Algebra MATH-310

Lecture 9

Anna Lachowska

November 18, 2024

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 2

(a) Principal ideals.
(b) Quotient rings.
(c) Principal ideal domain.
(d) Ring homomorphisms.
(e) Characteristic of a ring.

Recall: commutative rings

Definition

A commutative ring is a set A with two binary operations: $+$ and $\cdot$ such that

• A is an abelian group with respect to addition with the neutral element 0,

• The multiplication is associative, commutative, admits a neutral element $1 \neq 0$ and satisfies the distributivity laws.

Definition

The subset $I \subset A$ is an ideal in A if

1. $I \subset A$ is a subgroup with respect to addition.
2. $\forall x \in I$, $a \in A$ we have $xa \in I$.

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.

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

Examples $\{0\} = (0) \subset A$ and $A = (1) \subset A$ 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 $a \in I$, $I \neq \{0\}$, $a \neq 0$. Since A is a field

$\Rightarrow a^{-1} \in A$: $a^{-1} \cdot \underset{\in I}{a} = 1 \in I \Rightarrow I = A$

$\Leftarrow$) 0 and A the only ideals; let $a \neq 0$, $a \in A$. Consider $(a) = I = \{x \cdot a\}_{x \in A}$

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

$a \neq 0 \Rightarrow I \neq \{0\} \Rightarrow I = A$

$\Rightarrow A$ is a field. ▨

Equivalence and congruence

Definition

An equivalence relation in a set E is a relation satisfying

- reflexivity: $a \sim a$,
- symmetry: $a \sim b \implies b \sim a$,
- transitivity: $a \sim b, b \sim c \implies a \sim c$.

Definition

A congruence relation in a commutative ring A is an equivalence relation on the underlying set satisfying in addition

- $a \sim b, c \sim d \implies a + c \sim b + d$,
- $a \sim b, c \sim d \implies a \cdot c \sim b \cdot d$,

Ideals and congruence relations

Proposition

1. *If $I \subset A$ is an ideal, then $a \sim b \iff (b-a) \in I$ is a congruence relation.*
2. *If $\sim$ is a congruence relation in A, then $I = \{a \in A \;:\; a \sim 0\}$ is an ideal in A.*

Proof: (1) Check that $a \sim b \Leftrightarrow (b-a) \in I$ is an equivalence

it is also a congruence: $\overset{a\sim b}{b-a} \in I$, $\overset{c\sim d}{d-c} \in I \Rightarrow b-a+d-c =$
$= (b+d)-(a+c) \in I \Rightarrow b+d \sim a+c$

$ac \sim bd$: $a(c-d)+d(a-b) = ac-bd \in I \Rightarrow ac \sim bd$.

(2) $a \sim 0$, $b \sim 0 \Rightarrow a+b \sim 0$, $0 \sim 0$, $-a \sim 0 \Rightarrow I : \{a \in A : a \sim 0\}$ is an additive subgp.

$a \sim 0$, $x \in A \Rightarrow x \sim x \Rightarrow ax \sim 0 \cdot x = 0 \Rightarrow ax \in I$
$\Rightarrow \{a \in A : a \sim 0\} = I$ is an ideal ▨

Example: Congruence mod n in $\mathbb{Z}$: $a \sim b \Leftrightarrow b-a = kn$ for $k \in \mathbb{Z}$ Then:
$I = \{a \in \mathbb{Z} : a \sim 0\} = n\mathbb{Z} = (n)$

Quotient ring

Proposition

Let A be a commutative ring, and $\sim$ a congruence relation in A such that $1 \not\sim 0$. Then the set of congruence classes

$$A/\sim \ = \ A/\{x \in A \ : \ x \sim 0\}$$

is a commutative ring.

Proof: $\bar{a} = \{x \in A : x \sim a\}$. Define $\bar{a} + \bar{b} = \overline{a+b}$, $\bar{a} \cdot \bar{b} = \overline{ab}$ well defined because $a_1 \sim a_2$, $b_1 \sim b_2 \Rightarrow a_1 + b_1 \sim a_2 + b_2$; $a_1 b_1 \sim a_2 b_2$.

$\bar{1} \in A/\sim$

Example: $\mathbb{Z}/\sim$ where $a \sim b \Leftrightarrow (b-a) = kn$ (n fixed) for $k \in \mathbb{Z}$ $\Rightarrow \mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots [n-1]\}$ cong. classes mod n

Ideals in a polynomial ring

Example: Let $A = \mathbb{R}[x]$ and $I = \langle (x^2 - 4) \rangle$ a principal ideal.

Consider $B = \mathbb{R}[x]/I$.

$$\overline{(x+2)} \cdot \overline{(x+1)} = \overline{x^2+3x+2} \underset{-(x^2-4)}{=} \overline{3x+6} = \overline{3(x+2)} \text{ in } B$$

$$\bar{x} \cdot \bar{x} = \overline{x^2} = \bar{4} \quad \text{in } B$$

zero divisors in B ?

$$\underbrace{\overline{(x-2)}}_{\neq 0} \cdot \underbrace{\overline{(x+2)}}_{\neq 0} = \overline{x^2-4} = \bar{0} \text{ in } B$$

$\Rightarrow B$ is not integral domain.

Exercise: Any element in B can be written uniquely in the form $\overline{ax+b}$, $a, b \in \mathbb{R}$

Principal ideal domain

Definition

A commutative ring where every ideal is principal is called a principal ring. An integral domain where every ideal is principal is called a principal ideal domain (PID).

Conclusion: A principal ideal domain is

- A commutative ring
- that has no nontrivial zero divisors
- and where every ideal is generated by a single element.

PID: examples

Example 1. Any field is a PID. only 2 ideals: $A = (1)$ and $\{0\} = (0)$.

Example 2. $\mathbb{Z}$ is a PID.

Proof: If $I = \{0\} \Rightarrow I = (0)$. Suppose $I \neq \{0\} \Rightarrow \exists a \in I, a \neq 0$.
$\Rightarrow -a \in I \Rightarrow |a| \in I$. Let $d \in I$ be the smallest positive elt in I.
By Euclidean division, let $\forall n \in I \Rightarrow n = kd + r$, where $0 \leq r \leq d-1$

$\underbrace{n}_{\in I} = \underbrace{kd}_{\in I} + r \Rightarrow r \in I$, but d is the smallest positive in $I \Rightarrow r = 0$

$\Rightarrow n = kd \quad \forall n \in I \Rightarrow I = (d)$. $\blacksquare$

Ex. Let $J = (a_1, a_2 \ldots a_n) \subset \mathbb{Z}$, $a_1 \ldots a_n \in \mathbb{Z}$.
Then $J = (k)$ is principal, $k = \gcd(a_1 \ldots a_n)$
By induction on n: use Bezout's thm: $\exists x, y \in \mathbb{Z}: xa_1 + ya_2 = c \Leftrightarrow \gcd(a_1, a_2) \mid c$.

Ring homomorphisms

Definition

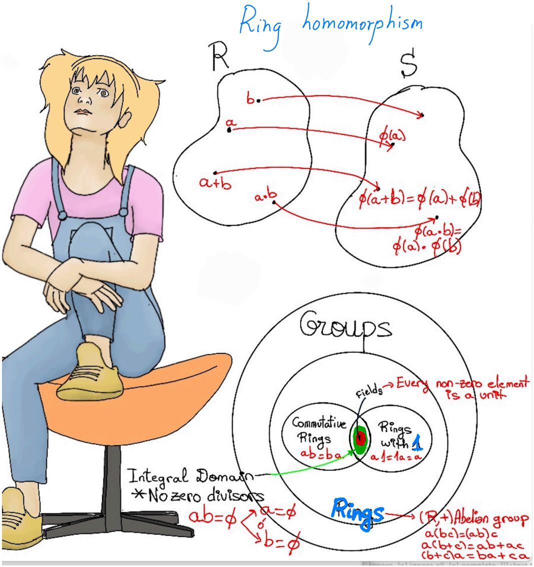
A map $f : A \to B$ is a ring homomorphism if

- $f(a+b) = f(a) + f(b)$, $\quad (\Rightarrow f(0_A) = 0_B)$
- $f(a \cdot b) = f(a) \cdot f(b)$,
- $f(1_A) = 1_B$.

Definition Very restrictive

A subring $C \subset B$ is a subset that is a ring with the same operations $(+, \cdot)$ and neutral elements $(0, 1)$ as in B.

Example: If $C \subset \mathbb{Z}$ is a subring, then $0 \in C$ and $1 \in C$ $\Longrightarrow \underbrace{1 + 1 + 1 + \ldots + 1}_{n} \in C$ for any number $n \in \mathbb{N}$. Similarly, $-1 \in C \implies -n \in C$. Therefore, $C = \mathbb{Z}$.



Rings and their homomorhpisms

Ring homomorphisms

Proposition

If $f : A \to B$ is a ring homomorphism, then

1. $\ker(f) \subset A$ *is an ideal,*
2. $\mathrm{im}(f) \subset B$ *is a subring.*

Exercise

① $x \in \ker f,\ y \in \ker f \Rightarrow f(x+y) = f(x) + f(y) = 0 \Rightarrow x+y \in \ker f$

$\underset{a \in A}{f(a \cdot x)} = f(a) \cdot \underbrace{f(x)}_{=0} = 0 \Rightarrow a \cdot x \in \ker f \Rightarrow \ker f \subset B$

is an ideal.

Example of a ring homomorphism

Example: Let $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$.

(1) $\mathrm{Im} f$ is a subring in $\mathbb{Z}/m\mathbb{Z}$ $\quad \mathrm{Im} f \ni [1]_m \Rightarrow \underbrace{[1]_m + [1]_m + \ldots + [1]_m}_{k} = [k]_m \in \mathrm{Im} f$

$\Rightarrow \mathrm{Im} f = \mathbb{Z}/m\mathbb{Z}$.

(2) $f([n]_n) = f([0]_n) = [0]_m$

$\quad \| $

$f([1]_n + [1]_n \cdots + [1]_n) = n \cdot [1]_m = [n]_m \in \mathbb{Z}/m\mathbb{Z}$

$\Rightarrow \boxed{m \text{ divides } n}$

$f : [1]_n \to [1]_m \Rightarrow f : [k]_n \to [k]_m \Rightarrow f$ is unique

Conclusion: A ring homomorphism

$$f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \quad \text{exists} \quad \Longleftrightarrow m \,|\, n.$$

Then f is unique.

Example of a ring homomorphism

Example 1: $f : \mathbb{Z}/10\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$

5 divides 10

$$\begin{array}{cccccccccc} [0] & [1] & [2] & [3] & [4] & [5] & [6] & [7] & [8] & [9] \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ [0] & [1] & [2] & [3] & [4] & [0] & [1] & [2] & [3] & [4] \end{array} \quad f$$

$\ker f = \{[0],[5]\} = ([5])$ $\quad \operatorname{im} f = \mathbb{Z}/5\mathbb{Z}$

Example 2: $f : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/12\mathbb{Z}$

no ring homomorphism: 12 does not divide 6.

Example 3: $f : \mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ $\quad$ yes; $f(0) = [0]$ $\quad f(k) = [k]_6 \quad \forall k \in \mathbb{Z}$

$\ker f = \{0, \pm 6, \pm 12, \dots\} = (6) \subset \mathbb{Z}$ $\quad$, $\operatorname{im} f = \mathbb{Z}/6\mathbb{Z}$

Characteristic of a ring

Fact:

For any ring A there exists a unique ring homomorphism $\tau : \mathbb{Z} \to A$.

Proof: Since $\tau(0) = 0$, $\tau(1) = 1 \in A \Rightarrow \tau(n \cdot 1) = \tau(1 + \dots + 1) =$

$$= \underbrace{1_A + 1_A + \dots + 1_A}_{n} = n \cdot 1_A \in A$$

$\Rightarrow \tau(n) = n \cdot 1_A \in A$ is uniquely determined, $\tau(n \cdot k) = \tau(n) \cdot \tau(k)$

$\blacksquare$

Two possibilities for $\ker(\tau)$: $\left[\begin{array}{l} \ker\tau = (0) \\ \ker\tau = (d) \quad d \geq 2 \end{array}\right.$ $\left(\ker\tau \neq (1) \text{ because } \tau(1) = 1_A \neq 0_A.\right)$

Characteristic of a ring

Definition

Let A be a ring and $\tau : \mathbb{Z} \to A$ the unique ring homomorphism. Then the characteristic of A is

- $c_A = 0$ if $\ker(\tau) = (0) \subset \mathbb{Z}$,
- $c_A = d$ if $\ker(\tau) = (d) \subset \mathbb{Z}$, where $d \geq 2$.

Examples.

$c(\mathbb{R}) = 0$ $\quad \tau : \mathbb{Z} \to \mathbb{R}$, $n \to n$ $\quad \Rightarrow \ker \tau = \{0\} = (0)$

$c(\mathbb{Z}) = 0$ $\quad \tau : \mathbb{Z} \to \mathbb{Z}$, $n \to n$ $\quad \forall n \in \mathbb{Z}$ identity map $\Rightarrow \ker \tau = (0)$

$c(\mathbb{Z}/_{n\mathbb{Z}}) = n$ $\quad \tau : \mathbb{Z} \to \mathbb{Z}/_{n\mathbb{Z}}$, $k \to [k]_n$ $\quad \ker \tau = (n) \subset \mathbb{Z}$

Properties of the characteristic

Proposition

If A is an integral domain, then $c_A = 0$ or $c_A = p$, where p is a prime.

Proof:

By contradiction: $c_A = m \cdot k \quad m > 1,\ k > 1,\ \underbrace{\tau(m)}_{\neq 0} \cdot \underbrace{\tau(k)}_{\neq 0} = \tau(mk) = 0$ in A

$\Rightarrow \tau(m)$ and $\tau(k)$ are nontrivial zero divisors. $\Rightarrow A$ is not an integral domain.

$\boxtimes$

Corollary (A field is an integral domain)

Characteristic of a field is either zero, or a prime.

$\Rightarrow \mathbb{Z}/_{n}\mathbb{Z}$ is a field $\Rightarrow n = p$ a prime.

Direct product of rings

Definition

If A and B are rings, then the direct product $A \times B = \{(a, b),\ a \in A,\ b \in B\}$ is a ring with the ring structure given by the component-wise operations:

$$(a_1,\ b_1) \pm (a_2,\ b_2) = (a_1 \pm a_2,\ b_1 \pm b_2)$$

$$(a_1,\ b_1) \cdot (a_2,\ b_2) = (a_1 \cdot a_2,\ b_1 \cdot b_2).$$

The neutral elements are $(0_A, 0_B)$ and $(1_A, 1_B)$.

Example. $A = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Compute c_A.

$\tau : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \quad \tau(1) = ([1]_n, [1]_m),\ \tau(k) = ([k]_n, [k]_m) \overset{?}{=} ([0]_n, [0]_m)$

$\Rightarrow k \equiv 0 \pmod{n}$ and $k \equiv 0 \pmod{m}$, $k > 0$ is the smallest

$\Rightarrow k = \operatorname{lcm}(m, n)$.

$$c(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}) = \operatorname{lcm}(n, m)$$

Characteristic of a direct product

Proposition

If $c_A \neq 0$, $c_B \neq 0$, *then* $c_{A\times B} = \mathrm{lcm}(c_A, c_B)$. *If* $c_A = 0$ *or* $c_B = 0$, *then* $c_{A\times B} = 0$.

Same proof as above.

Poll:

Let n be an even natural number. For a ring A, let $A[x]$ be the ring of polynomials with coefficients in A. Then the characteristic of the following ring is equal to n:

A: $\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ $\quad c_A = 0 \quad \tau : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \quad \tau(k) = (k, [k]_n) = (0, [0]_n) \Rightarrow k = 0.$

B: $(\mathbb{Z}/n\mathbb{Z})[x] \times \mathbb{Z}/(\frac{n}{2})\mathbb{Z}$

$\tau \; \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}[x] \quad \tau(k) = [k]_n = 0 \Rightarrow k = n \quad \tau(1) = [1]_n$

C: $(\mathbb{Z}/n\mathbb{Z})[x] \times \mathbb{Z} \times \mathbb{Z}/n^2\mathbb{Z}$ $\quad c_C = 0$

D: $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n^2\mathbb{Z} \times \mathbb{Z}/n^3\mathbb{Z}$ $\quad c_D = \mathrm{lcm}(n, n^2, n^3) = n^3.$

$\Rightarrow c(\mathbb{Z}/n\mathbb{Z}[x]) = n$

E: $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/(2n)\mathbb{Z}$ $\quad c_E = \mathrm{lcm}(n, 2n) = 2n$

$c(\mathbb{Z}/n\mathbb{Z}[x]) = n \Rightarrow c_B = \mathrm{lcm}(n, \frac{n}{2}) = n.$

Computation of the characteristic

Remark

Let $A[x]$ denote the polynomials with coefficients in a commutative ring A. Then the characteristic of $A[x]$ is equal to the characteristic of A.

Let $\tau: \mathbb{Z} \to A[x]$ $\quad \tau(1) = 1 \in A[x]$,

$= 1 \in A$

$\Rightarrow \tau(k) = k \in A \Rightarrow k = 0$ in $A[x]$

$\Leftrightarrow k = 0$ in A

$\Rightarrow c_{(A[x])} = c_A$.