Algebra MATH-310

Lecture 10

Anna Lachowska

November 24, 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 3

a. Chinese remainder theorem.
b. CRT for integers.
c. Polynomial rings: degree of a polynomial.
d. Euclidean division for polynomials.
e. Euclidean domains.

Recall: ring homomorphism and the direct product of rings

Definition

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

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

A bijective ring homomorphism is a ring isomorphism.

Definition

A direct product of two rings A, B is defined as the set of pairs

$$A \times B = \{(a, b),\ a \in A, b \in B\}$$

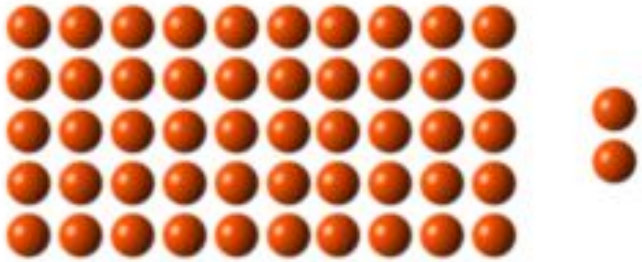
with component-wise operations and the neutral elements $(0_A, 0_B)$, $(1_A, 1_B)$.

Today: the Chinese remainder theorem

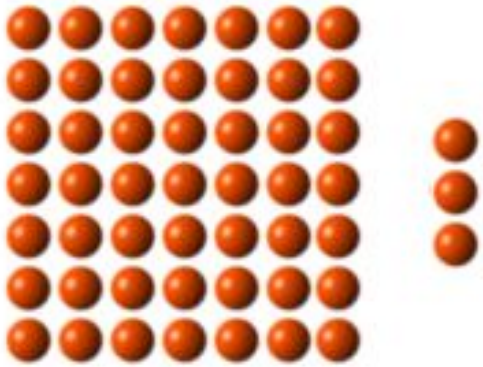
Sunzi Suanjing
4th century CE

If a collection of balls are arranged in rows of 3, there is one ball left over

If arranged in rows of 5, there are two balls left over



If arranged in rows of 7, there are three balls left over



The Chinese Remainder Theorem proves that the smallest number of balls must be 52

How to solve it? See Solution below

Chinese remainder theorem

Theorem

Let A be a commutative ring, $I, J \subset A$ two ideals such that $I + J = A$. Then there is a ring isomorphism

$$f : A/(I \cap J) \simeq A/I \times A/J$$

$$f([x]_{(I\cap J)}) = ([x]_I, [x]_J).$$

Proof: (1) f is a ring homomorphism:

$f: x \in A \to ([x]_I, [x]_J)$ and the ring operations are respected.

$1 \to ([1]_I, [1]_J)$

$0 \to ([0]_I, [0]_J)$

Chinese remainder theorem

(2) Surjectivity. Show that $\forall a_1, a_2 \in A \ \exists a \in A$ s.t. $a \equiv a_1 \pmod{I}$, $a \equiv a_2 \pmod{J}$

Since $I+J=A \Rightarrow \underbrace{a_1 - a_2}_{\in A} = \underbrace{-i}_{\in I} + \underbrace{j}_{\in J} \Leftrightarrow a_1 + i = a_2 + j \overset{\text{def}}{=} a \in A$

$\Rightarrow a \equiv a_1 \pmod{I} \equiv a_2 \pmod{J}$

$\Rightarrow f : X \longrightarrow ([x]_I \ [x]_J)$ is surjective.

(3) Injectivity Suppose $b \in A$: $b \equiv a_1 \pmod{I}$, $b \equiv a_2 \pmod{J}$

$\Rightarrow b = a_1 + \underbrace{i'}_{\in I} = a_2 + \underbrace{j'}_{\in J} \Rightarrow a - b = \underbrace{i - i'}_{\in I} = \underbrace{j - j'}_{\in J}$

$\Rightarrow a - b \in I \cap J$

$\Rightarrow f : A/_{I \cap J} \longrightarrow A/_I \times A/_J$ is injective

$\Rightarrow f : A/_{I \cap J} \longrightarrow A/_I \times A/_J$ is a ring isomorphism

The case $A = \mathbb{Z}$.

Corollary

Let $n, m \in \mathbb{Z}$ be coprime: $\gcd(n, m) = 1$. Then for any numbers $a_1, a_2 \in \mathbb{Z}$ there exist $a \in \mathbb{Z}$ such that

$$\begin{cases} a \equiv a_1 \pmod{n} \\ a \equiv a_2 \pmod{m} \end{cases}$$

The set of solutions of this pair of congruences is $\{a + (nm)\mathbb{Z}\}$.

Proof: $\gcd(n,m) = 1 \Rightarrow \exists x, y \in \mathbb{Z} : xn + ym = 1 \Rightarrow (n) + (m) = \mathbb{Z}$

$\Rightarrow$ By CRT $\mathbb{Z}/(n\mathbb{Z} \cap m\mathbb{Z}) \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ ($n\mathbb{Z} + m\mathbb{Z}$) $\Rightarrow$ for any pair ($a_1 \bmod n$, $a_2 \bmod m$)

there exist $a \in \mathbb{Z} : a \equiv a_1 \pmod{n} \equiv a_2 \pmod{m}$, a is unique

up to the ideal $(n\mathbb{Z}) \cap (m\mathbb{Z}) = (nm)\mathbb{Z}$

Since $\gcd(n,m) = 1 \Leftrightarrow \operatorname{lcm}(n,m) = nm$

$\Rightarrow$ the solutions are $\{a + nm\mathbb{Z}\}$ ▨

Generalization to $n > 2$ for $A = \mathbb{Z}$

Theorem

Let $d_1, d_2, \ldots d_r \in \mathbb{Z}$ be pairwise coprime, i.e. $\gcd(d_i, d_j) = 1$ for any $i \neq j$. Then for any numbers $a_1, a_2, \ldots a_r \in \mathbb{Z}$ there exist $a \in \mathbb{Z}$ such that

$$\begin{cases} a \equiv a_1 \pmod{d_1} \\ a \equiv a_2 \pmod{d_2} \\ \quad \ldots. \\ a \equiv a_r \pmod{d_r} \end{cases}$$

The number $a \in \mathbb{Z}$ is unique up to the ideal $(d_1 d_2 \ldots d_r) \subset \mathbb{Z}$. The set of solutions is given by $\{a + (d_1 d_2 \ldots d_r)\mathbb{Z}\}$.

Proof: by induction on r.

See rings_Math310.pdf on Moodle

$\exists a \quad a \equiv a_1 \pmod{d_1}, \; a \equiv a_2 \pmod{d_2} \Rightarrow \begin{cases} x \equiv a \pmod{d_1 d_2} \\ x \equiv a_3 \pmod{d_3} \end{cases}$

and so on.

Example.

Find $a \in \mathbb{Z}$ such that

$$\begin{cases} a \equiv 1 \pmod 3 \\ a \equiv 2 \pmod 5 \\ a \equiv 3 \pmod 7 \end{cases}$$

1. Explain why there is a solution. By CRT since 3, 5, 7 are pairwise coprime
2. Describe the set of all integer solutions.
3. Find the smallest positive solution.

$a = 3k+1 = 5t+2$ for example $a = 7$

$\begin{cases} a \equiv 7 \pmod{15} \\ a \equiv 3 \pmod 7 \end{cases}$ $\quad a = 15m + 7 = 7n + 3 \quad m = 3,\ n = 7$

$7n - 15m = 4 \quad \Rightarrow a = 45 + 7 = 52$

$\Rightarrow a \in \{52 + 105\mathbb{Z}\}$ all solutions $\quad 105 = 3 \cdot 5 \cdot 7$

the smallest positive solution is 52.

Algorithm for solving systems of congruences

Consider the system

$$\begin{cases} a \equiv a_1 \pmod{d_1} \\ a \equiv a_2 \pmod{d_2} \\ \quad \ldots. \\ a \equiv a_r \pmod{d_r} \end{cases}$$

$\gcd(d_i, d_j) = 1 \quad \forall i \neq j$

Let $D_i = (\prod_{i=1}^{r} d_i)/d_i$. Then $\gcd(D_i, d_i) = 1$ for all $i = 1 \ldots r$ and there exist $x_i, y_i \in \mathbb{Z}$ such that $D_i x_i + d_i y_i = 1$. Then

$$a = \sum_{i=1}^{r} a_i D_i x_i$$

is a solution of the system.

$a = \sum_{i=1}^{r} a_i D_i x_i \pmod{d_i} = a_i \underbrace{D_i x_i}_{1 - d_i y_i} \pmod{d_i} = a_i (1 - d_i y_i) \pmod{d_i} = a_i \pmod{d_i}$

Application: multiplicativity of the totient function $\varphi(n)$

Definition

Let A be a commutative ring. Then its invertible elements with respect to the multiplication form a group that is called the group of units and denoted A^*.

Example: $A = \mathbb{Z}$. $\Rightarrow$ $\mathbb{Z}^* = \{\pm 1\}$

$\mathbb{R}^* = \mathbb{R} \setminus \{0\}$

Remark: If $A \simeq B$ are isomorphic rings, then their groups of units are also isomorphic: $A^* \simeq B^*$.

Application: multiplicativity of the totient function $\varphi(n)$

Theorem

Let $n, m \in \mathbb{Z}$ such that $\gcd(n, m) = 1$. Then $\varphi(nm) = \varphi(n)\varphi(m)$.

Proof: By CRT $\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ $\Rightarrow$

$$\left(\mathbb{Z}/nm\mathbb{Z}\right)^* \simeq \left(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}\right)^* \simeq \left(\mathbb{Z}/n\mathbb{Z}\right)^* \times \left(\mathbb{Z}/m\mathbb{Z}\right)^*$$ direct product of groups of units

$$\left|\left(\mathbb{Z}/nm\mathbb{Z}\right)^*\right| = \varphi(nm), \quad \left|\left(\mathbb{Z}/n\mathbb{Z}\right)^*\right| = \varphi(n), \quad \left|\left(\mathbb{Z}/m\mathbb{Z}\right)^*\right| = \varphi(m)$$

$$\Rightarrow \quad \varphi(nm) = \varphi(n)\varphi(m)$$ ▨

prime factorization : $\{p_i\}$ distinct primes

This can be used to compute $\varphi(p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}) = \varphi(p_1^{a_1}) \cdot \dots \varphi(p_k^{a_k})$. $=$

$$= \left(p_1^{a_1} - p_1^{a_1-1}\right)\left(p_2^{a_2} - p_2^{a_2-1}\right) \cdots \left(p_k^{a_k} - p_k^{a_k-1}\right)$$

Converse to the Chinese remainder theorem

Theorem

$$\mathbb{Z}/(nm)\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \iff \gcd(n,m) = 1.$$

Proof: $\Leftarrow$ $\gcd(n,m)=1$ $\Rightarrow$ by CRT $\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$

$\Rightarrow$ If $\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ $\Rightarrow$ $c\left(\mathbb{Z}/mn\mathbb{Z}\right) = c\left(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}\right)$ (characteristic)

$nm = \operatorname{lcm}(n,m) \iff \gcd(n,m)=1$

Examples:

$\mathbb{Z}/80\mathbb{Z} \simeq \mathbb{Z}/16\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ ($\gcd(16,5)=1$)

$\mathbb{Z}/80\mathbb{Z} \not\simeq \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ ($\gcd(8,10)=2$)

$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \not\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z} \simeq \mathbb{Z}/54\mathbb{Z}$ ($\gcd(6,9)=3$, $\gcd(2,27)=1$)

$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ ($\gcd(2,3)=1$)

Poll:

Let $n, m \in \mathbb{N}$ be two odd natural numbers such that $n, m \geq 3$ and $\gcd(n, m) = 1$. Let $k \in \mathbb{N}^*$. Then

A: $\varphi(2^{2k}nm) = \varphi(2^k n)\varphi(2^k m)$

B: $\varphi(2^{2k}nm) < \varphi(2^k n)\varphi(2^k m)$

C: $\varphi(2^{2k}nm) > \varphi(2^k n)\varphi(2^k m)$

D: The relation between $\varphi(2^{2k}nm)$ and $\varphi(2^k n)\varphi(2^k m)$ depends on the numbers n, m.

$$\varphi(2^{2k}nm) = \varphi(2^{2k})\cdot\varphi(n)\varphi(m) = (2^{2k} - 2^{2k-1})\varphi(n)\varphi(m)$$

$$\varphi(2^k n)\varphi(2^k m) = \varphi(2^k)^2\varphi(n)\varphi(m) = (2^k - 2^{k-1})^2\varphi(n)\varphi(m) =$$

$$(2^{2k} - 2^{2k-1} - 2^{2k-1} - 2^{2k-2})\varphi(n)\varphi(m)$$

$$\Leftrightarrow (2^{2k} - 2^{2k-1}) - (2^{2k-1} - 2^{2k-2}) < (2^{2k} - 2^{2k-1})$$

$\forall k \in \mathbb{N}^*$

Conclusions:

- If A is a commutative ring and $I, J \subset A$ two ideals such that $I + J = A$, then
$$A/I \times A/J \simeq A/(I \cap J).$$
- $\mathbb{Z}/(nm)\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \iff \gcd(n, m) = 1.$
- $\varphi(nm) = \varphi(n)\varphi(m) \iff \gcd(n, m) = 1.$

Next goal: CRT for polynomial rings

Definition

Let A be a commutative ring. Then

$$A[x] = \{a_0 + a_1 x + \ldots + a_n x^n\}_{n \in \mathbb{N}}, \quad a_0, a_1, \ldots \in A$$

is the ring of polynomials with coefficients in A with respect to the usual addition and multiplication of polynomials. We have $0 \in A[x]$ and $1 \in A[x]$ same as in A.

Definition

If $f(x) \in A[x]$ is nonzero, define the degree of

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n$$

as the largest $n \in \mathbb{N}$ such that $a_n \neq 0$. Notation: $\deg(f) = n$.
If $f(x) = 0$, we set $\deg(f) = -\infty$. If $f(x) = a_0 \neq 0$, then $\deg(f) = 0$.

Polynomials with coefficients in an integral domain

Proposition

Let A be an integral domain. Then we have

1. $\deg(f+g) \leq \max(\deg(f), \deg(g))$.
2. $\deg(f \cdot g) = \deg(f) + \deg(g)$.

Proof:

(1) $\deg(f+g) = \max(\deg f, \deg g)$ unless $\deg f = \deg g$ and $a_n = -b_n$

Ex: $(3x^3 + 2x^2 + x - 1) + (-3x^3 + 5x + 6) = 2x^2 + 6x + 5$

$\deg = 3$ $\deg = 3$ $\deg = 2$

(2) $f(x) \cdot g(x) = (a_0 + a_1 x + \dots + a_n x^n)(b_0 + \dots + b_m x^m) = a_n b_m x^{n+m} + \text{lower terms}$

$a_n \neq 0$, $b_m \neq 0$, $a_n b_m \neq 0$ since A is an integral domain

$\Rightarrow \deg(f \cdot g) = \deg f + \deg g$

If $f(x) = 0 \Rightarrow f(x) \cdot g(x) = 0$

$\deg f \cdot g = -\infty = -\infty + m = -\infty$.

$\deg f$ $\deg g$

Polynomials with coefficients in an integral domain

Proposition

Let A be an integral domain. Then

1. *$A[x]$ is an integral domain.*
2. *The units (invertible elements) of $A[x]$ are the units of A.*

Proof:

(1) $f(x)\cdot g(x) = 0 \iff \deg(f\cdot g) = -\infty \Rightarrow \deg f + \deg g = -\infty$

$\iff \begin{cases} \deg f = -\infty \\ \deg g = -\infty \end{cases} \iff \begin{cases} f(x) = 0 \\ g(x) = 0 \end{cases}$

(2) $f(x)\cdot g(x) = 1 \iff \deg(f\cdot g) = 0 = \deg f + \deg g \Rightarrow \deg f = \deg g = 0$

$\Rightarrow f(x) = a_0,\ g(x) = b_0,\ a_0 b_0 = 1 \in A$

$\Rightarrow a_0, b_0$ are units in A. ▨

Examples: $\mathbb{R}[x]$, $\mathbb{Q}[x]$, $\mathbb{Z}[x]$ integral domains, $\mathbb{Z}/6\mathbb{Z}[x]$ is not: $(3x)(2x) = 0$

Euclidean division for polynomials in $\mathbb{F}[x]$

Theorem

Let $\mathbb{F}$ be a field. Let $f(x), d(x) \in \mathbb{F}[x]$ such that $\deg(d) \geq 1$. Then there exist polynomials $q(x), r(x) \in \mathbb{F}[x]$ such that

$$f(x) = q(x)d(x) + r(x),$$

and either $r(x) = 0$, or $\deg(r) < \deg(d)$.

Proof: If $\deg f < \deg d \Rightarrow f(x) = 0 \cdot d(x) + r(x) \Rightarrow f(x) = r(x)$.

If $\deg f > \deg g \Rightarrow f(x) = a_0 + \dots + a_m x^m$, $d(x) = d_0 + \dots + d_n x^n$, $n \leq m$

$\Rightarrow f(x) - d(x) \cdot \frac{a_m}{d_n} x^{m-n} = p_1(x)$, $\deg(p_1) < \deg f$ ($\mathbb{F}$ a field)

If $\deg p_1 > \deg d$, repeat $\Rightarrow f(x) - d(x) \cdot \underbrace{\frac{a_m}{d_n} x^{m-n}}_{q_1(x)} + d(x) \underbrace{\frac{a_{m-1}}{d_n} x^{m-n-1}}_{q_2(x)} + \dots$

until get $\deg(f - d(x)q_1(x)) < \deg d \Rightarrow f(x) = d(x)q(x) + r(x)$

$q_1(x) + q_2(x) + \dots$ $\deg r < \deg d$.

Euclidean division for polynomials in $\mathbb{F}[x]$

Example: $f(x) = 3x^5 + x^3 - 2x^2 + 1, \quad d(x) = x^2 - 2 \in \mathbb{R}[x]$.

$$
\begin{array}{l|l}
3x^5 + x^3 - 2x^2 + 1 & x^2 - 2 \\
\underline{3x^5 - 6x^3} & \\
7x^3 - 2x^2 + 1 & \\
\underline{7x^3 - 14x} & \\
-2x^2 + 14x + 1 & \\
\underline{-2x^2 + 4} & \\
14x - 3 &
\end{array}
\qquad 3x^3 + 7x - 2
$$

$\Rightarrow \quad q(x) = 3x^2 + 7x - 2$

$r(x) = 14x - 3$

$1 = \deg r < \deg d = 2.$

Euclidean domains

Definition

A commutative ring A is a Euclidean domain if

1. A is an integral domain,
2. There exist a function $\nu : A \setminus \{0\} \to \mathbb{N}$ such that for all $a, b \in A$, $b \neq 0$, there exist $q, r \in A$ such that $a = qb + r$ and either $r = 0$, or $\nu(r) < \nu(b)$.

Examples:

1. $\mathbb{Z}$ with $\nu(n) = |n| \in \mathbb{N}$. $a = bq + r$, $|r| < |b|$
2. Any field with $\nu : \mathbb{F} \setminus \{0\} \to \mathbb{N}$ any function $a = bq + 0$, $r = 0$
3. $\mathbb{F}[x]$, $\mathbb{F}$ a field with $\nu(f(x)) = \deg(f)$. $f(x) = q(x) \cdot d(x) + r(x)$
4. * $\mathbb{Z}[i] = \{a + bi\}_{a,b \in \mathbb{Z}}$ with $\nu(a + ib) = a^2 + b^2$. (not a part of the course)

← Gaussian integers

Euclidean domains

Proposition

A Euclidean domain is a PID (principal ideal domain).

Proof: Let E be a Euclidean domain, $I \subset E$ an ideal

If $I = \{0\}$, then $I = (0)$. done

If $I \neq \{0\}$, let $d \in I$ $d \neq 0$ s.t. $\nu(d)$ is the minimum on I

Suppose $a \in I$, $a \neq 0$ $\Rightarrow \exists q, r : \underbrace{a}_{\in I} = q\underbrace{d}_{\in I} + r \Rightarrow r \in I \Rightarrow \begin{cases} \nu(r) < \nu(d) \\ r = 0 \end{cases}$

$\nu(r) < \nu(d)$ impossible since $\nu(d)$ is minimal on I

$\Rightarrow r = 0$ and $a = qd \Rightarrow I = (d)$.

$\Rightarrow E$ is a PID.

Conclusions

Let $\mathbb{F}$ be a field. Then the ring $\mathbb{F}[x]$ is a PID, meaning that any ideal in $\mathbb{F}[x]$ is generated by a single element.

$\forall$ nonzero elt is invertible — admits Euclidean division — ideals gen by 1 elt — no nontrivial zero divisors — multiplication is comm.

Fields $\subset$ Euclidean domains $\subset$ PID $\subset$ Integral domains $\subset$ Comm. rings

$\mathbb{R}, \mathbb{C}$, $\mathbb{Z}/p\mathbb{Z}$ p prime

$\mathbb{Z}$, $\mathbb{R}[x]$

$\mathbb{Z}, \mathbb{C}[x]$

$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$

PID, not Euclidean

$\mathbb{Z}[x]$

$\mathbb{R}[x,y]$

$\mathbb{Z}/4\mathbb{Z}$