Algebra MATH-310

Lecture 8

Anna Lachowska

November ~~10~~ 11, 2024

Plan of the course

1. Integers: 1 lecture
2. Groups: 6 lectures

done

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.

(f) Principal ideals. $\longrightarrow$ next time :)

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

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

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

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

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

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

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

$$\text{Consider } \frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \underbrace{\frac{a}{a^2-2b^2}}_{\notin\mathbb{Z}} - \underbrace{\frac{b}{a^2-2b^2}}_{\notin\mathbb{Z} \text{ in general}}\sqrt{2} \notin A$$

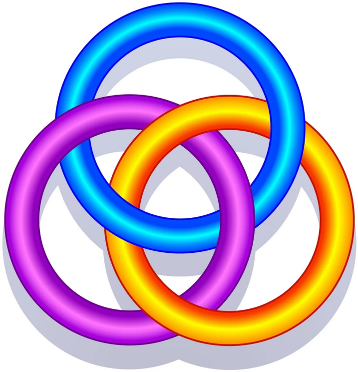
$\Rightarrow$ no multiplicative inverse in general

But A is a ring.

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 geometry, and they are pretty).

- 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

$k, n \in \mathbb{Z}$

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

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

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

Example: Rings without nontrivial zero divisors:

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

$\mathbb{R}$

$\mathbb{C}$

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

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

$\mathbb{Z}/n\mathbb{Z} \simeq C_n$ · is associative, $[1] \in \mathbb{Z}/n\mathbb{Z}$ neutral elt

$0 \leq a \leq n-1$

$\gcd(a, n) = d > 1$	$\gcd(a, n) = 1$
$[a] \cdot \left[\frac{n}{d}\right] = [0]$ in $\mathbb{Z}/n\mathbb{Z}$ $\Rightarrow [a]$ is a zero divisor	By Bézout'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 $[b]\cdot[a] = [0] \Rightarrow \underbrace{\underbrace{[b]\cdot[a]}_{[0]}\cdot[x]}_{=[0]} = [b]$, $\quad [b]\cdot\underbrace{[a]\cdot[x]}_{[1]} = [b]$ $\Rightarrow$ 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 $\Rightarrow$ no $a \in \mathbb{Z}$: $1 \le a \le n-1$ and $\gcd(a,n) > 1$
$\Rightarrow$ n has no divisors except 1 and n $\Rightarrow$ $n = p$ is a prime.
$\forall [b] \in \mathbb{Z}/p\mathbb{Z}$, $\gcd(b,p) = 1 \Leftrightarrow [b]$ 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 elts 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

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

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

$\Rightarrow$ $\mathbb{Z}/6\mathbb{Z}$ 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 $\exists\, a^{-1} \in A : a \cdot a^{-1} = 1$.

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

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

$\Rightarrow b = 0$ if a is invertible

$\Rightarrow$ 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.

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 $\Longleftrightarrow$ $\mathbb{Z}/n\mathbb{Z}$ is a field $\Longleftrightarrow$ $n = p$ 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. Let $A = \mathbb{Z} \Rightarrow 2\mathbb{Z} = \{2k, k \in \mathbb{Z}\} < \mathbb{Z}$ 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 in $\mathbb{Z}$, similarly.

Example 2. $\{0\} \subset A$ is an ideal : $x \cdot 0 = 0$ $\forall x \in A$

$A < A$ is an ideal $x \cdot y \in A$ $\forall x, y \in A$.

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* $1 \in I \implies$ $I = A$: $1 \cdot x = x \in I \ \forall x \in A \Rightarrow A = I$
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, $x, y \in I \cap J \Rightarrow x+y \in I$ and $x+y \in J \Rightarrow$
$x+y \in I \cap J$; $0 \in I$, $0 \in J \Rightarrow 0 \in I \cap J$, $-x \in I$, $-x \in J \Rightarrow -x \in I \cap J$
$\Rightarrow I \cap J$ is an additive subgroup.

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

(3) I, J ideals $\Rightarrow$ let $\overset{\in I}{x_1} + \overset{\in J}{x_2} \in I+J$, $\overset{\in I}{y_1} + \overset{\in J}{y_2} \Rightarrow x_1+x_2+y_1+y_2 = \overbrace{x_1+y_1}^{\in I} + \overbrace{x_2+y_2}^{\in J} \in I+J$
$\Rightarrow I+J$ is an additive subgroup

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

(4) I, J are ideals $\Rightarrow \left\{\sum_i x_i y_i\right\}_{x_i \in I, y_i \in J}$ is closed wrt $+$, $\sum(-x_i)y_i \in I \cdot J$
$\Rightarrow$ additive subgroup.

If $a \in A \Rightarrow a \cdot \sum x_i y_i = \sum \overbrace{a x_i}^{\in I} \overset{\in J}{y_i} \in I \cdot J \Rightarrow I \cdot J$ is an ideal.

(5) Example: $I = 2\mathbb{Z}$, $J = 3\mathbb{Z} \Rightarrow I \cup J = \{0, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 9 \dots\}$
$\Rightarrow 2+3=5$, but $5 \notin I \cup J$. $\Rightarrow$ not an additive subgroup. $\blacksquare$

Ideals in a ring

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

(1) $I \cap J = \{z \in \mathbb{Z} : z = 6n \text{ and } z = 10m\}_{n,m \in \mathbb{Z}} =$
$\{\text{all multiples of } 6 \text{ and } 10\} = \{\text{multiples of } \mathrm{lcm}(6,10) = 30\}$
$= 30 \cdot \mathbb{Z}$

(2) $I + J = \{6n + 10m\}_{n,m \in \mathbb{Z}} \underset{\text{Bézout's thm}}{=} \{\gcd(6,10) \cdot \mathbb{Z}\} = 2\mathbb{Z}$.
$6x + 10y = k \Leftrightarrow \gcd(6,10) \text{ divides } k$.

(3) $I \cdot J = \{\sum_i 6x_i \cdot 10y_i, \ x_i, y_i \in \mathbb{Z}\} = \{60 \sum_i x_i y_i, \ x_i y_i \in \mathbb{Z}\} = 60\mathbb{Z}$.

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

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

$$I \cdot J \subset I \cap J \begin{array}{l} \subset I \supset \\ \supset J \subset \end{array} I + J$$

$$\Big(\sum \underset{\in I}{x_i} \cdot \underset{\in J}{y_i}\Big) \begin{array}{l} \in I \\ \in J \end{array} \qquad\qquad x \in I \Rightarrow \underset{\in I}{x} + \underset{\in J}{0} \in I + J$$

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

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

3. $I + J = \left\{ (x+5) f(x) + (x^2+2) \cdot g(x) \right\}_{f(x), g(x) \in \mathbb{R}[x]}$

$$(x+5)\underbrace{(x-5)\left(-\frac{1}{27}\right)}_{f(x)} - (x^2+2) \cdot \underbrace{\left(-\frac{1}{27}\right)}_{g(x)} = (x^2-25-x^2-2) \cdot \left(-\frac{1}{27}\right) = 1 \in \mathbb{R}[x]$$

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

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

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

Then

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

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

C: $I^2 \cap J^2 = I^2 \cdot J$

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

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

$I+J = \{(x-1)\cdot f(x)\} \neq \mathbb{R}[x]$

$I \cap J = \{(x-1)^2(x+1)f(x)\} \neq I \cdot J = \{(x-1)^3\cdot(x+1)f(x)\}$

$I^2 = \{(x-1)^2(x+1)^2 f(x)\}, \quad J^2 = \{(x-1)^4 f(x)\}$

$I^2 \cap J^2 = \{(x-1)^4(x+1)^2 f(x)\}$

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

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

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

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