Algebra MATH-310

Lecture 11

Anna Lachowska

December 2, 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 4

(a) $\gcd$ and lcm in integral domains.

(b) Properties of a Euclidean domain.

(c) CRT in Euclidean domains and polynomial rings.

(d) Congruences in polynomials rings.

(e) Maximal ideals in PID.

Recall: Euclidean domains

Definition

E is an integral domain such that the Euclidean division works in E: There exist a function $\nu : E \setminus \{0\} \to \mathbb{N}$ such that for any $a, b \in E$, $b \neq 0$, there exist $q, r \in E$ such that $a = qb + r$ and either $r = 0$ or $\nu(r) < \nu(b)$.

$\nu : \mathbb{F}[x] \setminus \{0\} \to \mathbb{N}$ is the degree of the polynomial.

Properties:

1. Euclidean domain is a PID.
2. If F is a field, then $F[x]$ is a Euclidean domain.

Today: The Chinese remainder theorem for Euclidean domains.

Divisibility in commutative rings

Definition

1. Let A be a commutative ring. We say that a divides b for $a, b \in A$ if there exist $c \in A$ such that $b = ac$.
2. We say that $d = \gcd(a, b)$ if $d \,|a$, $d \,|b$, and if $c \,|a$, $c \,|b$, this implies that $c \,|d$.
3. We say that $k = \operatorname{lcm}(a, b)$ if $a \,|e$, $b \,|e$, and if $a \,|f$, $b \,|f$, this implies that $e \,|f$.

In general $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$ are not unique.

Proposition

Let A be an integral domain, $a, b \in A$ nonzero elements. If d_1, d_2 are greatest common divisors of a and b, then $d_1 = xd_2$, where $x \in A^*$ is a unit. If e_1, e_2 are least common multiples of a and b, then $e_1 = ye_2$, where $y \in A^*$ is a unit.

Proof: $d_1 = gcd(a,b)$, $d_2 = gcd(a,b) \Rightarrow d_1 = xd_2$; $d_2 = zd_1 \Rightarrow$

$d_1 = xd_2 = xzd_1 \Rightarrow d_1(1-xz) = 0 \Rightarrow (1-xz) = 0 \Rightarrow xz = 1$

A integral domain

$\Rightarrow$ both x and z are units in A.

The case of $lcm(a,b)$ is similar ▨

Definition

Let A be an integral domain. Elements $a, b \in A$ are associates if there exists a unit $u \in A^*$ such that $b = au$ (equivalently, there exist a unit $v \in A^*$ such that $a = vb$).

Associates in an integral domain

Proposition

Associates generate the same ideal in a PID.

If $g = u f$ (u unit) $\Rightarrow g \in (f) \Rightarrow (g) \subset (f)$, since $xg = xuf \in (f)$ $\forall x \in A$.

$f = u^{-1} g \Rightarrow f \in (g) \Rightarrow (f) \subset (g)$

$\Rightarrow (g) = (f)$ $\Leftrightarrow$ g and f are associates

Examples. $A = \mathbb{Z} \Rightarrow$ units $\{\pm 1\}$ n, m are associates $\Leftrightarrow n = \pm m$ in $\mathbb{Z}$

$(m) = (-m) \subset \mathbb{Z}$

$A = \mathbb{F}[x] \Rightarrow$ units $\mathbb{F}^* = \mathbb{F} \setminus \{0\} \Rightarrow f(x), g(x)$ are associates $\Leftrightarrow$

($\mathbb{F}$ field)

$f(x) = \alpha g(x)$, $\alpha \in \mathbb{F}^*$

$(f(x)) = (\alpha f(x)) \subset \mathbb{F}[x]$

Properties of a Euclidean domain

See rings.pdf

Let E be a Euclidean domain and $a, b \in E$ nonzero elements.

1. $\gcd(a, b)$ can be found by the Euclidean division.
2. $(a) + (b) = (\gcd(a, b))$. Bezout's theorem holds.
3. $(a) \cap (b) = (\mathrm{lcm}(a, b))$.
4. If $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$, then $\gcd(a, bc) = 1$.
5. If $\gcd(a, b) = 1$, then $\mathrm{lcm}(a, b) = ab$.

$a = q_1 b + r_1$
$b = q_2 r_1 + r_2$
$\vdots$

Chinese remainder theorem for a Euclidean domain

Theorem

pairwise coprime

Let E be a Euclidean domain, $m_1, \dots m_r \in E$ such that $\gcd(m_i, m_j) = 1$ for $i \neq j$. Then

$$f : E/(m_1 \dots m_r) \xrightarrow{\sim} E/(m_1) \times E/(m_2) \times \dots \times E/(m_r)$$

is a ring isomorphism given by

$$[x]_{(m_1 \dots m_r)} \to ([x]_{(m_1)}, [x]_{(m_2)}, \dots [x]_{(m_r)}).$$

Idea: (1) homomorphism of rings by construction

(2) Surjectivity by induction:

CRT for 2 factors : $\exists\, a_{12} \in E$: $a_{12} \equiv a_1 \pmod{m_1}$, $a_{12} \equiv a_2 \pmod{m_2}$ $\quad (m_1) + (m_2) = E$

$\gcd(m_3, m_1 m_2) = 1 \Rightarrow$ CRT for 2 factors $\Rightarrow (m_3) + (m_1 m_2) = E$

$\Rightarrow \exists\, a_{123} \in E$:

Chinese remainder theorem for a Euclidean domain

$\exists\, a_{123} \in E$: $\quad a_{123} \equiv a_{12} \pmod{m_1 m_2} \Rightarrow \begin{cases} a_{123} \equiv a_1 \pmod{m_1} \\ a_{123} \equiv a_2 \pmod{m_2} \end{cases}$

$a_{123} \equiv a_3 \pmod{m_3}$

$\Rightarrow$ continue until all congruences are solved.

(3) Injectivity: if $a \equiv a_i \pmod{m_i}$ and $b \equiv a_i \pmod{m_i}$ $\forall i \Rightarrow$

$a - b \in \bigcap_{i=1}^{r} (m_i) \Rightarrow a - b \in (\operatorname{lcm}(m_1, \dots m_r)) = (m_1 \cdot m_2 \cdot \dots \cdot m_r)$.

$\gcd(m_i, m_j) = 1$

Corollary $F[x]$ is a Euclidean domain.

Let F be a field, $\{f_1(x), \dots f_r(x)\}$ polynomials in $F[x]$ satisfying $\gcd(f_i(x), f_j(x)) = 1$ for all $i \neq j$. Then

$$F[x]/(f_1(x) \dots f_r(x)) \simeq F[x]/(f_1(x)) \times F[x]/(f_2(x)) \times \dots \times F[x]/(f_r(x)).$$

Monic $\gcd$ of two polynomials

Remark: $\gcd(f(x), g(x))$ is determined up to a unit in $F[x]$, which is a nonzero constant in F. Therefore there exist a unique $\gcd(f(x), g(x))$ with the leading coefficient equal to 1.

"coefficient of the highest degree in $f(x)$

Definition

A polynomial $f(x) \in F[x]$ is monic if its leading coefficient is 1.

For any nonzero $f(x)$ and $g(x)$ there exist a unique monic $\gcd(f(x), g(x))$.

Example: monic gcd of two polynomials

Find the monic $\gcd(f(x), g(x))$.

$f(x) = x^4 - x^3 + 3x^2 + 2x - 5$

$g(x) = x^2 - 2x + 1$ in $\mathbb{R}[x]$

$$\begin{array}{r|l} x^4 - x^3 + 3x^2 + 2x - 5 & x^2 - 2x + 1 \\ \hline -(x^4 - 2x^3 + x^2) & x^2 + x + 4 \\ \hline x^3 + 2x^2 + 2x - 5 & \\ -(x^3 - 2x^2 + x) & \\ \hline 4x^2 + x - 5 & \\ -(4x^2 - 8x + 4) & \\ \hline 9x - 9 & \end{array}$$

$r_1(x)$

$\deg r_1 = 1 < \deg g = 2$

$$\begin{array}{r|l} x^2 - 2x + 1 & 9x - 9 \\ \hline -(x^2 - x) & \frac{1}{9}x - \frac{1}{9} \\ \hline -x + 1 & \\ -(-x + 1) & \\ \hline 0 & \end{array}$$

$r_1 = 9x - 9 = \gcd(f(x), g(x))$

The monic $\gcd(f(x), g(x)) = x - 1$

leading coefficient is 1.

Application of CRT to systems of congruences in $F[x]$

Example: Let $\mathbb{F}_3 = \{0, 1, 2\} = \mathbb{Z}/3\mathbb{Z}$. Find all solutions of the system of congruences in $\mathbb{F}_3[x]$:

$$\begin{cases} f(x) \equiv x + 1 \pmod{(x^2+1)} \\ f(x) \equiv 1 \pmod{(x)} \\ f(x) \equiv -x \pmod{(x^2-1)} \end{cases}$$

$g_1(x)$ $g_2(x)$ $g_3(x)$

Check that (x^2+1) (x) (x^2-1) are pairwise coprime

(show that gcd = 1 for each pair)

or find $a(x), b(x) \in \mathbb{F}[x]$

$$a(x)g_1(x) + b(x)g_2(x) = 1$$

$$\Leftrightarrow \gcd(g_1(x), g_2(x)) = 1.$$

$$\begin{cases} (x^2+1)\cdot 1 + x\cdot(-x) = 1 \\ (x^2+1)\cdot 2 + (x^2-1)\cdot 1 = 1 \\ (x^2-1)\cdot 2 + x\cdot x = 1 \end{cases}$$

$\Rightarrow$ the polynomials $g_1(x), g_2(x), g_3(x)$ are pairwise coprime.

$\Rightarrow$ by CRT for Euclidean domains

$\exists$ solutions of the form $a(x) + ((x^2+1)\cdot x\cdot(x^2-1))$

How to find $a(x)$?

Example: How to solve a system of congruences? -I

Start with any 2 congruences : $\begin{cases} f(x) \equiv x+1 \pmod{(x^2+1)} \\ f(x) \equiv 1 \pmod{(x)} \end{cases}$

Try to find $h(x), g(x)$: $(x^2+1)h(x) + x + 1 = x \cdot g(x) + 1 \quad (= f(x))$

$$(x^2+1)h(x) - x \cdot g(x) = -x$$

Have: $(x^2+1)\cdot 1 + x\cdot(-x) = 1 \Rightarrow (x^2+1)\cdot(-x) + x\cdot(x^2) = -x$

$\Rightarrow f(x) = (x^2+1)\cdot(-x) + x + 1 = -x^3 + 1 \pmod{(x^3+x)} \equiv x+1 \pmod{(x^3+x)}$

$\Rightarrow$ Now we have $\begin{cases} f(x) \equiv x+1 \pmod{(x^3+x)} \\ f(x) \equiv -x \pmod{(x^2-1)} \end{cases}$

$h_1(x)\cdot(x^3+x) + x + 1 = g_1(x)\cdot(x^2-1) - x$

$h_1(x)(x^3+x) - g_1(x)(x^2-1) = x - 1$

$x(x^3+x) + (-x^2+1)(x^2-1) = -1 \Rightarrow$

$\underbrace{x(-x+1)}_{h(x)}(x^3+x) + \underbrace{(-x^2+1)(-x+1)}_{-g(x)}(x^2-1) = x-1$

$\Rightarrow f(x) = x(-x+1)(x^3+x) + x + 1 = x^5 + x^4 - x^3 + x^2 + x + 1 \pmod{(x^5-x)}$

$\Rightarrow f(x) = x^4 - x^3 + x^2 + 1 \pmod{(x^5-x)} \equiv x^4 + 2x^3 + x^2 + 1 \pmod{(x^5-x)}.$

Example: How to solve a system of congruences? -II

Let $g_1(x), g_2(x) \in F[x]$ polynomials such that $\gcd(g_1, g_2) = 1$.

$$\begin{cases} f(x) & \equiv & h_1(x) & (\mathrm{mod}(g_1(x))) \\ f(x) & \equiv & h_2(x) & (\mathrm{mod}(g_2(x))) \end{cases}$$

Since $\gcd(g_1, g_2) = 1$, we have $t_1(x), t_2(x) \in F[x]$ such that

$$t_1(x)g_1(x) + t_2(x)g_2(x) = 1.$$

$t_1(x), t_2(x)$ can be found by running the Euclidian algorithm backwards.

Therefore a solution can be written in the form

$$f(x) = h_1(x)t_2(x)g_2(x) + h_2(x)t_1(x)g_1(x).$$

$$f(x) = h_1(x)\underbrace{(1 - t_1(x)g_1(x))} + h_2(x)\underbrace{t_1(x)g_1(x)} \equiv h_1(x) \ (\mathrm{mod}(g_1(x))).$$

$$f(x) = h_1(x)t_2(x)g_2(x) + h_2(x)(1 - t_2(x)g_2(x)) \equiv h_2(x) \ (\mathrm{mod}(g_2(x))).$$

Solving congruences: general method

Let $g_1(x), g_2(x), \dots g_r(x) \in F[x]$ pairwise coprime polynomials. Consider the system of congruences

$\gcd(g_i(x), g_j(x)) = 1 \quad \forall i \neq j$

$$\begin{cases} f(x) \equiv h_1(x) \pmod{g_1(x)} \\ f(x) \equiv h_2(x) \pmod{g_2(x)} \\ \dots \quad \dots \quad \dots \\ f(x) \equiv h_r(x) \pmod{g_r(x)} \end{cases}$$

$G = g_1(x) \cdots g_r(x)$, $G_i(x) = G(x)/g_i(x)$

$\Rightarrow \gcd(G_i(x), g_i(x)) = 1 \quad \forall i$

$\Rightarrow \exists\, t_i(x), s_i(x) : t_i(x) G_i(x) + s_i(x) g_i(x) = 1 \quad \forall i$

$$\Rightarrow f(x) = \sum_{i=1}^{r} h_i(x) G_i(x) t_i(x)$$

Example: $r = 3$.

$$f(x) = h_1(x) \underbrace{G_1(x) t_1(x)}_{(1 - g_1(x) s_1(x))} + h_2(x) \underbrace{G_2(x) t_2(x)}_{(1 - g_2(x) s_2(x))} + h_3(x) \underbrace{G_3(x) h_3(x)}_{(1 - g_3(x) s_3(x))}$$

($g_1(x)$ over $G_2(x)$, $g_1(x)$ over $G_3(x)$)

$$\equiv h_1(x) \pmod{g_1(x)}$$
$$\equiv h_2(x) \pmod{g_2(x)}$$
$$\equiv h_3(x) \pmod{g_3(x)}$$

Example: How to solve a system of congruences? - III

$$\begin{cases} f(x) \equiv x+1 \pmod{(x^2+1)} & g_1(x) \\ f(x) \equiv 1 \pmod{(x)} & g_2(x) \\ f(x) \equiv -x \pmod{(x^2-1)} & g_3(x) \end{cases}$$

$G_1(x) = x(x^2-1)$ $G_2(x) = (x^2+1)(x^2-1)$

$G_3(x) = x(x^2+1)$

$\Rightarrow \gcd(G_i(x), g_i(x)) = 1 \quad \forall i$

$(x^2+1)(x^2+1)$	$-x\cdot(x^3-x)$	$= 1$
$x^3 \cdot x$	$-1\,(x^4-1)$	$= 1$
$(x^2-1)(x^2-1)$	$-x(x^3+x)$	$= 1$
	$t_i(x)\,G_i(x)$	

$\Rightarrow f(x) = \sum h_i(x)\,t_i(x)\,G_i(x) = (x+1)(-x)(x^3-x) + 1\cdot(-1)\cdot(x^4-1) + (-x)\cdot(-x)(x^3+x) =$

$= x^4+2x^3+x^2+1$ is a solution mod $(x(x^2+1)(x^2-1))$

$x^4+2x^3+x^2+1 \equiv 1 \pmod{x}$

$\Rightarrow f(x) = x^4+2x^3+x^2+1$ is a solution.

$x^4+2x^3+x^2+1 \;\big|\; x^2+1$

$-x^4 \quad -x^2 \;\big|\; x^2+2x$

$2x^3 \quad +1$

$2x^3+2x$

$-2x+1 = x+1 = h_1(x)$ in $\mathbb{F}_3[x]$

$x^4+2x^3+x^2+1 \;\big|\; x^2-1$

$x^4 \quad -x^2 \;\big|\; x^2+2x+2$

$2x^3+2x^2+1$

$-2x^3 \quad -2x$

$2x^2+2x+1$

$2x^2 \quad -2$

$2x = -x = h_3(x)$ in $\mathbb{F}_3[x]$

When is E/I a field?

We will consider in detail the rings of the form $F[x]/(f(x))$ where F is a field and $f(x) \in F[x]$ a polynomial. Since $F[x]$ is a PID, any ideal in $F[x]$ is generated by a single polynomial.
We want to know in which case $F[x]/(f(x))$ is a field.

Definition

Let A be an integral domain. An element $c \in A$ is irreducible if $c \neq 0$, c is not a unit and if $c = ab$, then either a or b is a unit.

Example. $A = \mathbb{Z}$. Irreducible elements?

$6 = 2 \cdot 3$ is not irreducible since 2, 3 are both non-units

$c = \pm p \Rightarrow p = (-1)\cdot(-p) = 1 \cdot p$

$-p = (-1)\cdot p = 1 \cdot (-p)$

where p is a prime are the only irreducible elts in $\mathbb{Z}$

Maximal ideals and irreducible elements

Definition

We say that an ideal $I \subset A$ is maximal if there is no ideal $J \subset A$ such that $I \subsetneq J \subsetneq A$.

Theorem

Let A be a PID. Then $p \in A$ is irreducible if and only if $p \neq 0$ and $(p) \subset A$ is maximal.

Proof: ($\Rightarrow$) p is irreducible. Suppose $\exists\, J \subset A : (p) \subsetneq J \subsetneq A$.

Since A is a PID $\Rightarrow J = (d) \Rightarrow p = dt$, $p \in J = (d)$

$p = dt$, p irreducible $\Rightarrow$
- d is a unit $\Rightarrow d \cdot d^{-1} = 1 \in J \Rightarrow J = A$ impossible
- t is a unit $\Rightarrow p$ and d are associates $\Rightarrow (d) = (p)$ impossible

$\Rightarrow (p) \subset A$ is maximal.

Maximal ideals and irreducible elements

($\Leftarrow$) $p \neq 0$ and $(p) \subset A$ is maximal. Show that p is irreducible

Suppose $p = yz$, y and z are both non-units.

$\Rightarrow p < (y) \subsetneq A$ (since y is not a unit)

Show that $(p) \subsetneq (y)$. Otherwise $y \in (p) \Rightarrow y = p \cdot t$, $p = y \cdot z = p \cdot t \cdot z$

$\Rightarrow p(1 - tz) = 0 = \begin{cases} p = 0 \text{ impossible, } p \neq 0 \\ tz = 1 \Rightarrow z \text{ is a unit, contradiction.} \end{cases}$

$\Rightarrow (p) \subsetneq (y) \subsetneq A$ contradicts $(p) \subset A$ is maximal

$\Rightarrow p$ is irreducible. ▨

Poll: Associates in a polynomial ring

Let $A = \mathbb{Z}/5\mathbb{Z}\,[x]$. Then

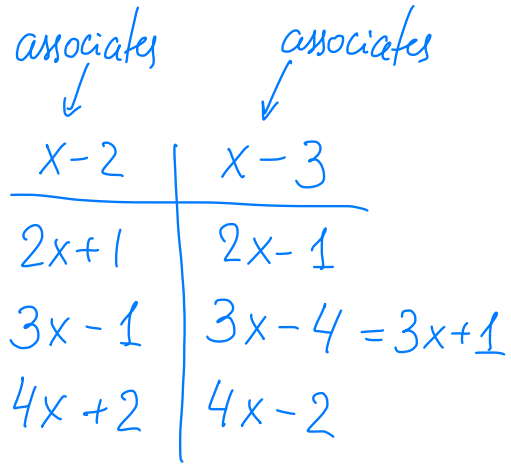
A: $(2x-1)$ and $(4x+2)$ are associates in A

B: $(x-2)$ and $(4x-2)$ are associates in A

C: $(2x-1)$ and $(3x+1)$ are associates in A

D: $(4x+2)$ and $(3x-4)$ are associates in A

E: $(2x+1)$ and $(x-3)$ are associates in A



When is E/I a field?

Theorem

Let A be a Euclidean domain. Then
$I \subset A$ is maximal $\iff$ A/I is a field
$\iff$ *$I = (d)$, $d \in A$ is irreducible.*

.... proof next time!

When is E/I a field?

Corollary

Let F be a field. Then
$F[x]/(f(x))$ is a field $\iff$ $f(x) \in F[x]$ is irreducible.