Algebra MATH-310

Lecture 8

Anna Lachowska

November 10, 2025

Plan of the course

1. Integers: 1 lecture
2. Groups: 6 lectures
3. Rings and fields: 5 lectures
4. Review: 1 lecture

Today: Rings: lecture 1

a) Rings: definition and first examples.
b) Zero divisors. Integral domains.
c) The ring $\mathbb{Z}/n\mathbb{Z}$
d) Ideals in a commutative rings. Intersection, sum and product of ideals.
e) Ideals in $\mathbb{Z}$ and in polynomial rings.

Rings: definition

Definition

A ring is a set A with two operations: $+$ and $\cdot$ satisfying the axioms:

1. A is an abelian group with respect to $+$ with the neutral element $0 \in A$.
2. The multiplication $\cdot$ is associative:

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \qquad \forall a, b, c \in A.$$

3. There exists the element $1 \in A$, $1 \neq 0$, such that

$$1 \cdot a = a \cdot 1 = a \qquad \forall a \in A.$$

4. Distributivity:

$$a \cdot (b + c) = a \cdot b + a \cdot c, \quad (a + b) \cdot c = a \cdot c + b \cdot c \quad \forall a, b, c \in A.$$

Rings: examples

Example 0. Any field; $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$

Example 1. $A = \mathbb{Z}$. $+, \cdot, 0, 1$ $(\mathbb{Z}, +, 0)$ is an abelian group

$n+m \in \mathbb{Z}$, $n \cdot m \in \mathbb{Z}$

$2 \in \mathbb{Z}$ no multiplicative inverse $\frac{1}{2} \notin \mathbb{Z}$

Example 2. $A = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2}\}_{a,b \in \mathbb{Z}}$. $0 \in A$, $1 \in A$

$\forall\, a, b, c, d \in \mathbb{Z}$

$-a - b\sqrt{2} \in \mathbb{Z}$

$(a+b\sqrt{2}) + (c+d\sqrt{2}) = \underbrace{(a+c)}_{\in \mathbb{Z}} + \underbrace{(b+d)}_{\in \mathbb{Z}}\sqrt{2} \in A$

$(a+b\sqrt{2}) \cdot (c+d\sqrt{2}) = \underbrace{a \cdot c + 2b \cdot d}_{\in \mathbb{Z}} + \underbrace{(ad+bc)}_{\in \mathbb{Z}}\sqrt{2} \in A$

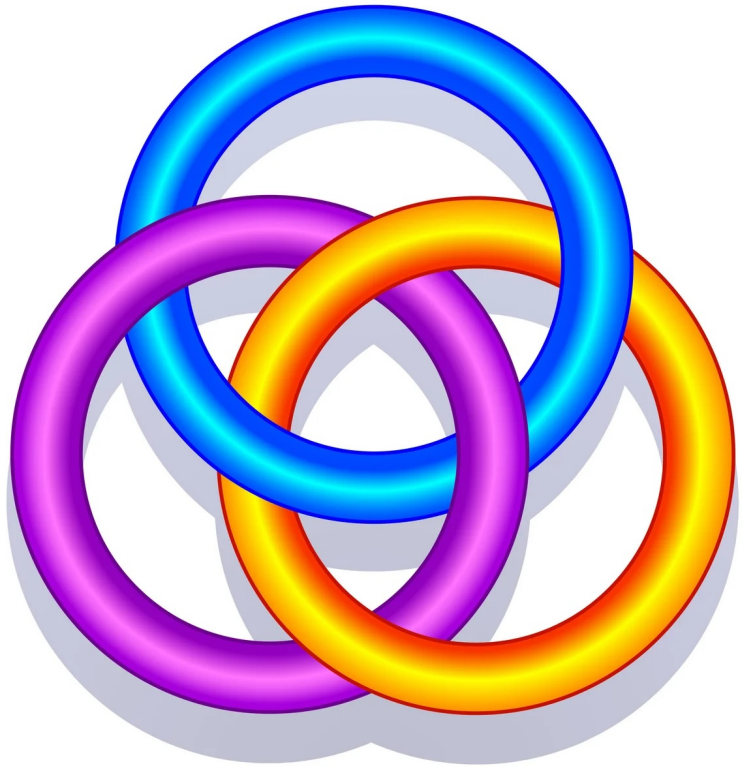
Consider $\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \underbrace{\frac{a}{a^2-2b^2}}_{\notin \mathbb{Z}} - \underbrace{\frac{b}{a^2-2b^2}}_{\notin \mathbb{Z} \text{ in general}}\sqrt{2} \notin A \Rightarrow$ no multiplicative inverse in general

A is a ring, not a field.

Example 3. $A = \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2}\}_{a,b \in \mathbb{Q}}$.

Exercise: this is a field

Why rings?



Borromean rings (nothing to do with algebraic rings, but important in topology and they are pretty)

Visit Borromean islands in Lago Maggiore

- They generalize fields such as $\mathbb{R}$ and $\mathbb{C}$.
- They are the next structure in complexity after groups.
- They provide an approach to study finite fields, useful in cryptography.

Commutative rings

Definition

A ring A is commutative if the multiplication is commutative:

$$a \cdot b = b \cdot a \qquad \forall a, b \in A.$$

Remark

If $a \in A$, then $a + a + a \ldots + a = na \in A$, similarly $-a - a - \ldots - a = -na \in A$, therefore $ka \in A$ for all $k \in \mathbb{Z}$. Many formulas known for numbers hold in commutative rings, for example

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \qquad \forall a, b \in A.$$

We will consider only commutative rings in this course.

Zero divisors

Definition

An element $a \in A$ is a zero divisor if there exists $x \in A$ such that $x \neq 0$ and $a \cdot x = 0$.

Example: $0 \in A$ is a zero divisor:

$0 = 0 + 0$

$0 \cdot x = (0+0) \cdot x = 0 \cdot x + 0 \cdot x \quad \forall x \in A$

$+ \quad (-0 \cdot x) \qquad (-0 \cdot x)$

$0 \qquad = 0 \cdot x$

Example: Rings without nontrivial ($\neq 0$) zero divisors:

$\mathbb{Z}$ $\quad n \cdot m = 0 \Rightarrow n = 0$ or $m = 0$ or both

$\mathbb{R}$

$\mathbb{C}$

The ring $\mathbb{Z}/n\mathbb{Z}$

Let $A = \mathbb{Z}/n\mathbb{Z} = \{[0], [1], \dots [n-1]\}$ equivalence classes modulo n.

wrt $+$: $\mathbb{Z}/n\mathbb{Z}$ is a cyclic group C_n ; $[1] \in \mathbb{Z}/n\mathbb{Z}$ neutral elt wrt. closed wrt. $\Rightarrow$ $\mathbb{Z}/n\mathbb{Z}$ is a ring

$[a] \in A : \ \gcd(a, n) = d > 1$	$[a] \in A : \ \gcd(a, n) = 1$
$[a]\left[\frac{n}{d}\right] = [0]$ in $\mathbb{Z}/n\mathbb{Z}$ $\Rightarrow [a]$ is a zero divisor	By Bezout's thm $\Rightarrow \exists x, y \in \mathbb{Z}$: $ax + ny = 1 \Leftrightarrow [a]\cdot[x] = [1]$ in $\mathbb{Z}/n\mathbb{Z}$ $\Leftrightarrow [a]$ has a multiplicative inverse in $\mathbb{Z}/n\mathbb{Z}$ if $[b]\cdot[a] = 0 \Rightarrow [b]\cdot[a]\cdot[a^{-1}] = [b]$ $[0]$ $[1]$ // $\Rightarrow [0]\cdot[a^{-1}] = [0]$ $\Rightarrow$ if $[b]\cdot[a] = 0 \Rightarrow [b] = 0$ $\Rightarrow [a]$ is not a zero divisor in $\mathbb{Z}/n\mathbb{Z}$

Conclusion: An element $[a] \in \mathbb{Z}/n\mathbb{Z}$ is either a zero divisor, or invertible.

Integral domain

Definition

A commutative ring with no nontrivial ($\neq 0$) zero divisors is called an integral domain.

Definition

A commutative ring where all nonzero elements have multiplicative inverses is called a field.

Corollary

The ring $\mathbb{Z}/n\mathbb{Z}$ either has nontrivial zero divisors, or it is a field.

Proof: No nontrivial zero divisors $\Leftrightarrow$ no $a \in \mathbb{Z}$: $1 \leq a \leq n-1$ and $\gcd(a,n) > 1$ $\Leftrightarrow$ n has no divisors except 1 and n $\Leftrightarrow$ $n = p$ is a prime

$\forall [b] \neq 0 \in \mathbb{Z}/p\mathbb{Z}$, $\gcd(b,p) = 1 \Leftrightarrow$ $[b]$ has a multiplicative inverse $\Leftrightarrow$ $\mathbb{Z}/p\mathbb{Z}$ is a field. ▨

The ring $\mathbb{Z}/n\mathbb{Z}$

Examples. $\mathbb{Z}/5\mathbb{Z} = \{[0], [1], [2], [3], [4]\}$ all except $[0]$ have multiplicative inverses

$[1]^2 = [1]$; $[2]\cdot[3] = [1]$, $[4]\cdot[4] = [1] \Rightarrow \mathbb{Z}/5\mathbb{Z}$ is a field.

$\mathbb{Z}/6\mathbb{Z} = \{[0], [1], [2], [3], [4], [5]\}$

$[2]\cdot[3] = [0]$ $[4]\cdot[3] = [0]$ nontrivial zero divisors

$\Rightarrow \mathbb{Z}/6\mathbb{Z}$ is not an integral domain

Fields are integral domains

Proposition

A field is an integral domain. An invertible element in a ring is not a zero divisor.

Proof: Suppose $a \cdot b = 0$, $a \neq 0$. If $\exists a^{-1} \in A \Rightarrow a \cdot a^{-1} = 1$

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

$a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 = 0$

$\Rightarrow b = 0$ if a is invertible and $ab = 0$

$\Rightarrow$ an invertible elt cannot be a zero divisor

If A is a field $\Rightarrow$ all nonzero elts are invertible $\Rightarrow$ they are not zero divisors $\Rightarrow$ A is an integral domain ∎

Remark: the converse is false. An integral domain is not necessarily a field

Example: $\mathbb{Z}$ is an integral domain, but not a field.

Conclusions

- Fields $\subset$ Integral domains $\subset$ Commutative rings
- $\mathbb{Z}/n\mathbb{Z}$ is an integral domain $\iff$ $\mathbb{Z}/n\mathbb{Z}$ is a field $\iff$ $n = p$ is a prime.

Ideals in a ring

Definition

Let A be a commutative ring. Then $I \subset A$ is an ideal if I has the following properties:

1. I is a subgroup with respect to $+$:
   $0 \in I$ and if $a, b \in I$, then $-a \in I$ and $a + b \in I$.
2. $\forall x \in A$, $a \in I$ we have $x \cdot a \in I$.

Example 1. $A = \mathbb{Z} \Rightarrow 2\mathbb{Z} = \{2k, k \in \mathbb{Z}\} \subset \mathbb{Z}$ is an ideal

$2a + 2b = 2(a+b) \in 2\mathbb{Z}$, $-2a \in 2\mathbb{Z}$, $0 \in 2\mathbb{Z}$, $\forall x \in \mathbb{Z}$, $2a \cdot x \in 2\mathbb{Z}$

Let $d \in \mathbb{Z} \Rightarrow I = d\mathbb{Z}$ is an ideal, similarly

Example 2. A any ring.

$\{0\} \subset A$ is an ideal : $0 \cdot x = 0 \quad \forall x \in A$

$A \subset A$ is an ideal : $x \cdot y \in A \quad \forall x, y \in A$

Properties of ideals

Definition

An ideal $I \subset A$ is proper if $I \neq A$.
An ideal $I \subset A$ is nontrivial if $I \neq \{0\}$.

Proposition

Let A be a commutative ring.

1. $I \subset A$ *is an ideal and* $1 \in I \implies I = A$: $1 \cdot x = x \in I \ \forall x \in A \Rightarrow I = A$
2. $I, J \subset A$ *two ideals* $\implies I \cap J \subset A$ is an ideal in A
3. $I, J \subset A$ *two ideals* $\implies I + J = \{x + y\}_{x \in I, y \in J} \subset A$ is an ideal in A
4. $I, J \subset A$ *two ideals* $\implies I \cdot J = \{\sum_i x_i \cdot y_i\}_{x_i \in I, y_i \in J} \subset A$ is an ideal in A
5. $I, J \subset A$ *two ideals* $\implies I \cup J \subset A$ is not an ideal in general

Properties of ideals: proof

(2) I, J ideals in A, $x, y \in I \cap J \Rightarrow x+y \in I$, $x+y \in J \Rightarrow x+y \in I \cap J$

$0 \in I$, $0 \cdot 6 \in J \Rightarrow 0 \in I \cap J$, $-x \in I$, $-x \in J \Rightarrow -x \in I \cap J \Rightarrow I \cap J$ additive subgroup.

If $a \in A \Rightarrow x \cdot a \in I$ and $x \cdot a \in J \Rightarrow x \cdot a \in I \cap J \Rightarrow I \cap J$ is an ideal.
$x \in I \cap J$

(3) I, J ideals $\Rightarrow$ let $\underset{\in I}{x_1} + \underset{\in J}{x_2} \in I+J$, $\underset{\in I}{y_1} + \underset{\in J}{y_2} \Rightarrow x_1 + x_2 + y_1 + y_2 = \underset{\in I}{(x_1 + y_1)} + \underset{\in J}{(x_2 + y_2)} \in I+J$

$\Rightarrow I+J$ additive subgroup

If $a \in A \Rightarrow a \cdot (x+y) = \underset{\in I}{a \cdot x} + \underset{\in J}{a \cdot y} \in I+J \Rightarrow I+J$ is an ideal.

(4) I, J ideals $\Rightarrow \left\{ \sum_i x_i y_i \right\}_{x_i \in I,\, y_i \in J}$ closed wrt $+$, $0 \in I \cdot J$, $\sum_i (-x_i) y_i \in I \cdot J$

$\Rightarrow$ additive subgroup

If $a \in A \Rightarrow a \cdot \sum_i x_i y_i = \sum_i \overbrace{(a x_i)}^{\in I} \underset{\in J}{y_i} \in I \cdot J \Rightarrow I \cdot J$ is an ideal.

(5) Example: $I = 2\mathbb{Z}$, $J = 3\mathbb{Z} \Rightarrow I \cup J = \{0, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 9, \ldots\}$

But $2+3 = 5 \notin I \cup J \Rightarrow$ not an additive subgroup.

Ideals in a ring

Example. Let $A = \mathbb{Z}$, $I = 6\mathbb{Z}$, $J = 10\mathbb{Z}$ ideals

(1) $I \cap J = \{z \in \mathbb{Z} : z = 6n \text{ and } z = 10m\}_{n,m \in \mathbb{Z}} =$

$= \{$ all multiples of 6 and 10$\} = \{$multiples of $\operatorname{lcm}(6,10) = 30\} =$

$= 30 \cdot \mathbb{Z}$

(2) $I + J = \{6n + 10m\}_{n,m \in \mathbb{Z}} \overset{\text{Bezout's thm}}{=} \{\gcd(6,10) \cdot \mathbb{Z}\} = 2\mathbb{Z}$

$6x + 10y = k \iff \gcd(6,10)$ divides k

(3) $I \cdot J = \{\sum_i 6n_i \cdot 10m_i \;,\; n_i, m_i \in \mathbb{Z}\} = \{60 \sum_i n_i m_i \;,\; m_i, n_i \in \mathbb{Z}\} = 60\mathbb{Z}$

Ideals in $\mathbb{Z}$.

Conclusion: Let $I = n\mathbb{Z}$, $J = m\mathbb{Z}$ ideals in $\mathbb{Z}$. Then $\forall n, m \in \mathbb{Z}^*$ we have

1. $I \cap J = \operatorname{lcm}(n, m)\mathbb{Z}$.
2. $I + J = \gcd(n, m)\mathbb{Z}$.
3. $I \cdot J = (n \cdot m)\,\mathbb{Z}$.

Remark $I, J \subset A$ two ideals $\Rightarrow$

$$I \cdot J \subset I \cap J \subset \begin{matrix} I \\ \subset \\ J \end{matrix} \subset I + J$$

$\sum x_i y_i \in I \cap J$ ($x_i \in I$, $y_i \in J$)

$x \in I \Rightarrow x + 0 \in I + J$ ($x \in I$, $0 \in J$)

Polynomial ring

Let $A = \mathbb{R}[x]$ polynomials in one variable with real coefficients.
Then A is a ring.

$f(x) + g(x) \in \mathbb{R}[x]$ a polynomial, $-f(x) \in \mathbb{R}[x]$,
$0 \in \mathbb{R}[x]$

$f(x) \cdot g(x) =$ a polynomial $\in \mathbb{R}[x]$

$1 \in \mathbb{R}[x]$

Consider

$I = \{(x+5) \cdot f(x)\}_{f(x) \in A}$ and $J = \{(x^2+2) \cdot f(x)\}_{f(x) \in A}$

1. $I \cap J =$ $\{(x+5)(x^2+2) f(x)\}_{f(x) \in A}$

Polynomial ring

2. $I \cdot J = \{ \sum (x+5) f_i(x) (x^2+2) g_i(x) \}_{g_i, f_i \in A} = \{ (x+5)(x^2+2) f(x) \}_{f(x) \in A}$.

3. $I + J = \{ (x+5) f(x) + (x^2+2) g(x) \}_{f(x), g(x) \in A}$

$$(x+5)\underbrace{(x-5)\left(-\frac{1}{27}\right)}_{f(x)} + (x^2+2)\underbrace{\left(+\frac{1}{27}\right)}_{g(x)} = 1 \in \mathbb{R}[x]$$

$$\Rightarrow I + J \ni 1 \Rightarrow I + J = \mathbb{R}[x]$$

Poll: Consider the ring $\mathbb{R}[x]$ and let

$$I = \{(x-1)^2 \cdot f(x)\}_{f(x)\in\mathbb{R}[x]}, \quad J = \{(x-1)(x+2) \cdot f(x)\}_{f(x)\in\mathbb{R}[x]}.$$

Then

A: $I \cap J = I \cdot J$

B: $I + J = \mathbb{R}[x]$

C: $(I + J) \cap (I - J) = I \cap J$

D: $J \cdot (I + J) = I \cap J$

E: $I \cdot (I + J) = J \cdot (I + J)$

$I \cap J = \{(x-1)^2(x+2) f(x)\}$

$I + J = \{(x-1) f(x)\}$

$(I + J) \cap (I - J) = \{(x-1) f(x)\}$

$J \cdot (I + J) = \{(x-1)^2 \cdot (x+2) f(x)\}$

$I \cdot (I + J) = \{(x-1)^3 f(x)\}$

$\{(x-1)^2 f + (x-1)(x+2) g\} = \{(x-1)\underbrace{((x-1) f + (x+2) g)}_{(x-1)(-\frac{1}{3}) + (x+2)(\frac{1}{3}) = 1}\} = \{(x-1) p(x)\}_{p(x)\in\mathbb{R}[x]}$

Principal ideal

Definition

Let $S \subset A$ be a subset of a ring. Let I be the minimal ideal that contains S. Then $I = (S)$ is the ideal generated by the set S.

$$S = \{s_i\} \implies \left\{ \sum_i a_i s_i \right\}_{a_i \in A} = (S).$$

Definition

Ideal $I \subset A$ is called principal if $I = (x)$ is generated by a single element.

$$I = \{x \cdot a\}_{a \in A}.$$

Example. $\{0\} = (0) \subset A$, $A = (1) \subset A$ are principal ideals

$n\mathbb{Z} \subset \mathbb{Z}$ is principal: $n\mathbb{Z} = (n)$

Ideals in a field

Proposition

A ring A is a field $\iff$ 0 and A are the only ideals in A.

Proof: $\Rightarrow$) A is a field. Let $I \neq \{0\} \Rightarrow \exists\, a \in I : a \neq 0$

$\Rightarrow$ Since A is a field $\Rightarrow \exists\, a^{-1} \in A \Rightarrow a \cdot a^{-1} = 1 \in I$

$\Rightarrow I = A$

$\Leftarrow$) 0 and A are the only ideals in A, let $a \in A$, $a \neq 0$

Consider $(a) = I = \{x \cdot a\}_{x \in A}$

Since $a \neq 0 \Rightarrow I = (a) = A \Rightarrow \exists\, y \in A : y \cdot a = 1 \Rightarrow y = a^{-1}$

$\neq \{0\}$

A is a field