# Discrete Algebraic Structures

WiSe 2025/2026

Prof. Dr. Antoine Wiehe
Research Group for Theoretical Computer Science

| Abstract | Concrete |
|---|---|
| **Structures** with multiplication, neutral elements | (relations, $\circ$, Id) $(\{0,1\}^*, \cdot, \epsilon)$ $\boxed{\text{Monoids}}$ |
| Every group is a monoid<br>**Structures** with multiplication, inverses, neutral elements | Real Numbers: $\times, 1/x, 1$ $a \times 1/a = 1$<br>Matrices: $\times, M^{-1}, I$ $M \cdot M^{-1} = I_n$ $\boxed{\text{Groups}}$<br>Bijective Functions: $\circ, f^{-1}, \mathrm{Id}_A$<br>Modular arithmetic: $\times, [a]_d^{-1}, [1]_d$ |
| | |
| | |

Definition of abstract object that generalizes something we know

Concrete examples we want to study

for example, Fermat's little theorem

Lagrange's theorem $a^{|G|} = e$

Identify some properties that are important in the concrete case

General theorems about all our examples

| Abstract | Concrete | |
|---|---|---|
| **Structures** with multiplication, neutral elements | (relations, $\circ$, Id) $(\{0,1\}^*, \cdot, \epsilon)$ | Monoids |
| **Structures** with multiplication, inverses, neutral elements | Real Numbers: $\times, 1/x, 1$<br>Matrices: $\times, M^{-1}, I$<br>Bijective Functions: $\circ, f^{-1}, \mathrm{Id}_A$<br>Modular arithmetic: $\times, [a]_d^{-1}, [1]_d$ | Groups |
| **Structures** with addition and multiplication | $(\mathbb{R}, +, \times)$ $(\mathbb{Z}/d\mathbb{Z}, +, \times)$<br>$(\mathbb{R}^{n\times n}, +, \times)$ $(\mathbb{R}[X], +, \times)$ | Rings |
| | | |

Definition of abstract object that generalizes something we know

Concrete examples we want to study

for example, Fermat's little theorem

Identify some properties that are important in the concrete case

General theorems about all our examples

| Abstract | Concrete |
|---|---|
| **Structures** with multiplication, neutral elements | (relations, $\circ$, Id) ($\{0,1\}^*, \cdot, \epsilon$) $\boxed{\text{Monoids}}$ |
| **Structures** with multiplication, inverses, neutral elements | Real Numbers: $\times, 1/x, 1$<br>Matrices: $\times, M^{-1}, I$<br>Bijective Functions: $\circ, f^{-1}, \mathrm{Id}_A$<br>Modular arithmetic: $\times, [a]_d^{-1}, [1]_d$<br>$\boxed{\text{Groups}}$ |
| **Structures** with addition and multiplication | $(\mathbb{R}, +, \times)$ $(\mathbb{Z}/d\mathbb{Z}, +, \times)$<br>$(\mathbb{R}^{n\times n}, +, \times)$ $(\mathbb{R}[X], +, \times)$ $\boxed{\text{Rings}}$ |
| **Structures** with addition and scalar multiplication | $(\mathbb{R}^n, +, \lambda\cdot)$ $\boxed{\text{Vector spaces}}$ |

Definition of abstract object that generalizes something we know

Concrete examples we want to study

for example, Fermat's little theorem

Identify some properties that are important in the concrete case

General theorems about all our examples

| Abstract | Concrete | |
|---|---|---|
| **Structures** with multiplication, neutral elements | (relations, $\circ$, Id) $(\{0,1\}^*, \cdot, \epsilon)$ | $\boxed{\text{Monoids}}$ |
| **Structures** with multiplication, inverses, neutral elements | Real Numbers: $\times, 1/x, 1$<br>Matrices: $\times, M^{-1}, I$<br>Bijective Functions: $\circ, f^{-1}, \mathrm{Id}_A$<br>Modular arithmetic: $\times, [a]_d^{-1}, [1]_d$ | $\boxed{\text{Groups}}$ |
| **Structures** with addition and multiplication | $(\mathbb{R}, +, \times)$ $(\mathbb{Z}/d\mathbb{Z}, +, \times)$<br>$(\mathbb{R}^{n\times n}, +, \times)$ $(\mathbb{R}[X], +, \times)$ | $\boxed{\text{Rings}}$ |
| **Structures** with addition and scalar multiplication | $(\mathbb{R}^n, +, \lambda\cdot)$ | $\boxed{\text{Vector spaces}}$ |

Plan for today:

- a bit more about groups: homomorphisms, how to compare groups
- structures with several binary operations: rings
- polynomials

Goal:

- overview of algebra for CS
- understand necessary notions for error-correcting codes (for next week)

**Definition.** An internal composition law or binary operation on $A$ is a function $\circ\colon A^2 \to A$. We write $a \circ b$ instead of $\circ(a, b)$.

$(A, \circ)$ is a **monoid** if $\circ$ is associative and has a neutral element

$(A, \circ)$ is a **group** if $\circ$ is associative, has a neutral element, and every $a \in A$ has an inverse

$a \circ (b \circ c) = (a \circ b) \circ c$

there is a special $e$ s.t.: $\forall a \in A$: $a \circ e = e \circ a = a$.

**Example.**

| | $a$ | $b$ | $c$ |
|---|---|---|---|
| $a$ | $a$ | $b$ | $c$ |
| $b$ | $b$ | $c$ | $a$ |
| $c$ | $c$ | $a$ | $b$ |

$b \circ c = a$.

$A = \{a, b, c\}$

**Definition.** An internal composition law or binary operation on $A$ is a function $\circ\colon A^2 \to A$. We write $a \circ b$ instead of $\circ(a, b)$.
$(A, \circ)$ is a **monoid** if $\circ$ is associative and has a neutral element
$(A, \circ)$ is a **group** if $\circ$ is associative, has a neutral element, and every $a \in A$ has an inverse

**Example.**

| | $a$ | $b$ | $c$ |
|---|---|---|---|
| $a$ | $a$ | $b$ | $c$ |
| $b$ | $b$ | $c$ | $a$ |
| $c$ | $c$ | $a$ | $b$ |

This is:
- A monoid? a neutral ✓
- A group? ✓
- Neither a monoid nor a group? ✗

$a^{-1} = a$
$b \cdot b^{-1} = a \Rightarrow b^{-1} = c$

**Definition.** An internal composition law or binary operation on $A$ is a function $\circ \colon A^2 \to A$.
We write $a \circ b$ instead of $\circ(a, b)$.
$(A, \circ)$ is a **monoid** if $\circ$ is associative and has a neutral element
$(A, \circ)$ is a **group** if $\circ$ is associative, has a neutral element, and every $a \in A$ has an inverse

**Example.**

| $\circ$ | $a$ | $b$ | $c$ |
|---|---|---|---|
| $a$ | $a$ | $b$ | $c$ |
| $b$ | $b$ | $c$ | $a$ |
| $c$ | $c$ | $a$ | $b$ |

**Example.**

| $\circ$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

$A = \{0, 1, 2\}$ $(\mathbb{Z}/3\mathbb{Z}, +)$

**Definition.** An internal composition law or binary operation on $A$ is a function $\circ\colon A^2 \to A$. We write $a \circ b$ instead of $\circ(a, b)$.
$(A, \circ)$ is a **monoid** if $\circ$ is associative and has a neutral element
$(A, \circ)$ is a **group** if $\circ$ is associative, has a neutral element, and every $a \in A$ has an inverse

**Example.**

| | $a$ | $b$ | $c$ |
|---|---|---|---|
| $a$ | $a$ | $b$ | $c$ |
| $b$ | $b$ | $c$ | $a$ |
| $c$ | $c$ | $a$ | $b$ |

**Example.**

| | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

Two different groups! But.. are they really different?

**Definition.** An internal composition law or binary operation on $A$ is a function $\circ\colon A^2 \to A$.
We write $a \circ b$ instead of $\circ(a, b)$.
$(A, \circ)$ is a **monoid** if $\circ$ is associative and has a neutral element
$(A, \circ)$ is a **group** if $\circ$ is associative, has a neutral element, and every $a \in A$ has an inverse

**Example.**

| | $a$ | $b$ | $c$ |
|---|---|---|---|
| $a$ | $a$ | $b$ | $c$ |
| $b$ | $b$ | $c$ | $a$ |
| $c$ | $c$ | $a$ | $b$ |

$a \mapsto 0$
$b \mapsto 1$
$c \mapsto 2$

**Example.**

| | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

Two different groups! But.. are they really different?

**Definition.** An internal composition law or binary operation on $A$ is a function $\circ\colon A^2 \to A$.
We write $a \circ b$ instead of $\circ(a, b)$.
$(A, \circ)$ is a **monoid** if $\circ$ is associative and has a neutral element
$(A, \circ)$ is a **group** if $\circ$ is associative, has a neutral element, and every $a \in A$ has an inverse

$(\mathbb{R}, +)$

neutral: $0$

"inverse" of $x$: $-x$

$(\mathbb{R}_{>0}, \times)$

neutral: $1$

inverse of $x$: $1/x$

**Definition.** An internal composition law or binary operation on $A$ is a function $\circ\colon A^2 \to A$.
We write $a \circ b$ instead of $\circ(a, b)$.
$(A, \circ)$ is a **monoid** if $\circ$ is associative and has a neutral element
$(A, \circ)$ is a **group** if $\circ$ is associative, has a neutral element, and every $a \in A$ has an inverse

$(\mathbb{R}, +)$ $(\mathbb{R}_{>0}, \times)$

Two different groups! But.. are they really different?

**Definition.** An internal composition law or binary operation on $A$ is a function $\circ \colon A^2 \to A$.
We write $a \circ b$ instead of $\circ(a, b)$.
$(A, \circ)$ is a **monoid** if $\circ$ is associative and has a neutral element
$(A, \circ)$ is a **group** if $\circ$ is associative, has a neutral element, and every $a \in A$ has an inverse

$2^{1/2 + 1/4 + \cdots + 1/1024}$

$\parallel$

$\frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{1024}$ $\qquad$ $2^{1/2} \times 2^{1/4} \times \cdots \times 2^{1/1024}$

$(\mathbb{R}, +)$ $\qquad$ $(\mathbb{R}_{>0}, \times)$

Two different groups! But.. are they really different?

**Definition.** An internal composition law or binary operation on $A$ is a function $\circ\colon A^2 \to A$.
We write $a \circ b$ instead of $\circ(a, b)$.
$(A, \circ)$ is a **monoid** if $\circ$ is associative and has a neutral element
$(A, \circ)$ is a **group** if $\circ$ is associative, has a neutral element, and every $a \in A$ has an inverse

$\frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{1024}$ $\qquad$ $2^{1/2} \times 2^{1/4} \times \cdots \times 2^{1/1024}$

$-1 \mapsto 2^{-1}$

$$(\mathbb{R}, +) \xrightarrow{x \mapsto 2^x} (\mathbb{R}_{>0}, \times)$$

Two different groups! But.. are they really different?

**Definition.** An internal composition law or binary operation on $A$ is a function $\circ\colon A^2 \to A$.
We write $a \circ b$ instead of $\circ(a, b)$.
$(A, \circ)$ is a **monoid** if $\circ$ is associative and has a neutral element
$(A, \circ)$ is a **group** if $\circ$ is associative, has a neutral element, and every $a \in A$ has an inverse

$$\underbrace{1 + 2 + \cdots + 7}_{= 28} \qquad [1]_8 + [2]_8 + \cdots + [7]_8$$

$$(\mathbb{Z}, +) \qquad (\mathbb{Z}/8\mathbb{Z}, +)$$

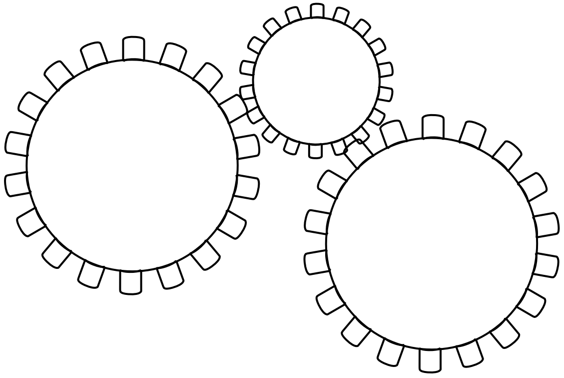
**Definition.** An internal composition law or binary operation on $A$ is a function $\circ\colon A^2 \to A$. We write $a \circ b$ instead of $\circ(a, b)$.
$(A, \circ)$ is a **monoid** if $\circ$ is associative and has a neutral element
$(A, \circ)$ is a **group** if $\circ$ is associative, has a neutral element, and every $a \in A$ has an inverse

$$28 \mapsto [28]_8 = [4]_8$$

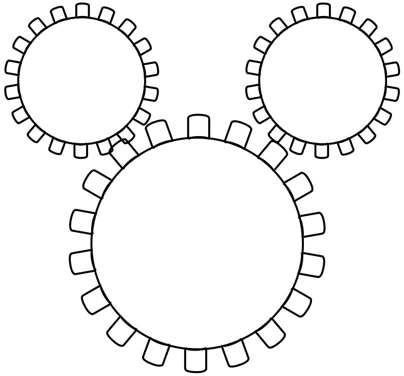
$$1 + 2 + \cdots + 7 \qquad [1]_8 + [2]_8 + \cdots + [7]_8$$

$$(\mathbb{Z}, +) \xrightarrow[x \mapsto [x]_8]{} (\mathbb{Z}/8\mathbb{Z}, +)$$

**Definition.** An internal composition law or binary operation on $A$ is a function $\circ\colon A^2 \to A$.
We write $a \circ b$ instead of $\circ(a, b)$.
$(A, \circ)$ is a **monoid** if $\circ$ is associative and has a neutral element
$(A, \circ)$ is a **group** if $\circ$ is associative, has a neutral element, and every $a \in A$ has an inverse



$h$



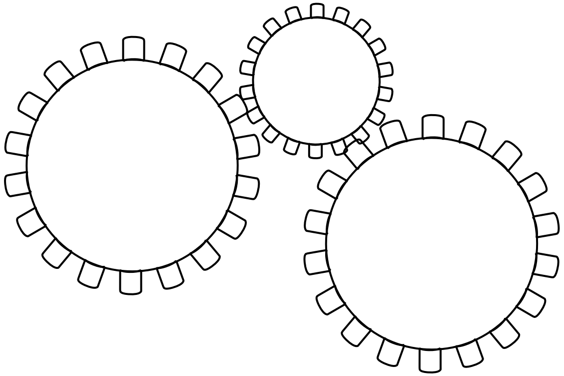
Computation in $(A, \circ)$

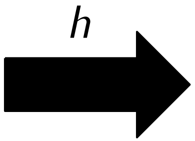
$\frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{1024}$

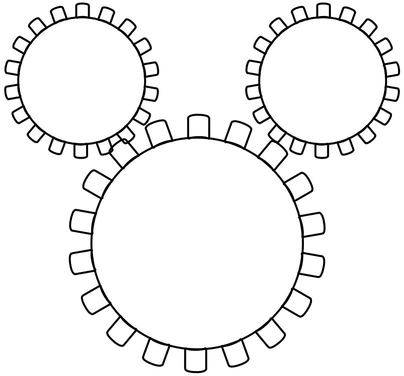
$1 + 2 + \cdots + 7$

Computation in $(B, \square)$

**Definition.** An internal composition law or binary operation on $A$ is a function $\circ\colon A^2 \to A$.
We write $a \circ b$ instead of $\circ(a, b)$.
$(A, \circ)$ is a **monoid** if $\circ$ is associative and has a neutral element
$(A, \circ)$ is a **group** if $\circ$ is associative, has a neutral element, and every $a \in A$ has an inverse





Computation in $(A, \circ)$

$\frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{1024}$

$1 + 2 + \cdots + 7$

Computation in $(B, \square)$

$2^{1/2} \times 2^{1/4} \times \cdots \times 2^{1/1024}$

$[1]_8 + [2]_8 + \cdots + [7]_8$

**Definition.** Let $(A, \circ)$ and $(B, \Box)$ be two monoids.
A homomorphism $h\colon (A, \circ) \to (B, \Box)$ is a function such that
$$h(a \circ a') = h(a) \Box h(a')$$

**Definition.** Let $(A, \circ)$ and $(B, \square)$ be two monoids.
A homomorphism $h\colon (A, \circ) \to (B, \square)$ is a function such that
$$h(a \circ a') = h(a) \square h(a')$$

From Math 1:

**Definition.** A map $f\colon \mathbb{R}^n \to \mathbb{R}^m$ is called linear if for all $x, y \in \mathbb{R}^n$ and $\lambda \in \mathbb{R}$, we have:
$$f(x+y) = f(x)+f(y)$$
$$f(\lambda x) = \lambda f(x)$$

**Definition.** Let $(A, \circ)$ and $(B, \square)$ be two monoids.
A homomorphism $h\colon (A, \circ) \to (B, \square)$ is a function such that

$$h(a \circ a') = h(a) \square h(a')$$

From Math 1:

**Definition.** A map $f\colon \mathbb{R}^n \to \mathbb{R}^m$ is called linear if for all $x, y \in \mathbb{R}^n$ and $\lambda \in \mathbb{R}$, we have:

$$f(x+y) = f(x)+f(y)$$
$$f(\lambda x) = \lambda f(x)$$

$\rightsquigarrow$ a linear map is a homomorphism $(\mathbb{R}^n, +) \to (\mathbb{R}^m, +)$!

**Definition.** Let $(A, \circ)$ and $(B, \square)$ be two monoids.
A homomorphism $h\colon (A, \circ) \to (B, \square)$ is a function such that

$$h(a \circ a') = h(a) \square h(a')$$

**Examples.**

- Linear maps $\mathbb{R}^n \to \mathbb{R}^m$
- Exponential map: $x \mapsto e^x$ is a homomorphism $(\mathbb{R}, +) \to (\mathbb{R}_{>0}, \times)$
- Logarithm?
- The "mod $d$" function $x \mapsto [x]_d$ is a homomorphism $(\mathbb{Z}, +) \to (\mathbb{Z}/d\mathbb{Z}, +)$

$\log : (\mathbb{R}_{>0}, \times) \longrightarrow (\mathbb{R}, +)$

$\log(a \times b) = \log(a) + \log(b)$

**Definition.** Let $(A, \circ)$ and $(B, \square)$ be two monoids.
A homomorphism $h\colon (A, \circ) \to (B, \square)$ is a function such that

$$h(a \circ a') = h(a) \square h(a')$$

**Examples.**

- Linear maps $\mathbb{R}^n \to \mathbb{R}^m$
- Exponential map: $x \mapsto e^x$ is a homomorphism $(\mathbb{R}, +) \to (\mathbb{R}_{>0}, \times)$
- Logarithm?
- The "mod $d$" function $x \mapsto [x]_d$ is a homomorphism $(\mathbb{Z}, +) \to (\mathbb{Z}/d\mathbb{Z}, +)$

For $x \in \{0, \dots, d-1\}$, define $h([x]_d) = x$.
This is a function $\mathbb{Z}/d\mathbb{Z} \to \mathbb{Z}$.
Is this a homomorphism $(\mathbb{Z}/d\mathbb{Z}, +) \to (\mathbb{Z}, +)$?

$$h(\underbrace{[x]_d+[y]_d}) \stackrel{?}{=} h([x])+h([y])$$

$$0 = h([0]_d) \qquad 1 + (d-1) = d$$

$x = 1$

$y = d-1$

**Definition.** Let $(A, \circ)$ and $(B, \square)$ be two monoids.
A homomorphism $h\colon (A, \circ) \to (B, \square)$ is a function such that

$$h(a \circ a') = h(a) \square h(a')$$

$A, B \quad A = I \quad B = -B$

$\det(A+B) \neq \det(A) + \det(B)$

$\det(AB) = \det(A)\det(B)$

**Examples.**

- Linear maps $\mathbb{R}^n \to \mathbb{R}^m$
- Exponential map: $x \mapsto e^x$ is a homomorphism $(\mathbb{R}, +) \to (\mathbb{R}_{>0}, \times)$
- Logarithm?
- The "mod $d$" function $x \mapsto [x]_d$ is a homomorphism $(\mathbb{Z}, +) \to (\mathbb{Z}/d\mathbb{Z}, +)$

Consider det as a function from $n \times n$-matrices to $\mathbb{R}$.
Is it a homomorphism:

- $(\mathbb{R}^{n \times n}, +) \to (\mathbb{R}, +)$?
- $(\mathbb{R}^{n \times n}, \times) \to (\mathbb{R}, +)$?
- $(\mathbb{R}^{n \times n}, \times) \to (\mathbb{R}, \times)$? ✓
- $(\mathbb{R}^{n \times n}, \times) \to (\mathbb{R}, +)$?

**Definition.** Let $(A, \circ)$ and $(B, \square)$ be two monoids.
A homomorphism $h\colon (A, \circ) \to (B, \square)$ is a function such that

$$h(a \circ a') = h(a) \square h(a')$$

**Examples.**

- Linear maps $\mathbb{R}^n \to \mathbb{R}^m$
- Exponential map: $x \mapsto e^x$ is a homomorphism $(\mathbb{R}, +) \to (\mathbb{R}_{>0}, \times)$
- Logarithm?
- The "mod $d$" function $x \mapsto [x]_d$ is a homomorphism $(\mathbb{Z}, +) \to (\mathbb{Z}/d\mathbb{Z}, +)$

If $h$ is a bijection, we say that it is an isomorphism.

**Definition.** Let $(A, \circ)$ and $(B, \square)$ be two monoids.
A homomorphism $h\colon (A, \circ) \to (B, \square)$ is a function such that
$$h(a \circ a') = h(a) \square h(a')$$

**Examples.**
- Linear maps $\mathbb{R}^n \to \mathbb{R}^m$
- Exponential map: $x \mapsto e^x$ is a homomorphism $(\mathbb{R}, +) \to (\mathbb{R}_{>0}, \times)$
- Logarithm?
- The "mod $d$" function $x \mapsto [x]_d$ is a homomorphism $(\mathbb{Z}, +) \to (\mathbb{Z}/d\mathbb{Z}, +)$

If $h$ is a bijection, we say that it is an isomorphism.

**Example.** $G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$ is a group (with matrix multiplication).

Which group has an isomorphism with $G$?
- $(\mathbb{Z}/2\mathbb{Z}, +)$ ✓
- $(\mathbb{Z}, +)$
- $(\mathbb{Z}/3\mathbb{Z}, +)$

$h: [0] \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$[1] \mapsto \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$

**Definition.** Let $(A, \circ)$ and $(B, \square)$ be two monoids.
A homomorphism $h\colon (A, \circ) \to (B, \square)$ is a function such that
$$h(a \circ a') = h(a) \square h(a')$$

**Examples.**

- Linear maps $\mathbb{R}^n \to \mathbb{R}^m$
- Exponential map: $x \mapsto e^x$ is a homomorphism $(\mathbb{R}, +) \to (\mathbb{R}_{>0}, \times)$
- Logarithm?
- The "mod $d$" function $x \mapsto [x]_d$ is a homomorphism $(\mathbb{Z}, +) \to (\mathbb{Z}/d\mathbb{Z}, +)$

If $h$ is a bijection, we say that it is an isomorphism.
Up to isomorphism, there is only one group of size $2$.

**Definition.** Let $(A, \circ)$ and $(B, \square)$ be two monoids.
A homomorphism $h\colon (A, \circ) \to (B, \square)$ is a function such that
$$h(a \circ a') = h(a) \square h(a')$$

**Examples.**

- Linear maps $\mathbb{R}^n \to \mathbb{R}^m$
- Exponential map: $x \mapsto e^x$ is a homomorphism $(\mathbb{R}, +) \to (\mathbb{R}_{>0}, \times)$
- Logarithm?
- The "mod $d$" function $x \mapsto [x]_d$ is a homomorphism $(\mathbb{Z}, +) \to (\mathbb{Z}/d\mathbb{Z}, +)$

If $h$ is a bijection, we say that it is an isomorphism.
Up to isomorphism, there is only one group of size 2.

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| number of groups | 1 | 1 | 1 | 2 | 1 | 2 | 11 | 5 | 2 | 2 | 1 | 5 |

**Message:**

- if the "thing" you are studying is a group, then there is a lot of structure to exploit
- even if your group is not we saw in class, it could be isomorphic to one

# Rings, Fields, and Polynomials

| Abstract | Concrete |
|---|---|
| **Structures** with multiplication, neutral elements | Relations: $\circ$, Id $(\{0,1\}^*, \cdot, \epsilon)$ $\boxed{\text{Monoids}}$ |
| **Structures** with multiplication, inverses, neutral elements | Real Numbers: $\times$, $1/x$, $1$<br>Matrices: $\times$, $M^{-1}$, $I$<br>Bijective Functions: $\circ$, $f^{-1}$, $\mathrm{Id}_A$<br>Modular arithmetic: $\times$, $[a]_d^{-1}$, $[1]_d$<br>$\boxed{\text{Groups}}$ |
| **Structures** with addition and multiplication | $(\mathbb{R}, +, \times)$ $(\mathbb{Z}/d\mathbb{Z}, +, \times)$<br>$(\mathbb{R}^{n\times n}, +, \times)$ $(\mathbb{R}[X], +, \times)$<br>$\boxed{\text{Rings}}$ |
| **Structures** with addition and scalar multiplication | $(\mathbb{R}^n, +, \lambda\cdot)$ $\boxed{\text{Vector spaces}}$ |

| Abstract | Concrete | |
|---|---|---|
| **Structures** with multiplication, neutral elements | Relations: $\circ$, Id $(\{0,1\}^*, \cdot, \epsilon)$ | Monoids |
| **Structures** with multiplication, inverses, neutral elements | Real Numbers: $\times, 1/x, 1$<br>Matrices: $\times, M^{-1}, I$<br>Bijective Functions: $\circ, f^{-1}, \mathrm{Id}_A$<br>Modular arithmetic: $\times, [a]_d^{-1}, [1]_d$ | Groups |
| **Structures** with addition and multiplication | $(\mathbb{R}, +, \times)$ $(\mathbb{Z}/d\mathbb{Z}, +, \times)$<br>$(\mathbb{R}^{n\times n}, +, \times)$ $(\mathbb{R}[X], +, \times)$ | Rings |
| **Structures** with addition and scalar multiplication | $(\mathbb{R}^n, +, \lambda\cdot)$ | Vector spaces |

What can we say about how $+$ and $\times$ relate in our examples?

| Abstract | Concrete | |
|---|---|---|
| **Structures** with multiplication, neutral elements | Relations: $\circ$, Id $(\{0,1\}^*, \cdot, \epsilon)$ | Monoids |
| **Structures** with multiplication, inverses, neutral elements | Real Numbers: $\times, 1/x, 1$<br>Matrices: $\times, M^{-1}, I$<br>Bijective Functions: $\circ, f^{-1}, \mathrm{Id}_A$<br>Modular arithmetic: $\times, [a]_d^{-1}, [1]_d$ | Groups |
| **Structures** with addition and multiplication | $(\mathbb{R}, +, \times)$ $(\mathbb{Z}/d\mathbb{Z}, +, \times)$<br>$(\mathbb{R}^{n\times n}, +, \times)$ $(\mathbb{R}[X], +, \times)$ | Rings |
| **Structures** with addition and scalar multiplication | $(\mathbb{R}^n, +, \lambda\cdot)$ | Vector spaces |

What can we say about how $+$ and $\times$ relate in our examples?

**Definition.** Let $+$ and $\times$ be internal composition laws on $A$.
We say that $\times$ distributes over $+$ if for all $a, b, c \in A$

$$a \times (b + c) = a \times b + a \times c \qquad (b + c) \times a = b \times a + c \times a$$

**Definition.** Let $+$ and $\times$ be internal composition laws on $A$.
We say that $\times$ distributes over $+$ if for all $a, b, c \in A$

$$a \times (b + c) = a \times b + a \times c \qquad (b + c) \times a = b \times a + c \times a$$

- All addition/multiplication operations you know
- $\varphi \wedge (\psi \vee \theta) \equiv (\varphi \wedge \psi) \vee (\varphi \wedge \theta)$
- $\varphi \vee (\psi \wedge \theta) \equiv (\varphi \vee \psi) \wedge (\varphi \vee \theta)$
- same with $\cap$ and $\cup$

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

**Definition.** Let $+$ and $\times$ be internal composition laws on $A$.
We say that $\times$ distributes over $+$ if for all $a, b, c \in A$

$$a \times (b + c) = a \times b + a \times c \qquad (b + c) \times a = b \times a + c \times a$$

- All addition/multiplication operations you know
- $\varphi \wedge (\psi \vee \theta) \equiv (\varphi \wedge \psi) \vee (\varphi \wedge \theta)$
- $\varphi \vee (\psi \wedge \theta) \equiv (\varphi \vee \psi) \wedge (\varphi \vee \theta)$
- same with $\cap$ and $\cup$

**Definition.** Let $+$ and $\times$ be binary operations on $A$.
Then $(A, +, \times)$ is a **ring** if:
- $(A, +)$ is a commutative group,
- $(A, \times)$ is monoid,
- $\times$ distributes over $+$.

**Definition.** Let $+$ and $\times$ be internal composition laws on $A$.
We say that $\times$ distributes over $+$ if for all $a, b, c \in A$

$$a \times (b + c) = a \times b + a \times c \qquad (b + c) \times a = b \times a + c \times a$$

- All addition/multiplication operations you know
- $\varphi \wedge (\psi \vee \theta) \equiv (\varphi \wedge \psi) \vee (\varphi \wedge \theta)$
- $\varphi \vee (\psi \wedge \theta) \equiv (\varphi \vee \psi) \wedge (\varphi \vee \theta)$
- same with $\cap$ and $\cup$

**Definition.** Let $+$ and $\times$ be binary operations on $A$.
Then $(A, +, \times)$ is a **ring** if:

- $(A, +)$ is a commutative group,
- $(A, \times)$ is monoid,
- $\times$ distributes over $+$.

**Exercise**: for each of the following, think about why it is a ring.

- $(\{0, 1\}, \wedge, \vee)$
- $(\{0, 1\}, \vee, \wedge)$
- $(\mathbb{Z}/d\mathbb{Z}, +, \times)$
- $(\mathbb{R}^{n\times n}, +, \times)$

**Definition.** Let $+$ and $\times$ be internal composition laws on $A$.
We say that $\times$ distributes over $+$ if for all $a, b, c \in A$

$$a \times (b + c) = a \times b + a \times c \qquad (b + c) \times a = b \times a + c \times a$$

- All addition/multiplication operations you know
- $\varphi \wedge (\psi \vee \theta) \equiv (\varphi \wedge \psi) \vee (\varphi \wedge \theta)$
- $\varphi \vee (\psi \wedge \theta) \equiv (\varphi \vee \psi) \wedge (\varphi \vee \theta)$
- same with $\cap$ and $\cup$

**Definition.** Let $+$ and $\times$ be binary operations on $A$.
Then $(A, +, \times)$ is a **ring** if:

- $(A, +)$ is a commutative group,
- $(A, \times)$ is monoid,
- $\times$ distributes over $+$.

**Exercise**: for each of the following, think about why it is a ring.

- $(\{0, 1\}, \wedge, \vee)$
- $(\{0, 1\}, \vee, \wedge)$
- $(\mathbb{Z}/d\mathbb{Z}, +, \times)$
- $(\mathbb{R}^{n\times n}, +, \times)$

Neutral element for $+$: written 0
Neutral element for $\times$: written 1

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0$$

$\boxed{\text{Groups}} \subseteq \boxed{\text{Monoids}}$ $\boxed{\text{Rings}}$

Group “=” monoid with subtraction

$\boxed{\text{Groups}} \subseteq \boxed{\text{Monoids}}$

Group "=" monoid with subtraction

$\boxed{\text{Fields}} \subseteq \boxed{\text{Rings}}$

Field "=" commutative ring with division

$\boxed{\text{Groups}} \subseteq \boxed{\text{Monoids}}$ $\boxed{\text{Fields}} \subseteq \boxed{\text{Rings}}$

Group "=" monoid with subtraction Field "=" commutative ring with division

**Definition.** Let $(R, +, \times)$ be a ring. We call it a **field** if:

- every $a \neq 0$ has a multiplicative inverse: some $a^{-1}$ such that $a \times a^{-1} = 1$
- $\times$ is commutative

# Last stop: fields



$\boxed{\text{Groups}} \subseteq \boxed{\text{Monoids}}$ $\boxed{\text{Fields}} \subseteq \boxed{\text{Rings}}$

Group "=" monoid with subtraction Field "=" commutative ring with division

**Definition.** Let $(R, +, \times)$ be a ring. We call it a **field** if:

- every $a \neq 0$ has a multiplicative inverse: some $a^{-1}$ such that $a \times a^{-1} = 1$
- $\times$ is commutative

**Examples.** The following are fields:

- $(\mathbb{R}, +, \times)$
- $(\mathbb{Q}, +, \times)$
- Rational fractions (with addition and multiplication)
- $(\mathbb{Z}/d\mathbb{Z}, +, \times)$?

$[a]^{-1}$ exists if $a$ and $d$ are coprime

$d = 4$ $[2]_4$ has no inverse

<u>Theorem</u>

If $d$ prime: $(\mathbb{Z}/d\mathbb{Z}, +, \times)$ is a field.

$\boxed{\text{Groups}} \subseteq \boxed{\text{Monoids}}$ $\boxed{\text{Fields}} \subseteq \boxed{\text{Rings}}$

Group "=" monoid with subtraction Field "=" commutative ring with division

**Definition.** Let $(R, +, \times)$ be a ring. We call it a **field** if:

- every $a \neq 0$ has a multiplicative inverse: some $a^{-1}$ such that $a \times a^{-1} = 1$
- $\times$ is commutative

**Examples.** The following are fields:

- $(\mathbb{R}, +, \times)$
- $(\mathbb{Q}, +, \times)$
- Rational fractions (with addition and multiplication)
- $(\mathbb{Z}/d\mathbb{Z}, +, \times)$?

Most of what you learn for $\mathbb{R}^n$ is true for every $\mathbb{K}^n$ if $\mathbb{K}$ is a field
Since $\mathbb{Z}/2\mathbb{Z}$ is a field so:

- can talk about linear maps and inverses and ... with vectors in $\{0, 1\}^n$
- can talk about Fourier transforms
- a lot of modern CS (pratice and theory) does not exist without this algebraic concept

# Polynomials

**Definition.** Let $(R, +, \times)$ be a ring. A polynomial with coefficients in $R$ is an expression of the form

$$a_0 + a_1X + a_2X^2 + \cdots + a_mX^m$$

where $a_0, \ldots, a_m \in R$.

**Definition.** Let $(R, +, \times)$ be a ring. A polynomial with coefficients in $R$ is an expression of the form

$$a_0 + a_1 X + a_2 X^2 + \cdots + a_m X^m$$

where $a_0, \ldots, a_m \in R$.

- $a_i$ are called the coefficient of degree $i$ of the polynomial

**Definition.** Let $(R, +, \times)$ be a ring. A polynomial with coefficients in $R$ is an expression of the form

$$a_0 + a_1 X + a_2 X^2 + \cdots + a_m X^m$$

where $a_0, \ldots, a_m \in R$.

- $a_i$ are called the coefficient of degree $i$ of the polynomial
- Two polynomials are equal if, and only if, for every $i \in \mathbb{N}$, they have the same coefficient of degree $i$

**Definition.** Let $(R, +, \times)$ be a ring. A polynomial with coefficients in $R$ is an expression of the form

$$a_0 + a_1X + a_2X^2 + \cdots + a_mX^m$$

where $a_0, \ldots, a_m \in R$.

- $a_i$ are called the coefficient of degree $i$ of the polynomial
- Two polynomials are equal if, and only if, for every $i \in \mathbb{N}$, they have the same coefficient of degree $i$
- If $m \in \mathbb{N}$ is the largest integer such that $a_m \neq 0$, we say that it is the degree of the polynomial

# The most important ring: polynomials



**Definition.** Let $(R, +, \times)$ be a ring. A polynomial with coefficients in $R$ is an expression of the form

$$a_0 + a_1X + a_2X^2 + \cdots + a_mX^m$$

where $a_0, \ldots, a_m \in R$.

- $a_i$ are called the coefficient of degree $i$ of the polynomial
- Two polynomials are equal if, and only if, for every $i \in \mathbb{N}$, they have the same coefficient of degree $i$
- If $m \in \mathbb{N}$ is the largest integer such that $a_m \neq 0$, we say that it is the degree of the polynomial

**Notation.** The set of all polynomials with coefficients in $R$ is written $R[X]$.

- $2 + 5X$: polynomial in $\mathbb{Z}[X]$ of degree 1
- $5X + 2$: same polynomial, order of the terms does not matter
- $0X^2 + 5X + 2$: same polynomial, terms with 0 coefficient don't matter.

**Definition.** Let $(R, +, \times)$ be a ring. A polynomial with coefficients in $R$ is an expression of the form

$$a_0 + a_1 X + a_2 X^2 + \cdots + a_m X^m$$

where $a_0, \ldots, a_m \in R$.

- $a_i$ are called the coefficient of degree $i$ of the polynomial
- Two polynomials are equal if, and only if, for every $i \in \mathbb{N}$, they have the same coefficient of degree $i$
- If $m \in \mathbb{N}$ is the largest integer such that $a_m \neq 0$, we say that it is the degree of the polynomial

**Notation.** The set of all polynomials with coefficients in $R$ is written $R[X]$.

- $2 + 5X$: polynomial in $\mathbb{Z}[X]$ of degree 1
- $5X + 2$: same polynomial, order of the terms does not matter
- $0X^2 + 5X + 2$: same polynomial, terms with 0 coefficient don't matter.

Note: polynomials work over every ring! This is a polynomial with coefficients in $\mathbb{R}^{2\times 2}$:

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ 1 & \frac{1}{2} \end{pmatrix} X^2 + \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} X + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

**Definition.** Let $(R, +, \times)$ be a ring. A polynomial with coefficients in $R$ is an expression of the form

$$a_0 + a_1X + a_2X^2 + \cdots + a_mX^m$$

where $a_0, \ldots, a_m \in R$.

- $a_i$ are called the coefficient of degree $i$ of the polynomial
- Two polynomials are equal if, and only if, for every $i \in \mathbb{N}$, they have the same coefficient of degree $i$
- If $m \in \mathbb{N}$ is the largest integer such that $a_m \neq 0$, we say that it is the degree of the polynomial

$X^2 + X = X + X^2$

**Notation.** The set of all polynomials with coefficients in $R$ is written $R[X]$.

$0X^0 + 0X + 0X^2 = 0$

$1X^0 + 0X + 0X^2$

$\vdots$

$1 + X + X^2$

- $2 + 5X$: polynomial in $\mathbb{Z}[X]$ of degree 1
- $5X + 2$: same polynomial, order of the terms does not matter
- $0X^2 + 5X + 2$: same polynomial, terms with 0 coefficient don't matter.

Enumerate all the polynomials of degree $\leq 2$ with coefficients in $\mathbb{Z}/2\mathbb{Z}$.
How many are there?

- 1
- 2
- 4
- 8 ✓
- infinitely many

**Definition.** Let $(R, +, \times)$ be a ring. A polynomial with coefficients in $R$ is an expression of the form

$$a_0 + a_1 X + a_2 X^2 + \cdots + a_m X^m$$

where $a_0, \ldots, a_m \in R$.

- $a_i$ are called the coefficient of degree $i$ of the polynomial
- Two polynomials are equal if, and only if, for every $i \in \mathbb{N}$, they have the same coefficient of degree $i$
- If $m \in \mathbb{N}$ is the largest integer such that $a_m \neq 0$, we say that it is the degree of the polynomial

**Notation.** The set of all polynomials with coefficients in $R$ is written $R[X]$.

- $2 + 5X$: polynomial in $\mathbb{Z}[X]$ of degree 1
- $5X + 2$: same polynomial, order of the terms does not matter
- $0X^2 + 5X + 2$: same polynomial, terms with 0 coefficient don't matter.

**Implementation:** a polynomial $A \in R[X]$ is just implemented as an array `A` where `A[i]` is the coefficient of degree $i$.

$(X^2 + 2X + 2) + (X^3 + X + 1) = 3 + 3X + X^2 + X^3$ (things you already probably know)

$(X^2 + 2X + 2) \times (X^3 + X + 1) = X^5 + X^3 + X^2 + \dots + 2X^3 + 2X + 2$

$(X^2 + 2X + 2) + (X^3 + X + 1) =$ (things you already probably know)

$(X^2 + 2X + 2) \times (X^3 + X + 1) =$

$(X^2+2X+2)+(X^3+X+1)= \; X^3+X^2+3X+1$ (things you already probably know)

$(X^2+2X+2)\times(X^3+X+1)= \; X^5+2X^4+3X^3+3X^2+4X+2$

In general:

**Definition.** Let $A = a_0 + a_1X + \cdots + a_dX^d$ and $B = b_0 + b_1X + \cdots + b_dX^d$. Define

$$A + B = (a_0 + b_0) + (a_1 + b_1)X + \cdots + (a_d + b_d)X^d$$

and

$$A \times B = a_0b_0 + (a_0b_1 + a_1b_0)X + \cdots + a_db_dX^{2d}$$

$(X^2 + 2X + 2) + (X^3 + X + 1) = X^3 + X^2 + 3X + 1$ (things you already probably know)

$(X^2 + 2X + 2) \times (X^3 + X + 1) = X^5 + 2X^4 + 3X^3 + 3X^2 + 4X + 2$

In general:

**Definition.** Let $A = a_0 + a_1X + \cdots + a_dX^d$ and $B = b_0 + b_1X + \cdots + b_dX^d$. Define

$$A + B = (a_0 + b_0) + (a_1 + b_1)X + \cdots + (a_d + b_d)X^d$$

and

$$A \times B = a_0b_0 + (a_0b_1 + a_1b_0)X + \cdots + a_db_dX^{2d}$$

(Coefficient of degree $i$ in $A \times B$ is $\sum_{j=0}^{i} a_jb_{i-j}$)

$(X^2+2X+2)+(X^3+X+1) = X^3+X^2+3X+1$ (things you already probably know)

$(X^2+2X+2)\times(X^3+X+1) = X^5+2X^4+3X^3+3X^2+4X+2$

In general:

**Definition.** Let $A = a_0 + a_1X + \cdots + a_dX^d$ and $B = b_0 + b_1X + \cdots + b_dX^d$. Define

$$A + B = (a_0 + b_0) + (a_1 + b_1)X + \cdots + (a_d + b_d)X^d$$

and

$$A \times B = a_0b_0 + (a_0b_1 + a_1b_0)X + \cdots + a_db_dX^{2d}$$

(Coefficient of degree $i$ in $A \times B$ is $\sum_{j=0}^{i} a_jb_{i-j}$)

$\boxed{\text{Different operations! On different sets!}}$

$(X^2 + 2X + 2) + (X^3 + X + 1) = X^3 + X^2 + 3X + 1$ (things you already probably know)

$(X^2 + 2X + 2) \times (X^3 + X + 1) = X^5 + 2X^4 + 3X^3 + 3X^2 + 4X + 2$

In general:

**Definition.** Let $A = a_0 + a_1 X + \cdots + a_d X^d$ and $B = b_0 + b_1 X + \cdots + b_d X^d$. Define

$$A + B = (a_0 + b_0) + (a_1 + b_1)X + \cdots + (a_d + b_d)X^d$$

and

$$A \times B = a_0 b_0 + (a_0 b_1 + a_1 b_0)X + \cdots + a_d b_d X^{2d}$$

Different operations! On different sets!

(Coefficient of degree $i$ in $A \times B$ is $\sum_{j=0}^{i} a_j b_{i-j}$)

What happens to the degree?

- $\deg(A + B) \leq \max(\deg(A), \deg(B))$
- $\deg(A \times B) \leq \deg(A) + \deg(B)$
- $\deg(A \times B) = \deg(A) + \deg(B)$ if coefficients in a field (we define $\deg(0) = -\infty$ for this to be true)

$(X^2+2X+2)+(X^3+X+1) = X^3+X^2+3X+1$ (things you already probably know)

$(X^2+2X+2)\times(X^3+X+1) = X^5+2X^4+3X^3+3X^2+4X+2$

In general:

**Definition.** Let $A = a_0 + a_1X + \cdots + a_dX^d$ and $B = b_0 + b_1X + \cdots + b_dX^d$. Define

$$A + B = (a_0 + b_0) + (a_1+b_1)X + \cdots + (a_d+b_d)X^d$$

and

$$A \times B = a_0b_0 + (a_0b_1 + a_1b_0)X + \cdots + a_db_dX^{2d}$$

Different operations! On different sets!

(Coefficient of degree $i$ in $A\times B$ is $\sum_{j=0}^{i} a_jb_{i-j}$)

**Theorem.** Let $R$ be a ring. Then $(R[X],+,\times)$ is a ring.

**Theorem.** Let $a, b \in \mathbb{Z}$ with $a \neq 0$. There exists a unique pair of integers $q, r$ such that:

- $b = qa + r$
- $r \in \{0, \ldots, |a| - 1\}$

The first item makes sense if we see $a, b, q, r$ as polynomials, but the second does not.

**Theorem.** Let $\mathbb{K}$ be a field. Let $A, B \in \mathbb{K}[X]$ with $A \neq \mathbf{0}$.
There exists a unique pair $Q, R \in \mathbb{K}[X]$ of polynomials such that:

- $B = QA + R$
- $\deg(R) < \deg(A)$.

**Theorem.** Let $\mathbb{K}$ be a field. Let $A, B \in \mathbb{K}[X]$ with $A \neq \mathbf{0}$.
There exists a unique pair $Q, R \in \mathbb{K}[X]$ of polynomials such that:

- $B = QA + R$
- $\deg(R) < \deg(A)$.

what is called `divmod` in Python

**Theorem.** Let $\mathbb{K}$ be a field. Let $A, B \in \mathbb{K}[X]$ with $A \neq \mathbf{0}$.
There exists a unique pair $Q, R \in \mathbb{K}[X]$ of polynomials such that:

- $B = QA + R$
- $\deg(R) < \deg(A)$.

what is called `divmod` in Python

**Definition.** $A$ divides $B$ if $R = 0$

**Theorem.** Let $\mathbb{K}$ be a field. Let $A, B \in \mathbb{K}[X]$ with $A \neq \mathbf{0}$.
There exists a unique pair $Q, R \in \mathbb{K}[X]$ of polynomials such that:

- $B = QA + R$
- $\deg(R) < \deg(A)$.

what is called `divmod` in Python

**Definition.** $A$ divides $B$ if $R = 0$

```
def divmod(B,A):
  assert(A != 0)
  Q,R = 0,B
  while deg(R) >= deg(A):
    a,r = A[deg(A)],R[deg(R)]
    S = (r/a) * X**(deg(R)-deg(A))
    Q = Q+S
    R = R - S*A
  return (Q,R)
```

**Theorem.** Let $\mathbb{K}$ be a field. Let $A, B \in \mathbb{K}[X]$ with $A \neq \mathbf{0}$.
There exists a unique pair $Q, R \in \mathbb{K}[X]$ of polynomials such that:
- $B = QA + R$
- $\deg(R) < \deg(A)$.

what is called `divmod` in Python

**Definition.** $A$ divides $B$ if $R = 0$

```
def divmod(B,A):
  assert(A != 0)
  Q,R = 0,B
  while deg(R) >= deg(A):
    a,r = A[deg(A)],R[deg(R)]
    S = (r/a) * X**(deg(R)-deg(A))
    Q = Q+S
    R = R - S*A
  return (Q,R)
```

$$
\begin{array}{l|l}
X^6 + 3X^5 + 7X^4 + 7X^3 + 6X^2 + 3 & X^2 + 2X + 3 \\
\hline
 & X^4
\end{array}
$$

$$X^6 + 3X^5 + 7X^4 + 7X^3 + 6X^2 + 3 = (\qquad)(X^2 + 2X + 3) +$$

**Theorem.** Let $\mathbb{K}$ be a field. Let $A, B \in \mathbb{K}[X]$ with $A \neq \mathbf{0}$.
There exists a unique pair $Q, R \in \mathbb{K}[X]$ of polynomials such that:

- $B = QA + R$
- $\deg(R) < \deg(A)$.

what is called `divmod` in Python

**Definition.** $A$ divides $B$ if $R = 0$

```
def divmod(B,A):
  assert(A != 0)
  Q,R = 0,B
  while deg(R) >= deg(A):
    a,r = A[deg(A)],R[deg(R)]
    S = (r/a) * X**(deg(R)-deg(A))
    Q = Q+S
    R = R - S*A
  return (Q,R)
```

$$
\begin{array}{rrrrrr|l}
X^6 & +3X^5 & +7X^4 & +7X^3 & +6X^2 & +3 & X^2 + 2X + 3 \\
\cline{7-7}
-(X^6 & + 2X^5 & + 3X^4) & & & & X^4 + X^3 \\
\cline{1-6}
 & X^5 & +4X^4 & +7X^3 & +6X^2 & +3 &
\end{array}
$$

$$X^6 + 3X^5 + 7X^4 + 7X^3 + 6X^2 + 3 = (X^4 \qquad\qquad )(X^2 + 2X + 3) +$$

**Theorem.** Let $\mathbb{K}$ be a field. Let $A, B \in \mathbb{K}[X]$ with $A \neq \mathbf{0}$.
There exists a unique pair $Q, R \in \mathbb{K}[X]$ of polynomials such that:

- $B = QA + R$
- $\deg(R) < \deg(A)$.

what is called `divmod` in Python

**Definition.** $A$ divides $B$ if $R = 0$

```
def divmod(B,A):
  assert(A != 0)
  Q,R = 0,B
  while deg(R) >= deg(A):
    a,r = A[deg(A)],R[deg(R)]
    S = (r/a) * X**(deg(R)-deg(A))
    Q = Q+S
    R = R - S*A
  return (Q,R)
```

$$\begin{array}{rrrrrr|l}
X^6 & +3X^5 & +7X^4 & +7X^3 & +6X^2 & +3 & X^2+2X+3 \\
\hline
-(X^6 & +2X^5 & +3X^4) & & & & X^4+X^3+2X^2 \\
\hline
 & X^5 & +4X^4 & +7X^3 & +6X^2 & +3 & \\
 & -(X^5 & +2X^4 & +3X^3) & & & \\
\hline
 & & 2X^4 & +4X^3 & +6X^2 & +3 &
\end{array}$$

$$X^6 + 3X^5 + 7X^4 + 7X^3 + 6X^2 + 3 = (X^4 + X^3 \qquad )(X^2 + 2X + 3) +$$

**Theorem.** Let $\mathbb{K}$ be a field. Let $A, B \in \mathbb{K}[X]$ with $A \neq \mathbf{0}$.
There exists a unique pair $Q, R \in \mathbb{K}[X]$ of polynomials such that:

- $B = QA + R$
- $\deg(R) < \deg(A)$.

what is called `divmod` in Python

**Definition.** $A$ divides $B$ if $R = 0$

```
def divmod(B,A):
  assert(A != 0)
  Q,R = 0,B
  while deg(R) >= deg(A):
    a,r = A[deg(A)],R[deg(R)]
    S = (r/a) * X**(deg(R)-deg(A))
    Q = Q+S
    R = R - S*A
  return (Q,R)
```

$$
\begin{array}{rrrrrr|l}
X^6 & +3X^5 & +7X^4 & +7X^3 & +6X^2 & +3 & X^2+2X+3 \\
\hline
-(X^6 & +2X^5 & +3X^4) & & & & X^4+X^3+2X^2 \\
\hline
 & X^5 & +4X^4 & +7X^3 & +6X^2 & +3 & \\
 & -(X^5 & +2X^4 & +3X^3) & & & \\
\hline
 & & 2X^4 & +4X^3 & +6X^2 & +3 & \\
 & & -(2X^4 & +4X^3 & +6X^2) & & \\
\hline
 & & & & & 3X^0 &
\end{array}
$$

$$X^6 + 3X^5 + 7X^4 + 7X^3 + 6X^2 + 3 = (X^4 + X^3 + 2X^2)(X^2 + 2X + 3) +$$

**Theorem.** Let $\mathbb{K}$ be a field. Let $A, B \in \mathbb{K}[X]$ with $A \neq \mathbf{0}$.
There exists a unique pair $Q, R \in \mathbb{K}[X]$ of polynomials such that:

- $B = QA + R$
- $\deg(R) < \deg(A)$.

what is called `divmod` in Python

**Definition.** $A$ divides $B$ if $R = 0$

```
def divmod(B,A):
  assert(A != 0)
  Q,R = 0,B
  while deg(R) >= deg(A):
    a,r = A[deg(A)],R[deg(R)]
    S = (r/a) * X**(deg(R)-deg(A))
    Q = Q+S
    R = R - S*A
  return (Q,R)
```

$$
\begin{array}{rrrrrr|l}
X^6 & +3X^5 & +7X^4 & +7X^3 & +6X^2 & +3 & X^2+2X+3 \\
\hline
-(X^6 & +2X^5 & +3X^4) & & & & X^4+X^3+2X^2 \\
\cline{1-6}
 & X^5 & +4X^4 & +7X^3 & +6X^2 & +3 & \\
 & -(X^5 & +2X^4 & +3X^3) & & & \\
\cline{2-6}
 & & 2X^4 & +4X^3 & +6X^2 & +3 & \\
 & & -(2X^4 & +4X^3 & +6X^2) & & \\
\cline{3-6}
 & & & & & 3 &
\end{array}
$$

$$X^6 + 3X^5 + 7X^4 + 7X^3 + 6X^2 + 3 = (X^4 + X^3 + 2X^2)(X^2 + 2X + 3) + 3$$

**Theorem.** Let $\mathbb{K}$ be a field. Let $A, B \in \mathbb{K}[X]$ with $A \neq \mathbf{0}$.
There exists a unique pair $Q, R \in \mathbb{K}[X]$ of polynomials such that:

- $B = QA + R$
- $\deg(R) < \deg(A)$.

what is called `divmod` in Python

**Definition.** $A$ divides $B$ if $R = 0$

```
def divmod(B,A):
  assert(A != 0)
  Q,R = 0,B
  while deg(R) >= deg(A):
    a,r = A[deg(A)],R[deg(R)]
    S = (r/a) * X**(deg(R)-deg(A))
    Q = Q+S
    R = R - S*A
  return (Q,R)
```

We need $\mathbb{K}$ to be a field! Otherwise $1/a$ $(= a^{-1})$ does not necessarily exist.

**Example.** $A = 2, B = X$ polynomials in $\mathbb{Z}[X]$.

- Suppose $B = QA + R$, where $Q, R \in \mathbb{Z}[X]$
- Then $X = (q_0 + q_1 X)2 = 2q_0 + 2q_1 X$
- So $1 = 2q_1$

**Definition.** Let $A, B \in \mathbb{K}[X]$. We say that $D \in \mathbb{K}[X]$ is a gcd of $A$ and $B$ if:

- $D$ divides $A$ and $B$
- Every divisor of $A$ and $B$ has degree at most $\deg(D)$

(note: it is not unique. If $D$ is a gcd, then $2D$ is also a gcd)

$$\begin{array}{ccc} a & & b \\ & \searrow \; \swarrow & \\ & \gcd(a,b) & \end{array}$$

**Definition.** Let $A, B \in \mathbb{K}[X]$. We say that $D \in \mathbb{K}[X]$ is a gcd of $A$ and $B$ if:

- $D$ divides $A$ and $B$
- Every divisor of $A$ and $B$ has degree at most $\deg(D)$

(note: it is not unique. If $D$ is a gcd, then $2D$ is also a gcd)

Can be computed using Euclid's algorithm!
Also get Bézout's coefficients directly from this

```
def euclid(A,B):
  if deg(A) > deg(B):
    A,B = B,A # swap A and B
  if A == 0:
    return B

  remainders = [B,A]
  while remainders[-1] != 0:
    B = remainders[-2]
    A = remainders[-1]
    Q,R = divmod(B,A)
    remainders.append(R)

  return remainders[-2]
```

**Definition.** Let $A, B \in \mathbb{K}[X]$. We say that $D \in \mathbb{K}[X]$ is a gcd of $A$ and $B$ if:

- $D$ divides $A$ and $B$
- Every divisor of $A$ and $B$ has degree at most $\deg(D)$

(note: it is not unique. If $D$ is a gcd, then $2D$ is also a gcd)

Can be computed using Euclid's algorithm!
Also get Bézout's coefficients directly from this

```
def euclid(A,B):
  if deg(A) > deg(B):
    A,B = B,A # swap A and B
  if A == 0:
    return B

  remainders = [B,A]
  while remainders[-1] != 0:
    B = remainders[-2]
    A = remainders[-1]
    Q,R = divmod(B,A)
    remainders.append(R)

  return remainders[-2]
```

$\gcd(X^2 - X - 6, X^2 + 3X + 2)$

1. $X^2 - X - 6 = 1 \cdot (X^2 + 3X + 2) + (-4X - 8)$
2. $X^2 + 3X + 2 = (-1/4X - 1/4)(-4X - 8) + 0$

**Definition.** Let $A, B \in \mathbb{K}[X]$. We say that $D \in \mathbb{K}[X]$ is a gcd of $A$ and $B$ if:

- $D$ divides $A$ and $B$
- Every divisor of $A$ and $B$ has degree at most $\deg(D)$

(note: it is not unique. If $D$ is a gcd, then $2D$ is also a gcd)

Can be computed using Euclid's algorithm!
Also get Bézout's coefficients directly from this

```
def euclid(A,B):
  if deg(A) > deg(B):
    A,B = B,A # swap A and B
  if A == 0:
    return B

  remainders = [B,A]
  while remainders[-1] != 0:
    B = remainders[-2]
    A = remainders[-1]
    Q,R = divmod(B,A)
    remainders.append(R)

  return remainders[-2]
```

$$\gcd(X^2 - X - 6, X^2 + 3X + 2) = -4X - 8 = -4(X + 2)$$

$$X^2 - X - 6 = 1 \cdot (X^2 + 3X + 2) + (-4X - 8)$$

$$X^2 + 3X + 2 = (-1/4X - 1/4)(-4X - 8) + 0$$

$\exists\, U, V$ polynomials s.t.:

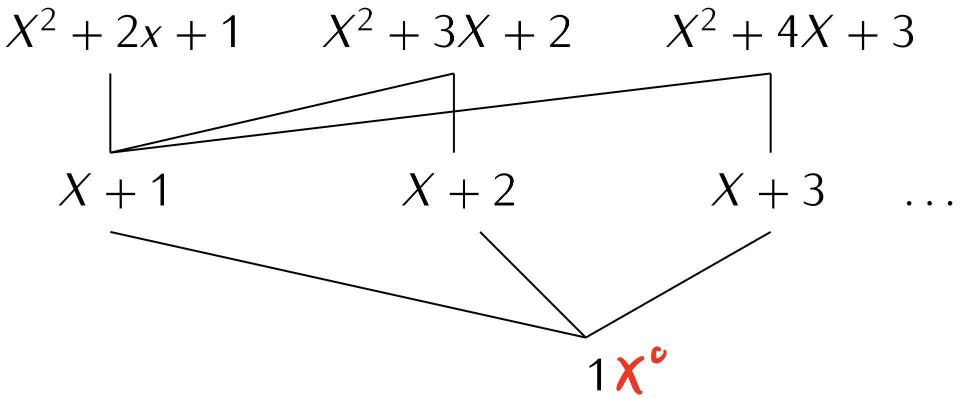
$$\gcd(A,B) = U \cdot A + V \cdot B$$

# polynomials over field ↔ integers

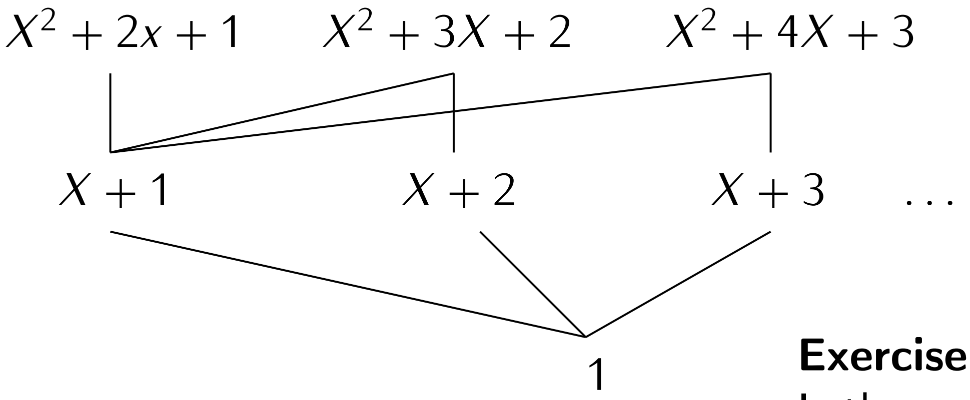
Antoine Wiehe

$(\mathbb{Z}/2\mathbb{Z})[X]$

- "$A$ divides $B$" is an order on $\mathbb{K}[X]$
- can define prime polynomials just like for numbers
- can prove the existence/uniquess of prime decompositions
- there are infinitely many prime polynomials
- can define an equivalence relation $\equiv_D$ for $D \in \mathbb{R}[X]$
- ...



- "$A$ divides $B$" is an order on $\mathbb{K}[X]$
- can define prime polynomials just like for numbers
- can prove the existence/uniquess of prime decompositions
- there are infinitely many prime polynomials
- can define an equivalence relation $\equiv_D$ for $D \in \mathbb{R}[X]$
- ...




**Exercise** Think about these things!
Is the polynomial $X^2 + 1$ in $\mathbb{R}[X]$ prime? Why/why not?

- Rings "ultimate" structures that generalizes the notions you know about addition/multiplication
- Commutative rings with division = fields
- Polynomials with coefficients in a field behave a lot like $\mathbb{Z}$ (division, gcd, primes, ...)
- fields/polynomials pop up all the time in CS

- Rings "ultimate" structures that generalizes the notions you know about addition/multiplication
- Commutative rings with division = fields
- Polynomials with coefficients in a field behave a lot like $\mathbb{Z}$ (division, gcd, primes, ...)
- fields/polynomials pop up all the time in CS

Next week

- A bit more about finite fields
- Application: error-correcting codes
  (QR codes, space communication, ...)

- Rings "ultimate" structures that generalizes the notions you know about addition/multiplication
- Commutative rings with division = fields
- Polynomials with coefficients in a field behave a lot like $\mathbb{Z}$ (division, gcd, primes, ...)
- fields/polynomials pop up all the time in CS

Next week

- A bit more about finite fields
- Application: error-correcting codes (QR codes, space communication, ...)

Final week

- Final exam organisation
- Recap of notions
- Quizzes