7. Rings

7.1 Definition of a ring

Definition 7.1.1

A **ring** $(R, +_R, \cdot_R)$ is a set R equipped with **two** binary **operations**

$$+_R : R \times R \to R \qquad \text{and} \qquad \cdot_R : R \times R \to R$$

such that the following axioms hold:

1. $(R, +_R)$ is an **abelian group** (the *additive* group). The identity element of this group is denoted by 0_R.
2. There exists an **identity element** 1_R for the operation $\cdot_R$ such that for all $x \in R$, we have
$$x \cdot_R 1_R = 1_R \cdot_R x = x.$$
3. The operation $\cdot_R$ is **associative**: for all $x, y, z \in R$, we have
$$(x \cdot_R y) \cdot_R z = x \cdot_R (y \cdot_R z).$$
4. The operations $+_R$ and $\cdot_R$ satisfy the **distributive laws**: for all $x, y, z \in R$, we have
$$x \cdot_R (y +_R z) = (x \cdot_R y) +_R (x \cdot_R z)$$
and
$$(x +_R y) \cdot_R z = (x \cdot_R z) +_R (y \cdot_R z).$$

Ex. 7.11: Identity elements

The only ring in which $1_R = 0_R$ is the zero-ring $(\{0_R\}, +_R, \cdot_R)$.

One element $\neq$ zero element

$$R \neq \{0_R\} \implies \boxed{1_R \neq 0_R}$$

It is **not** necessary to assume that $(R, +_R)$ is an **abelian** group: If $(R, +_R)$ is a non-necessarily-abelian group, then the other ring axioms would imply that for all $x, y \in R$, $x +_R y = y +_R x$.

Ex. 7.11

Let $(R, +_R, \cdot_R)$ be a ring. Then

1. $\forall x \in R:$ $\boxed{x \cdot_R 0_R = 0_R \cdot_R x = 0_R}$
2. $\boxed{0_R \neq 1_R}$ unless R is the zero-ring $(\{0_R\}, +_R, \cdot_R)$.

Ex. 7.15

Let $(R, +_R, \cdot_R)$ be a ring. Then

- $\forall u \in R:$ $\boxed{-u = (-1_R) \cdot_R u = u \cdot_R (-1_R)}$
- If u is a unit, then so is $-u$:

$$! \quad \boxed{u \in R^* \implies -u \in R^*} \quad !$$

From this we deduce that $(-1_R) \cdot_R (-1_R) = 1_R$ and thus any positive power m of -1_R is given by

$$(-1_R)^m = \begin{cases} 1_R & \text{if } m \text{ is even} \\ -1_R & \text{if } m \text{ is odd} \end{cases}.$$

Commutative ring

A ring $(R, +_R, \cdot_R)$ is called a **commutative ring** if the operation $\cdot_R$ is commutative.

Examples of commutative rings are $(R, +, \cdot)$ where $R \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$.

Powers in a commutative ring

In a **commutative** ring, for any $x, y \in R$ and any $n \in \mathbb{Z}_{\geq 0}$, we have

$$\boxed{(x \cdot_R y)^n = x^n \cdot_R y^n}$$

because $(x \cdot_R y) \cdot \ldots \cdot (x \cdot_R y) = (x \cdot_R x \cdots x) \cdot_R (y \cdot_R y \cdots y) = x^n \cdot_R y^n$.

Definition 7.1.5: Units and the set R^* of units

Let $(R, +_R, \cdot_R)$ be a ring. An element $x \in R$ is called a **unit** if there exists an element $y \in R$ such that

$$\boxed{x \cdot_R y = y \cdot_R x = 1_R}$$

The set of all units in R is denoted by R^*:

$$\boxed{R^* := \{x \in R \mid \exists y \in R : x \cdot_R y = y \cdot_R x = 1_R\}}$$

In other words: the set R^* consists of all elements x from R having a multiplicative inverse.
Just as for groups, **multiplicative inverses** (if they exist) **are unique** and one writes x^{-1} for this inverse.

Lemma 7.1.6: The group $(R^*, \cdot_R)$

Let $(R, +_R, \cdot_R)$ be a ring. Then

$$\boxed{(R^*, \cdot_R) \textbf{ is a group}} \text{ with identity element } 1_R.$$

Example: consider the ring $(\mathbb{Z}_6, +_6, \cdot_6)$. The units in this ring are 1 and 5.

We already showed in Chapter 3 that $(\mathbb{Z}_6, \cdot_6)$ is not a group, because $2, 3, 4$ do not have multiplicative inverses.
However, we defined the group $((\mathbb{Z}_n)^*, \cdot_n)$ in Chapter 3 with

$$(\mathbb{Z}_n)^* = \{z \in \mathbb{Z}_n \mid \gcd(z, n) = 1\}.$$

Now we see that this group is precisely the group of units of the ring $(\mathbb{Z}_n, +_n, \cdot_n)$:

$$(\mathbb{Z}_n)^* = \mathbb{Z}_n^*.$$

So, for the ring $(\mathbb{Z}_6, +_6, \cdot_6)$, we have $\mathbb{Z}_6^* = \{1, 5\}$.

Definition 7.1.11: Zero-divisor

Let $(R, +_R, \cdot_R)$ be a ring. An element $x \in R$ is called a **zero-divisor** if

$$\boxed{x \neq 0_R} \quad \text{and} \quad \boxed{\exists y \in R \setminus \{0_R\} : x \cdot_R y = 0_R \quad y \cdot_R x = 0_R}$$

WARNING: For rings R with at least one zero-divisor, then

$$x \cdot_R y = 0_R \quad \Longrightarrow \quad x = 0_R \quad y = 0_R$$

This **cancellation rule only** holds in rings without zero-divisors, i.e. in **integral domains**!

Deduction

A ring has **no zero-divisors** if and only if for all $x, y \in R$,

$$(x \neq 0_R \wedge y \neq 0_R) \implies (x \cdot_R y \neq 0_R).$$

or equivalently,

$$(x \cdot_R y) = 0_R \implies (x = 0_R \ \ y = 0_R).$$

Exercise 7.17: A unit is not a zero-divisor

Let $u \in R^*$ be a unit in the ring $(R, +_R, \cdot_R)$. Then u **is not a zero-divisor.**

Because of this fact, we conclude that:

fields $\subseteq$ integral domains

$$\boxed{\textbf{Every field is an integral domain.}}$$

To prove that for a field $(R, +, \cdot)$, with $R^* = R \setminus \{0\}$, there can be a zero-divisor, we would need to find $x, y \in R \setminus \{0\}$ such that $x \cdot y = 0$. But this is impossible because both x and y are units (by definition of a field) and thus not zero-divisors (by the exercise above).

Proposition 7.1.15

Let n be a positive integer and let $a \in \mathbb{Z}_n$ be an element different from 0.
Then **exactly one** of the following two statements is true in $(\mathbb{Z}_n, +_n, \cdot_n)$:

1. a is a zero-divisor $\iff \gcd(a, n) > 1$.
2. a is a unit $\iff \gcd(a, n) = 1$.

This is true because a unit can never be a zero-divisor (Exercise 7.17).

Ex. 7.16: The characteristic of a ring

Let $(R, +_R, \cdot_R)$ be a ring. The **characteristic** of R is defined as the smallest positive integer n such that

$$\boxed{\underbrace{1_R +_R 1_R +_R \cdots +_R 1_R}_{n \text{ times}} = 0_R}$$

and is denoted by

$$\boxed{\text{char}(R) := n}$$

If this sum **never reaches the zero element** 0_R, then the ring has **characteristic zero**, like for example $\boxed{\text{char}(\mathbb{Z}) = 0}$

Ex. 7.16: Boolean rings

A ring $(R, +_R, \cdot_R)$ is called a **Boolean ring** if for all $r \in R$, we have

$$r \cdot_R r = r^2 = r.$$

Every boolean ring is commutative and we can define

$$x \wedge y := x \cdot_R y, \quad x \ y := x +_R y +_R (x \cdot_R y), \quad x := 1_R +_R x.$$

Boolean rings have characteristic 2, since $1_R = -1_R \implies \underbrace{1_R +_R 1_R}_{2 \text{ times}} = 0_R.$

Why is $1_R = -1_R$ in a boolean ring? Because

$$1_R = 1_R \cdot_R 1_R = (-1_R) \cdot_R (-1_R) = -1_R.$$

7.2 Domains and fields

Integral domain

An **integral <u>domain</u>** is a **commutative** ring $(R, +, \cdot)$ with **<u>no zero-divisors</u>**.

Examples of integral domains are $(R, +, \cdot)$ where $R \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$.

Note that we now leave out the R subscripts for the operations $+$ and $\cdot$ when there is no risk of confusion.

Proposition 7.2.1

Let $(R, +, \cdot)$ be an (integral) domain (i.e. a commutative ring without zero-divisors).

$$\boxed{x \cdot y = 0 \implies x = 0 \ y = 0}$$

Consequently,

$$\boxed{x \cdot y = x \cdot z \quad \wedge \quad x \neq 0 \quad \implies \quad y = z}$$

So we see that

$$\boxed{\textbf{Te cancellation la olds in domains.}}$$

Why does the cancellation law hold in domains? Assume that $x, y, z \in R$ such that $x \cdot y = x \cdot z$ and $x \neq 0$. Then

$$x \cdot y - x \cdot z = 0 \implies x \cdot (y - z) = 0.$$

Because there are no zero-divisors in R and $x \neq 0$, we must have that $y - z = 0$, so $y = z$.

Definition 7.2.4: Field

A **field** is a **commutative** ring $(R, +, \cdot)$ such that

$$\boxed{R^* = R \setminus \{0\}}$$

Examples of fields are $(R, +, \cdot)$ where $R \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$.

Note that

$$\boxed{(\mathbb{Z}, +, \cdot) \textbf{ is not a field}}$$

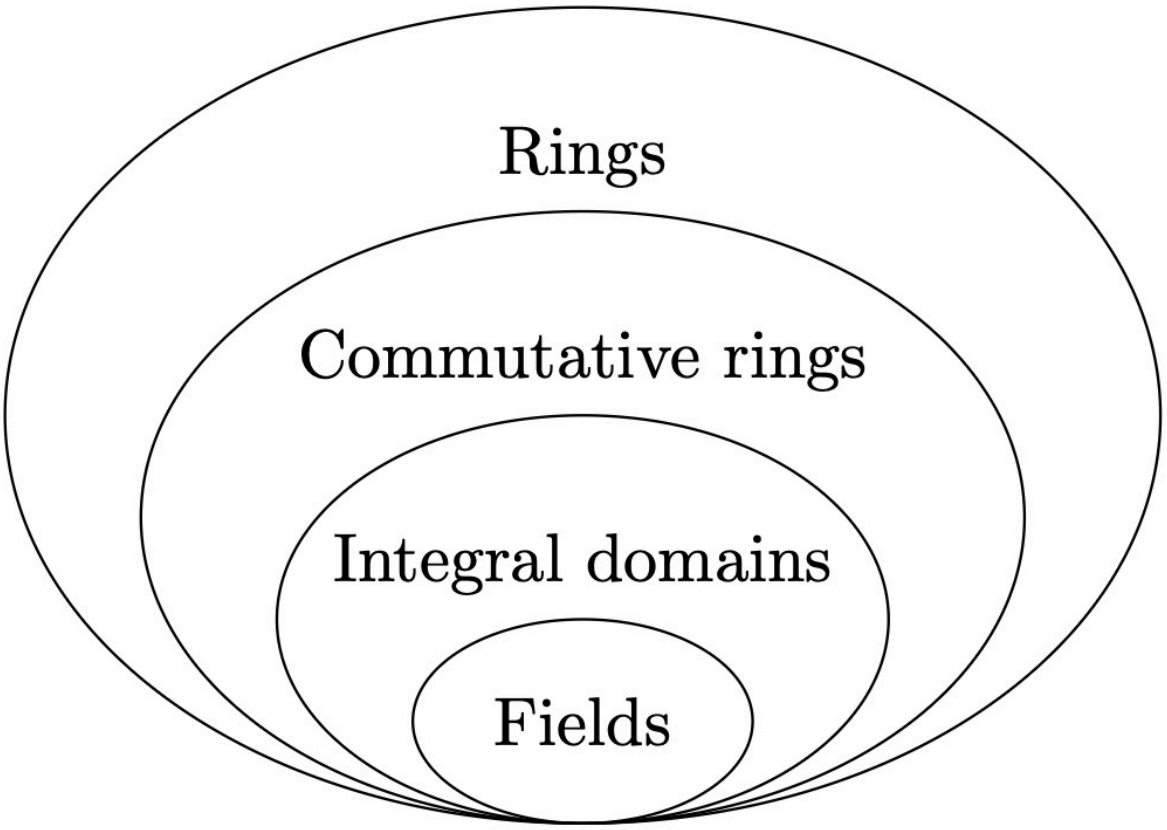
because not every non-zero integer has a multiplicative inverse in $\mathbb{Z}$! In fact, $\boxed{\mathbb{Z}^* = \{1, -1\}} \neq \mathbb{Z} \setminus \{0\}$.

Fields

If $(R, +, \cdot)$ is a field, then

1. every $x \in R \setminus \{0\}$ admits a multiplicative inverse for $\cdot_R$
2. $(R \setminus \{0\}, \cdot_R)$ is a group

In fact, $(R \setminus \{0\}, \cdot_R)$ is an abelian group because the ring is commutative!



Why are fields always integral domains?

Assume that $(R, +, \cdot)$ is a field and let $x, y \in R$ such that

$$x \cdot y = 0$$

If $x \neq 0$, then x is a unit (by definition of a field) and thus has a multiplicative inverse x^{-1}. Multiplying both sides of the equation $x \cdot y = 0$ by x^{-1} gives

$$x^{-1} \cdot (x \cdot y) = x^{-1} \cdot 0 \implies 1 \cdot y = 0 \implies y = 0.$$

Because there exists no $y \neq 0$ such that $x \cdot y = 0$, we conclude that x is not a zero-divisor. By symmetry, the same argument applies if $y \neq 0$. Therefore, a field has no zero-divisors and is thus an integral domain.

Exam

$$\boxed{(\mathbb{Z}_n, +_n, \cdot_n) \text{ is a field} \iff n \text{ is a prime number.}}$$

Finite field

A **finite field** is a field with a finite number of elements.

Finite field with p elements

Let p be a **prime** number. The **finite** field $\mathbb{Z}_p$ with p elements is denoted by

$$(\mathbb{Z}_p, +_p, \cdot_p) = \boxed{(_p, +_p, \cdot_p) = (\mathrm{GF}(p), +_p, \cdot_p)}$$

where $\mathrm{GF}(p)$ stands for **Galois Field** (*Évariste Galois*).

We write $_p$ instead of $\mathbb{Z}_p$ to emphasize that it is a **field** rather than just a ring.

Why is $(\mathbb{Z}_p, +_p, \cdot_p)$ *a field?* Because if p is a prime,

$$\begin{aligned} \mathbb{Z}_p^* &= \{p \in \mathbb{Z}_p \mid \gcd(p, n) = 1\} \\ &= \mathbb{Z}_p \setminus \{0\} \qquad \text{because the only divisor of } p \text{ is } 1 \text{ and } p \text{ itself.} \end{aligned}$$

so every non-zero element has a multiplicative inverse and thus $\mathbb{Z}_p$ is a field.

7.3 Polynomials with coefficients in a commutative ring

We will assume that

$$(R, +_R, \cdot_R) \text{ is a } \textbf{commutative ring}.$$

🕮 Definition 7.3.1: Polynomial with coefficients in R

Let $(R, +, \cdot)$ be a (commutative) ring. A **polynomial** $p()$ **with coefficients in** R is a formal expression of the form

$$p() = r_0 + r_1 + r_2{}^2 + \cdots + r_d{}^d$$

where $d \in \mathbb{Z}_{\geq 0}$ and $r_0, r_1, \ldots, r_d \in R$.

- The ring elements $r_0, r_1, \ldots, r_d$ are called the **coefficients** of the polynomial $p()$,
- is called the **indeterminate** of the polynomial.

If $r_d \neq 0$, then the **degree** of $p()$ is defined as

$$\deg(p()) = d,$$

and r_d is called the **leading coefficient**.

✎ Convention

The coefficient of ^{i} for $i > d$ is assumed to be 0_R. In other words, we can write any polynomial $p()$ as

$$\boxed{p() = \sum_{i=0}^{\infty} r_i{}^i} \text{ with } r_i = 0_R \text{ for } i > d$$

If a term $r_i{}^i$ has coefficient $r_i = 0_R$, then it is omitted.

🕮 Monic polynomial

A polynomial $p() \in R[]$ is called **monic** if its leading coefficient is $\boxed{r_d = 1_R}$.

For example, $p() = r_0 + r_1 + \ldots + {}^d$ is monic.

🕮 Zero polynomial

If $p() = 0_R$, then $p()$ is called the **zero polynomial** and its degree is defined as

$$\boxed{\deg(0_R) = -\infty}$$

🕮 Set of polynomials $R[]$

The **set of all polynomials** with coefficients in the ring R is denoted by

$$\boxed{R[]} := \{p() \mid p() \text{ is a polynomial with coefficients in } R\}.$$

WARNING: Be careful <u>not</u> to think of $p()$ as a map $p : R \to R$!
However, we can define an evaluation of $p()$ at a point $a \in R$ as follows:

$$p(a) = r_0 + r_1 a + r_2 a^2 + \cdots + r_d a^d \in R$$

🕮 Evaluation map

The **evaluation map** at a point $a \in R$ is the map

$$p \begin{cases} R & \to R \\ a & \mapsto p(a) \end{cases}$$

We have the risk of treating two different polynomials as the same if we think of them as maps.
However, **two distinct polynomials can have the same evaluation at all points in R.**

Consider for example $R = \mathbb{Z}_2 = \{0, 1\}$ and the two polynomials

$$p_1() = \quad \text{and} \quad p_2() = {}^2.$$

Then we have

$$p_1 \begin{cases} 0 & \mapsto 0 \\ 1 & \mapsto 1 \end{cases} \quad \text{and} \quad p_2 \begin{cases} 0 & \mapsto 0^2 = 0 \cdot_2 0 = 0 \\ 1 & \mapsto 1^2 = 1 \cdot_2 1 = 1 \end{cases}$$

So, both polynomials have the same evaluation at all points in $\mathbb{Z}_2$, even though they are different polynomials!

In general, a polynomial is **uniquely determined by its coefficients**. In other words, two polynomials $p() = \sum_{i=0}^{d} r_i{}^i$ and $q() = \sum_{i=0}^{e} s_i{}^i$ are equal if and only if $d = e$ and $r_i = s_i$ for all $i = 0, 1, \ldots, d$.

Polynomials are uniquely determined by their coefficients

Assume that

- $p() = \sum_{i=0}^{\infty} r_i{}^i \quad$ and $\quad \deg(p()) = d \implies r_i = 0 \text{ for } i > d,$
- $q() = \sum_{i=0}^{\infty} s_i{}^i \quad$ and $\quad \deg(q()) = e \implies s_i = 0 \text{ for } i > e.$

Then

$$\boxed{p() = q() \iff \forall i \in \{0, 1, 2, \ldots\} : r_i = s_i}.$$

Or in other notation,

$$\boxed{p() = q() \iff (r_0 r_1 \cdots) = (s_0 s_1 \cdots)}.$$

We can give a ring structure to $R[]$ by defining addition and multiplication of polynomials.

Definition 7.3.4: Addition and multiplication of polynomials

Let $p(), q() \in R[]$ be two polynomials defined as above:

$$p() = \sum_{i=0}^{d} r_i{}^i \quad \text{and} \quad q() = \sum_{i=0}^{e} s_i{}^i.$$

Where $d = \deg(p())$ and $e = \deg(q())$, so $r_i = 0$ for $i > d$ and $s_i = 0$ for $i > e$.
The **sum** $p() + q()$ and the **product** $p() \cdot q()$ are defined as follows:

$$\begin{aligned} p() + q() &= \sum_{j=0}^{\infty} (r_j + s_j)^j &&= \sum_{\ell=0}^{\max(d,e)} (r_\ell + s_\ell)^\ell \\ p() \cdot q() &= \sum_{i=0}^{\infty} \left(\sum_{j=0}^{i} r_j s_{i-j} \right)^i &&= \sum_{\ell=0}^{d+e} \left(\sum_{i=0}^{\ell} r_i s_{\ell-i} \right)^\ell \end{aligned}$$

For example,

$$(r_i{}^i) \cdot (s_j{}^j) = (r_i \cdot s_j)^{i+j},$$

but it is **not always true** that

$$\deg(p() \cdot q()) = \deg(p()) + \deg(q()).$$

This, in fact, **does** hold if R is an integral domain (Theorem 7.3.7).

Definition 7.3.5: The polynomial ring $(R[], +, \cdot)$

Let $(R, +, \cdot)$ be a commutative ring and let $R[]$ be the set of all polynomials with coefficients in R. Then the following holds:

$(R[], +, \cdot)$ equipped with the addition and multiplication of polynomials from Definition 7.3.4 is a ring:

$$\boxed{(R[], +, \cdot) \text{ is a ring}}$$

This ring is called the **ring of polynomials with coefficents in R**

Theorem 7.3.6: The polynomial ring $D[]$ over a domain D is a domain

Let $(D, +, \cdot)$ be an integral **domain**. Then

$$(D[], +, \cdot) \text{ is an integral } \mathbf{domain\ as\ ell}$$

It is tempting to say that $\deg(p() \cdot q()) = \deg(p()) + \deg(q())$, but this is **not** true in general. Clearly, it holds that $\deg(p() \cdot q()) \leq \deg(p()) + \deg(q())$, because the highest possible degree in the product $p() \cdot q()$ is $d + e$. To see what $\deg(p() \cdot q())$ really is, we have a look at the coefficient of the leading term $^{d+e}$ in the product $p() \cdot q()$:

$$\text{coefficient of } ^{d+e} = {}_{d+e}\sum_{j=0} r_j s_{(d+e)-j} = \boxed{r_d s_e}.$$

- $\boxed{j > d}$: $r_j = 0$, so $r_j s_{(d+e)-j} = 0$,
- $\boxed{j < d}$: $d - j > 0 \Rightarrow e + (d - j) > e$, so $s_{(d+e)-j} = 0$ and thus $r_j s_{(d+e)-j} = 0$,
- $\boxed{j = d}$: this is the only term that remains, so the coefficient of $^{d+e}$ in $p() \cdot q()$ is $r_d s_e$.

The only way for the degree of the product $p() \cdot q()$ to be **less** than $d + e$ is if $r_d s_e = 0$. Because $\deg(p()) = d$, r_d can't be zero. Completely analogously, s_e can't be zero either. So the only way for $r_d s_e = 0$ is if at least one of r_d or s_e is a zero-divisor. This cannot be the case if $(R, +, \cdot)$ is an integral domain, because then there are no zero-divisors.

We conclude that

Deduction

$$\deg(p() \cdot q()) \leq \deg(p()) + \deg(q())$$

- is a **strict** inequality if r_d or s_e is a **zero-divisor**
- is an **equality** if $(R, +, \cdot)$ is an **integral domain**, because then $r_d s_e \neq 0$.

Corollary 7.3.7: Degrees of products of polynomials over a domain

Let $(D, +, \cdot)$ be an integral **domain** and let $p(), q() \in D[]$ be two non-zero polynomials. Then

$$\boxed{\deg(p() \cdot q()) = \deg(p()) + \deg(q())}$$

7.4 Division with remainder for polynomials

Theorem 7.4.1: Division with remainder for polynomials over a commutative ring

Let $(R, +, \cdot)$ be a commutative ring and let $p(), q() \in R[]$ be two polynomials different from zero. Assume that $d()$ is **monic** (i.e. its leading coefficient is 1_R). Then there exist polynomials $q(), r() \in R[]$ such that

1. $p() = d() \cdot q() + r()$
2. $\deg(r()) < \deg(d())$

What if $d()$ is not monic? In that case, we can multiply both sides of the equation $p() = d() \cdot q() + r()$ by the multiplicative inverse of the leading coefficient of $d()$ (if it exists).

We defined the degree of the zero polynomial as $-\infty$ so that the condition $\deg(r()) < \deg(d())$ automatically holds.

The proof of this theorem gives an algorithm to compute the quotient and remainder polynomials $q()$ and $r()$. When performing this **division algorithm**, one ends up with a schematic following the following form:

$$\begin{array}{l|l|l} d(X) & p(X) & q(X) \\ \hline & \cdots & \\ \hline & \ddots & \\ \hline & r(X) & \end{array}$$

Factorizing a polynomial in $\mathbb{Z}_n[]$

1. Find roots of the polynomial $p()$ in $\mathbb{Z}_n$:
   - $p(1) \equiv 0 \pmod 6$?
   - $p(-1) \equiv 0 \pmod 6$? If so, $p(-1+n) \equiv 0 \pmod 6$, so $-1+n$ is a root.
   - $p(2) \equiv 0 \pmod 6$?
   - $p(-2) \equiv 0 \pmod 6$? If so, $p(-2+n) \equiv 0 \pmod 6$, so $-2+n$ is a root.
   - ...
2. a is a root $\implies p() = (-a) \cdot q()$ for some $q() \in \mathbb{Z}_n[]$ of degree $\deg(q()) = \deg(p()) - 1$ (Proposition 7.4.3).
3. Apply long division to compute $q()$. **The remainer should be $p(a) = 0$.**
4. Find roots of $q()$ and repeat until $q()$ cannot be factored anymore.

Root of a polynomial

Let $(R, +, \cdot)$ be a commutative ring and let $p() \in R[]$ be a polynomial. An element $a \in R$ is called a **root** of the polynomial $p()$ if

$$\boxed{p(a) = \sum_{i=0}^{\infty} r_i a^i = 0_R}$$

In other words, a is a root of $p()$ if and only if $p()$ evaluates to 0_R in a.

Finding a root of a polynomial $p() \in \mathbb{Z}_n[]$

For $a \in \mathbb{Z}_n$ to be a root of $p() \in \mathbb{Z}_n[]$, we need to have

$$p(a) = r_0 +_n r_1 a +_n r_2 a^2 +_n \cdots +_n r_d a^d = 0_{\mathbb{Z}_n} = 0$$

It holds that $a^i = \underbrace{a \cdot_n a \cdot \cdots \cdot_n a}_{i \text{ times}}$.

$$\implies \boxed{\textbf{it is sufficient to cec if } p(a) \equiv 0 \pmod{n}}$$

Proposition 7.4.3: Roots and factors of polynomials

Let $(R, +, \cdot)$ be a commutative ring and let $p() \in R[]$ be a *non-zero* polynomial of degree $\deg(p()) = n \geq 1$. Then there exists a polynomial $q() \in R[]$ of degree $\deg(q()) = n - 1$ such that

$$\boxed{p() = (\,-a) \cdot q() + p(a)}$$

Moreover, if a is a root of $p()$, then $(\,-a)$ divides $p()$:

$$\boxed{a \text{ is a root of } p()} \iff p() = (\,-a) \cdot q() \iff p() \text{ is divisible by } (\,-a).$$

▷▷ Corollary 7.4.4: Number of roots of a polynomial over a domain

Let $(D, +, \cdot)$ be an integral **domain** (or a field) and let $p() \in D[]$ be a **non-zero** polynomial. Then

$$\boxed{\deg(p()) = n \quad \implies \quad p() \textbf{ as at most } n \textbf{ distinct roots in } D}$$

Since Corollary 7.4.4 holds for any integral **domain**, it also holds for **fields**, since fields are integral domains.

The proof of 7.4.4 uses the **cancellation rule for domains**, so Corollary 7.4.4 holds for any integral domain, but it is in general **not** true if $(D, +, \cdot)$ has zero-divisors (and thus is not an integral domain).

Example: consider $2 \in \mathbb{Z}_4[]$. Note that $\mathbb{Z}_4$ has zero-divisors and hence is not an integral domain. The polynomial 2 has degree 1, but it has two distinct roots in $\mathbb{Z}_4$, namely 0 and 2, since $2 \cdot 0 = 0$ and $2 \cdot 2 = 4 \equiv 0 \mod 4$.

🕮 Definition: center of a ring

Let $(R, +_R, \cdot_R)$ be a ring. The **center** of the ring R is defined as

$$Z(R) := \{z \in R \mid \forall r \in R : z \cdot_R r = r \cdot_R z\}.$$

Exercise 7.12 : The center of a ring

Let $(R, +_R, \cdot_R)$ be a ring. Then

$$Z(R) \text{ is a commutative ring contained in } R.$$

and

$$Z(R) = R \quad \iff \quad (R, +_R, \cdot_R) \text{ is a commutative ring.}$$

Why is $Z(R) = R$ if and only if R is a commutative ring? If $Z(R) = R$, then for all $r_1, r_2 \in R$, we have that $r_1 \in Z(R)$ and thus $r_1 \cdot_R r_2 = r_2 \cdot_R r_1$, so the ring is commutative. Conversely, if the ring is commutative, then for all $z \in R$ and all $r \in R$, we have that $z \cdot_R r = r \cdot_R z$, so $z \in Z(R)$ and thus $Z(R) = R$.