sum_{i=0}^{k} a_i b_{k-i} \right) x^k =
\]

\[
= \sum_{k=0}^{n} \sum_{i+j=k} \left( \sum_{j=0}^{k} a_i b_{i-j} \right) x^k
\]

\[\text{Exercise: write this down for } n=2, \quad m=3 \text{ and think through the form of coefficients of } x^k \]

and what these sums look like

\[k=4: \quad a_0b_4 + a_1b_3 + a_2b_2 + a_3b_1 + a_4b_0 \quad k+1 \text{ terms (5 terms)}\]

\[\text{why is multiplication associative?} \quad (fg)h = f(gh) \]

\[
\sum a_i x^i \cdot g(x) = \sum b_j x^j \quad h(x) = \sum c_k x^k
\]

\[
(fg)h = \sum_{e} \left( \sum_{i+j=k} (a_i b_j) c_k \right) x^e
\]

\[
a_i x^i \cdot b_j x^j \cdot c_k x^k \rightarrow a_i b_j c_k x^{i+j+k}
\]

\[
(fgh) = \sum_{e} \left( \sum_{i+j=k} a_i (b_j c_k) \right) x^e
\]

\[
(a_i b_j c_k) x^{i+j+k} \rightarrow (a_i b_j c_k) x^{i+j+k}
\]

\[
(a_i b_j c_k) x^{i+j+k} \rightarrow (a_i b_j c_k) x^{i+j+k}
\]

\[
\text{true for monomials, then distributivity}
\]

\[
(a_i b_j c_k) = a_i (b_j c_k)
\]
Exercise) \( R \) is a subring of \( R[x] \), \( R \subseteq R[x] \), of constant polynomials.

2) \( R[x] \) is commutative iff (if and only if) \( R \) is.

(anyway, we’ll study only commutative rings for most of this course)

Noncommutative rings have even higher complexity. You’ve spent an entire semester course (linear algebra) studying elements of matrix rings \( M_n (R), M_n (C) \) and some variations (nxm matrices, linear maps \( V \rightarrow W \) between different vector spaces) + elements there + applications.

Group of invertible elements of a ring

\[ R^* = \{ a \in R : \exists b, \ ab = ba = 1 \} \quad b = a^{-1} \]

Prop \( R^* \) is a group under multiplication

1) Contains \( 1 \), \( 1^{-1} = 1 \) \( 1 \cdot 1 = 1 \).

2) If \( a_1, a_2 \in R^* \Rightarrow \exists b_1, b_2 \ a_1 b_1 = b_1 a_1 = 1 \quad a_2 b_2 = b_2 a_2 = 1 \)
   \[ a_1 a_2 \mapsto b_2 b_1 \quad a_1 a_2 b_2 b_1 = a_1 b_1 = 1 \]
   \[ b_2 b_1 a_1 a_2 = b_2 a_2 = 1 \]

3) If \( a \in R^* \) take \( b \), declare \( a^{-1} \).

Why is \( b \) unique?

We result that the inverse in a group is unique or prove.

\( R^* \) is not all of \( R \), \( 0 \in R^* \) unless up to date R was

\[ R = \{ 0 \} \]
Examples 1) \( \mathbb{Z}^* = \{ \pm 1 \} \)

2) \( \mathbb{Q}^* = \) all nonzero rationals, \( \left( \frac{a}{m} \right)^{-1} = \frac{m}{a} \), \( \mathbb{Q}^* = \mathbb{Q} \setminus \{0\} \)

3) \( \mathbb{R}^* = \) all nonzero reals, \( \mathbb{R}^* = \mathbb{R} \setminus \{0\} \)

4) \( \mathbb{C}^* = \) all nonzero complex numbers, \( \mathbb{C}^* = \mathbb{C} \setminus \{0\} \)

5) \( M_n(\mathbb{R})^* = \mathbb{GL}(n, \mathbb{R}) \) or \( \mathbb{GL}(n, \mathbb{R}) \) - invertible n x n matrices

Examples 2), 3), 4) above are special (all nonzero elements are invertible)

Definition: A commutative ring \( R \) is called a field if \( R^* = R \setminus \{0\} \).

That is, if every nonzero element of \( R \) is invertible.

\( \mathbb{Q}, \mathbb{R}, \mathbb{C} \) are fields.

(soon we'll see that linear algebra can be done over any field)

\( \mathbb{Z} \) is not a field.

\( \mathbb{Z}/n \) is sometimes a field.

\( n = 5 \) \( \mathbb{Z}/5 \) residues \( 0, 1, 2, 3, 4 \)

Invertible \( \{1, 2, 3, 4\} \)

\( \left( \mathbb{Z}/5 \right)^* = \{1, 2, 3, 4\} \)

\( 2 \cdot 3 \equiv 6 \equiv 1 \pmod{5} \)

4 \equiv -1 \pmod{5} \)

\( (-1)(-1) = 1 \)

\( 2^{-1} \equiv 3 \pmod{5} \)

Theorem: \( \mathbb{Z}/n \) is a field if and only if \( n \) is prime.

(try to prove, will discuss soon)

\( \mathbb{Z}/2, \mathbb{Z}/3, \mathbb{Z}/5, \mathbb{Z}/7, \mathbb{Z}/11 \) fields.

Common notation for a field: \( F \)
Let $R, S$ be rings.

**Definition.** A **ring homomorphism** $\phi : R \to S$ is a map (or function) from set $R$ to set $S$ such that:

1. $\phi(a + b) = \phi(a) + \phi(b)$ for all $a, b \in R$.
2. $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in R$.
3. $\phi(1) = 1$.

It takes identity in $R$ to identity in $S$.

In some books, (3) is omitted. We keep it.

**Examples.**

- **a)** Inclusions of rings $R \subseteq S$.
  \[ R \hookrightarrow S \quad \phi(1) = 1. \]

  \[ \varphi \quad \begin{array}{c} \text{a) Inclusions of rings } R \subseteq S \quad R \hookrightarrow S \quad \varphi(1) = 1. \end{array} \]

- **b)** $\varphi : R \to \{0\}$ is a ring homomorphism.

- **c)** $\varphi : \mathbb{Z} \to \mathbb{Z}/n$ is a ring homomorphism.

  \[ \varphi(a + n\mathbb{Z}) = a + n\mathbb{Z} \quad \text{residue mod } n \quad \varphi(a) = a \]

  \[ \varphi(a + b) = a + b + n\mathbb{Z} = (a + n\mathbb{Z}) + (b + n\mathbb{Z}) \]

  \[ \varphi(ab) = ab + n\mathbb{Z} = (a + n\mathbb{Z})(b + n\mathbb{Z}) \quad \text{matches our definition of product of cosets.} \]

  \[ \varphi(1) = 1 \mod(n) \]

  \[ \varphi \text{ is a surjective homomorphism. Not an isomorphism.} \]
Direct product of rings \( R_1, R_2 \) rings

\( R_1 \times R_2 \) Cartesian product of sets

\[ R_1 \times R_2 = \{ (a, b) \mid a \in R_1, b \in R_2 \} \]

addition, multiplication term-wise

\[(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)\]

\[(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 b_2)\]

\((1, 1)\) is identity

\((0, 0)\) is zero

Exercise 1) \( R_1 \times R_2 \) is a ring

2) \( R_1 \times R_2 \) is commutative if both \( R_1, R_2 \) are commutative

3) \( R_1 \times R_2 \xrightarrow{\alpha} R_1 \)

\((a, b) \xrightarrow{\alpha} a\)

\(\alpha\) is a homomorphism

\( R_1 \times R_2 \xrightarrow{\beta} R_2 \)

\((a, b) \xrightarrow{\beta} b\)

\(\beta\) is a homomorphism

but \( R_1 \rightarrow R_1 \times R_2 \)

\(a \mapsto (a, 0)\)

is not a homomorphism. Why?

Elements \((1, 0), (0, 1)\) are special

\((1, 0)^2 = (1, 0) (1, 0) = (1, 0)\) itself

\((0, 1)^2 = (0, 1)\)

\((1, 1) = (1, 0) + (0, 1)\)

\(e \in R\) is called an idempotent

If \(e^2 = e\), \(0, 1\) are idempotents
$e$ in $R$ is called an idempotent if $e^2 = e$.

0, 1 are idempotents. Sometimes, a ring may have additional idempotents.

(a) In direct product $R_1 \times R_2$, $(1,0), (0,1)$ are idempotents.

Exercise. $e$ is an idempotent $\Rightarrow$ $1-e$ is an idempotent.

Note: $e$ and $(1-e)$ annihilate each other.

\[
e(1-e) = e - e^2 = e - e = 0
\]

\[
(1-e)e = e - e^2 = 0
\]

Complementary idempotents

(b) In $\mathbb{Z}/6\mathbb{Z}$ have usual idempotents 0, 1. Also

$3^2 = 9 \equiv 3 \pmod{6}$

$4^2 = 16 \equiv 4 \pmod{6}$.

$3 + 4 = 1$ complementary idempotents

(Continued. Note's due to $\mathbb{Z}/6 = \mathbb{Z}/2 \times \mathbb{Z}/3$ as rings)

(c) $M_n(\mathbb{R})$ projection operators $P : P^2 = P$

are idempotents

\[
\begin{array}{c}
\downarrow \quad \downarrow P \\
W \quad \uparrow P
\end{array}
\]

$P(w) = 0$

$P(w) = w$

$\forall w \in W$