Algebra MATH-310

Lecture 9

Anna Lachowska

November 17, 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 2

a) Equivalence and congruence relations.
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 $xa \in I$.

Definition

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

$= \{ax\}_{a \in A}$

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 $a \sim b \overset{def}{\iff} (b-a) \in I$ 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 $a \sim b \iff b-a \in I$ is an equivalence: $a-a \in I$

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

$\overset{\in I}{\Rightarrow} (b+d)-(a+c) \overset{\in I}{\in} I \Rightarrow b+d \sim a+c$

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

(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 subgroup

$a \sim 0$, $x \in A$: $x \sim x \Rightarrow a \cdot x \sim 0 \cdot x = 0 \Rightarrow ax \in I$

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

Example: Congruence mod n in $\mathbb{Z}$: $a \sim b \iff b-a = kn$ 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 $\bar{a} + \bar{b} = \overline{a+b}$, $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$ 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 $a \sim b \Leftrightarrow (b-a) \in n\mathbb{Z} \Rightarrow \mathbb{Z}/n\mathbb{Z} = \{[0], [1] \ldots [n-1]\}$ (n fixed; 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 $B = \mathbb{R}[x]/I$.

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

$$-(x^2-4)$$

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

zero divisors in B ? $\overline{(x-2)} \cdot \overline{(x+2)} = \overline{x^2-4} = \bar{0}$ in B

$\neq 0$ $\neq 0$

$\Rightarrow B$ is not an 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 PID

- 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 $n \in I \Rightarrow n = kd + r$ where $0 \leq r \leq d-1$

$n = kd + r \Rightarrow r \in I$ but d is the smallest positive in $I \Rightarrow r = 0$
($n \in I$, $kd \in I$)

$\Rightarrow n = kd \ \forall n \in I \Rightarrow I = (d)$ ▨

Ex. Let $J = (a_1, \dots a_n) \subset \mathbb{Z}$ $a_1, \dots a_n \in \mathbb{Z}$ $\left\{\sum_{i=1}^{n} x_i a_i\right\} = J$
Then $J = (k)$ is principal $\Rightarrow \gcd(a_1, \dots a_n)$
By induction on n: $\exists x, y \in \mathbb{Z} : xa_1 + ya_2 = c \Leftrightarrow \gcd(a_1, a_2) \mid c$

Ring homomorphisms

Definition Very restrictive

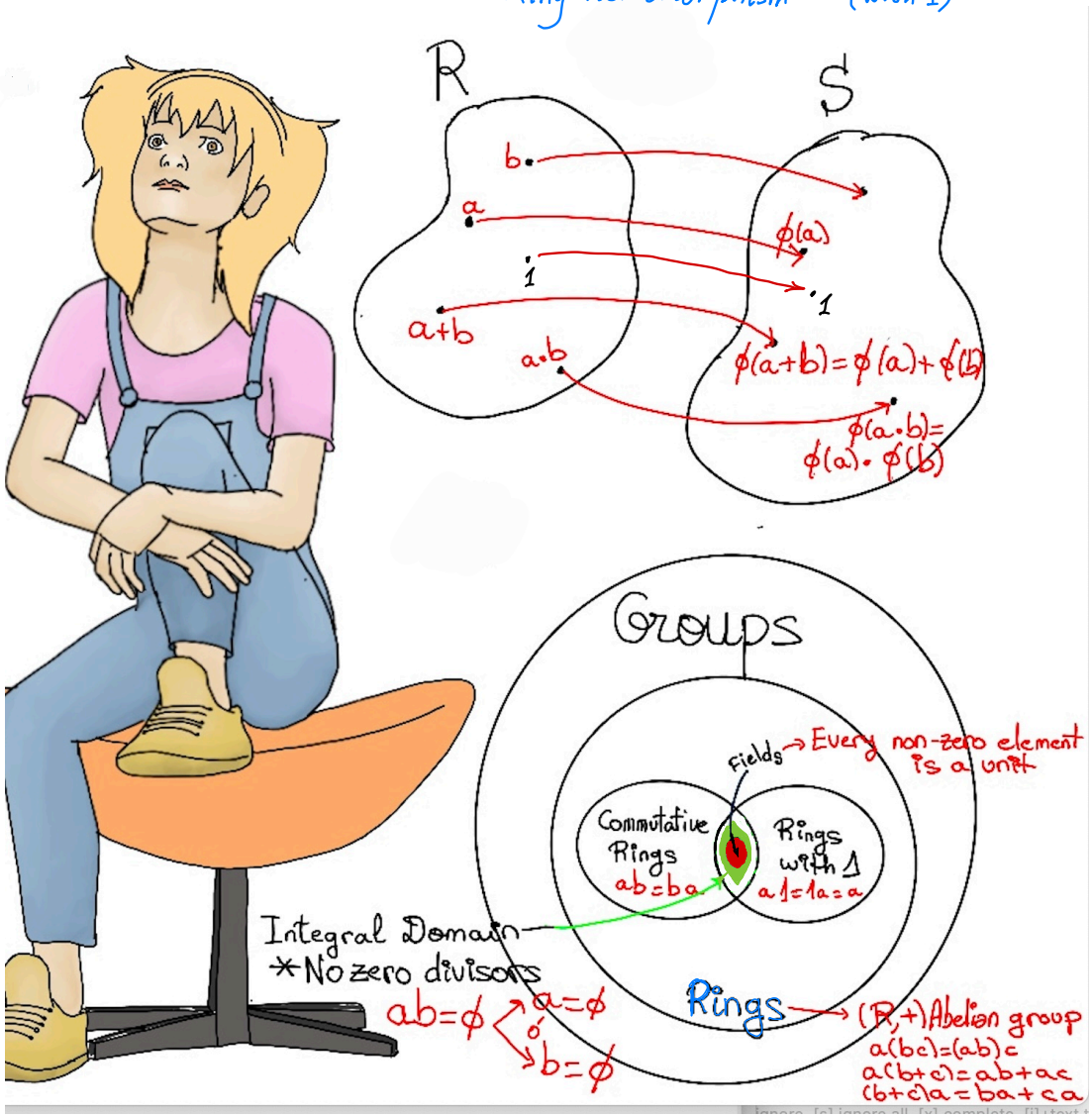
A map $f : A \to B$ is a ring homomorphism if

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

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 $1 \in C$ $\implies 1+1+1+\ldots+1 \in C$ 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.*

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

$f(x) = 0$, $f(y) = 0$

$f(a \cdot x) = f(a) \cdot f(x) = f(a) \cdot 0 = 0 \Rightarrow a \cdot x \in \ker f$

$a \in A$, $x \in \ker f$; $f(x) = 0$; $\forall a \in A$, $x \in \ker f$

$\Rightarrow \ker f = I$.

Example of a ring homomorphism

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

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

$= [k]_m \Rightarrow \operatorname{Im} f = \mathbb{Z}/m\mathbb{Z}.$

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

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

$\Rightarrow$ **m divides n**

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

Conclusion: A ring homomorphism

$$f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \quad \text{exists} \iff m \mid n.$$

Then f is unique.

Example of a ring homomorphism

Example 1: $f : \mathbb{Z}/10\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$ $[0]\ [1]\ [2]\ [3]\ [4]\ [5]\ [6]\ [7]\ [8]\ [9]$

5 divides 10

f: $[0]\ [1]\ [2]\ [3]\ [4]\ [0]\ [1]\ [2]\ [3]\ [4]$

$\ker f = \{[0],[5]\} = ([5])$ ideal in $\mathbb{Z}/10\mathbb{Z}$ $\quad f([2]+[6]) = [2]+[1] = [3] = f([8])$

$\operatorname{im} f = \mathbb{Z}/5\mathbb{Z}$

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

no ring homomorphism: 12 does not divide 6

Example 3: $f : \mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ yes: $f(0) = [0]$ $f(1) = [1] \Rightarrow f(k) = [k]_6$ $\forall k \in \mathbb{Z}$

$\ker f = 6\mathbb{Z} = (6)$ $\quad \operatorname{im} f = \mathbb{Z}/6\mathbb{Z}$.

Characteristic of a ring

Fact:

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

Proof: Since $\tau(0) = 0$, $\tau(1) = 1_A \in A \Rightarrow \tau(n \cdot 1) = \tau(\underbrace{1 + 1 + 1 \ldots + 1}_{n}) = \underbrace{1_A + 1_A + \ldots + 1_A}_{n} = n \cdot 1_A \in A$

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

$\tau(nk) = \tau(n) \cdot \tau(k)$

$\ker \tau = I \subset \mathbb{Z}$ an ideal

Two possibilities for $\ker(\tau)$:

- $\ker \tau = (0)$
- $\ker \tau = (d)$, $d \geq 2$

($\ker \tau \neq (1)$ because $\tau(1) = 1_A \neq 0_A$.)

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.

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

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

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

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: Suppose $c_A = m \cdot k$, $m > 1$, $k > 1$

$\tau(m) \cdot \tau(k) = \tau(mk) = 0$ in A

$\tau(c_A) = 0$ in A

$\tau(m) \neq 0$, $\tau(k) \neq 0$

$\Rightarrow$ $\tau(m)$ and $\tau(k)$ are nontrivial zero divisors

$\Rightarrow$ A is not an integral domain.

Corollary (A field is an integral domain)

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

(in particular $\mathbb{Z}/n\mathbb{Z}$ is a field $\Leftrightarrow$ $n = p$ is 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* $c_{A\times B} = \operatorname{lcm}(c_A, c_B)$. *If* $c_A = 0$ *or* $c_B = 0$, *then* $c_{A\times B} = 0$.

Same proof as above (for $c_A \neq 0$, $c_B \neq 0$).

If $c_A = 0 \Rightarrow \tau(1) = (1_A, 1_B) \Rightarrow \tau(k) = (k\cdot 1_A, k\cdot 1_B) \overset{?}{=} (0_A, 0_B) \Rightarrow$

$\ker\tau = \{0\} \Rightarrow c_{A\times B} = 0$.

$c_A = 0 \Rightarrow \tau_A : \mathbb{Z} \to A$ is such that $\ker\tau_A = \{0\}$

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 $\tau : \mathbb{Z} \to A[x]$

$\tau(1) = 1 \in A[x]$

$= 1 \in A$

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

$\Leftrightarrow k = 0$ in A

$\Rightarrow C_{(A[x])} = C_A$.

Poll:

Let $n \geq 2$ be a 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^2:

A: $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

B: $\mathbb{Z}/n^2\mathbb{Z} \times \mathbb{Z}[x] \times \mathbb{Z}/n^2\mathbb{Z}$

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

D: $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n^2\mathbb{Z} \times \mathbb{Z}/n^3\mathbb{Z}$

E: $\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n^2\mathbb{Z}$

$\tau(k) = ([k]_n, [k]_n) = (0,0) \Rightarrow c = \operatorname{lcm}(n,n) = n$

$\tau(k) = ([k]_{n^2}, k, [k]_{n^2}) = (0,0,0) \Rightarrow c = 0$

$\tau(k) = ([k]_n, [k]_{n^2}) \Rightarrow c = \operatorname{lcm}(n, n^2) = n^2$ ✓

$\tau(k) = ([k]_n, [k]_{n^2}, [k]_{n^3}) \Rightarrow c = \operatorname{lcm}(n, n^2, n^3) = n^3$

$\tau(k) = (k, [k]_n, [k]_{n^2}) = (0,0,0) \Rightarrow c = 0.$