A ring $R$ is a set with two operations $+$, such that

1. $(R, +)$ is an abelian group
2. $\cdot$ is associative and has a neutral element 1
3. There is distributivity

$$x \cdot (y + z) = (x \cdot y) + (x \cdot z)$$

$$x + (y \cdot z) = (x \cdot z) + (y \cdot z)$$

A ring is called commutative if $\cdot$ is commutative.

(All rings from now on are commutative.)
If a ring has elements $x, y$ where $x \neq 0, y \neq 0, xy = 0$
then $x, y$ are called **zero divisors**.

If a commutative ring $R$ has no zero divisors
then $R$ is called an **integral domain**.

If every non-zero element $x \in R$ has a
reciprocal ($= multiplicative inverse$), we call
$R$ a **field**.

(Examples of fields: $\mathbb{Q}$ - rational numbers
$\mathbb{R}$ - real numbers
$\mathbb{C}$ - complex numbers)
Examples of integral domains which are not fields:

\( \mathbb{Z} \) - integers.

If \( R \) is an integral domain,

\( R[x] = \text{polynomials in one variable } x \text{ with coefficients in } R \)

\[ a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0, \quad a_0, \ldots, a_n \in R \]

\( a_n \neq 0 \)

0 is also a polynomial.
Technically, a polynomial is just the \((n+1)\)-tuple of elements of \(\mathbb{F}\): \((a_n, a_{n-1}, \ldots, a_1, a_0)\).

Example: \(\mathbb{Z}/5\mathbb{Z} = \mathbb{F}_5\) (\(\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p\) if \(p\) prime, considered as a field).

\[ x^5 - x \in \mathbb{F}_5[x] \]

\[ (1, 0, 0, 0, -1, 0) \]

\[ \begin{array}{c|c|c}
\mathbb{F}_5 \times \mathbb{F}_5 & x^5 - x \in \mathbb{F}_5 \\
0 & 0 \\
1 & 0 \\
2 & 0 \\
3 & 0 \\
4 & 0 \\
\end{array} \]

the function corresponding to the polynomial is 0, but the polynomial isn't.
Why polynomials over an integral domain $R$ form an integral domain? (Just look at the top coefficient.)

\[
\begin{align*}
&\left( a_n x^n + \text{LOT} \right) \left( b_m x^m + \text{LOT} \right) = \\
&\left( a_n x^n + \sum_{i=1}^{\infty} a_i x^i \right) \left( b_m x^m + \sum_{i=1}^{\infty} b_i x^i \right) \\
&= a_m b_m x^{n+m} + \text{LOT} \\
\neq 0 & \text{ since } R \text{ is an integral domain.}
\end{align*}
\]
Polynomials do not form a field.

\[ \mathbb{R}[x, y] = (\mathbb{R}[x])[y] \]

ring

\[ = (\mathbb{R}[y])[x]. \]

Theorem: A finite integral domain is a field. □

finitely many elements

Ex. Commutative rings which are not integral
domains: \( \mathbb{Z}/k \mathbb{Z} \)

\( k \) is not a prime (e.g., 1, -1)

\( \mathbb{Z}/k \mathbb{Z} [x] \)

The general formulations of how we constructed \( \mathbb{Z}/k \mathbb{Z} \) as a ring.

If \( R \) is a commutative ring and \( I \in (R_+^+) \) is a subgroup, then we can always form cosets \( (R/I, +) \): an abelian group. What is the condition that will guarantee
being able to multiply cosets?

\[(x + I) - (y + I) = x \cdot y + I\]

\[
\sqrt{\text{not in}}
\]

additive notation

I need to say: if \(x - x' \in I\), \(y - y' \in I\)

\[
x \cdot y - x' \cdot y' \in I
\]

\[
= x \cdot y - x' \cdot y + x' \cdot y - x' \cdot y'
\]

\[
= (x - x') \cdot y + x' \cdot (y - y')
\]

\[
\in I
\]

\[
\in I
\]
The condition we need to ask of $I$ is:

$I \leq (\mathbb{R}, +)$ be an abelian subgroup, and an $R$-multiple of an element of $I$ as always in $I$: If $a \in I$ and $r \in R$ then $r \cdot a \in I$

If $I$ satisfies this, $I$ is called an **ideal**.

Redekind
(HW) Prove that the set of all polynomials

\[ a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Q}[x] \]

such that \( a_0 = 0 \), and \( 0 \in \mathbb{Q}[x] \)

forms an ideal.