Algebra MATH-310

Lecture 12

Anna Lachowska

December 9, 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 5

(a) When is A/I a field?

(b) Irreducible elements in polynomial rings

(c) Finite fields

Recall: Maximal ideals and irreducible elements

1. Maximal ideal: $I \subset A$ is maximal if there is no ideal $J \subset A$ such that $I \subsetneq J \subsetneq A$.
2. Let A be a PID. Then $p \in A$ is irreducible if and only if $p \neq 0$ and $(p) \subset A$ is maximal.

When is A/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: $\Leftarrow$) If $I=(0) \Rightarrow A/I = A$ is a field $\Rightarrow$ any $b \neq 0$ is a unit
$\Rightarrow (b) = A \Rightarrow (0) < A$ is maximal.

If $I=(a)$, $a \neq 0$. If (a) is not maximal $\Rightarrow (a) \subsetneq (b) \subsetneq A \Rightarrow$
$a = bt$, b and t are non-units

If b is a unit $\Rightarrow (b) = A$ ✗
If t is a unit $\Rightarrow (b) = (a)$ ✗
$b \neq ka$ otherwise $b \in (a) \Rightarrow (b) = (a)$ ✗
$t \neq sa$ otherwise $a = bt = bsa \Rightarrow a(1-bs) = 0$
$a \neq 0 \Rightarrow 1 - bs = 0 \Rightarrow b, s$ are units ✗

$\Rightarrow [b]_{(a)} \cdot [t]_{(a)} = [0]_{(a)} \Rightarrow A/(a)$ is not a field
$\neq 0$ $\neq 0$ nontrivial zero divisors

When is A/I a field?

($\Rightarrow$) Suppose $[b]_{(a)}$ is not invertible in $A/(a)$ $\Rightarrow$ $[b]$ generates an ideal in A/I, which is proper, $[b] \neq 0 \Rightarrow b \notin (a)$

$\Rightarrow (a) \subsetneq (b) \subsetneq A \Rightarrow (a)$ is not maximal in A.

Corollary

Let F be a field. Then

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

Conclusions: Properties of polynomial rings over a field F

1. $F[x]$ is a Euclidean domain $\Longrightarrow$ it is a PID $\Longrightarrow$ any ideal $I \subset F[x]$ is generated by a single element, $I = (f(x))$.
2. $F[x]/(f(x))$ is a field $\Longleftrightarrow$ $f(x) \in F[x]$ is irreducible $\Longleftrightarrow$ $f(x)$ is not a product of two polynomials of degrees ≥ 1.
3. CRT for $F[x]$: can solve systems of congruences modulo pairwise coprime polynomials.
4. $(f(x)) + (g(x)) = (\gcd(f(x), g(x))$;
   $(f(x)) \cap (g(x)) = (\mathrm{lcm}(f(x), g(x))$.
   The $\gcd$ and lcm of two polynomials are defined up to a multiplication by a unit. There exists a unique monic $\gcd(f(x), g(x))$.

When is a polynomial $f(x) \in F[x]$ irreducible?

Theorem

1. *Any polynomial of degree* 1 *is irreducible in* $F[x]$.
2. *A polynomial of degree* **2,3** *is irreducible* $\iff$ *it has no roots in* F.
3. *Let* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ *considered over* $\mathbb{Q}[x]$. *Suppose that* $\alpha = \frac{r}{s} \in \mathbb{Q}$ *is a root of* $f(x)$. *Then* s *divides* a_n *and* r *divides* a_0.

(1) $f(x) = g(x)h(x)$, $\deg = 1$

$\deg f = \deg g + \deg h$ $\Rightarrow$ at least one of $h(x), g(x)$ is a nonzero const.

$1 = 0 + 1$

$1 = 1 + 0$

(2) $f(x) = g(x)h(x)$, $\deg = 2$ or 3

$\deg f = \deg g + \deg h$ $\Rightarrow$ at least one of $h(x), g(x)$ of $\deg = 1$

$2, 3 =$ non-const. $g(x) = ax + b$, $a \neq 0$ $\Rightarrow a\left(x + \frac{b}{a}\right) \Rightarrow f\left(-\frac{b}{a}\right) = 0$.

(3)

$$f\left(\frac{r}{s}\right) \cdot s^n = \overbrace{a_n r^n + a_{n-1} r^{n-1} s + \ldots + a_1 r s^{n-1}}^{s \text{ divides}} + a_0 s^n = 0 \Rightarrow \begin{matrix} r \text{ divides } a_0 \\ s \text{ divides } a_n \end{matrix}$$

(r divides)

In particular, in $\mathbb{Q}$ roots of monic ($a_n = 1$) polynomials with integer coeff are integers

When is a polynomial $f(x) \in F[x]$ irreducible?

Theorem

(The Eisenstein criterion).
Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ *such that* $\gcd(a_0, \ldots a_n) = 1$. *Suppose that* p *is a prime such that* p *divides* a_i $\forall\ 0 \leq i \leq n-1$, p *does not divide* a_n *and* p^2 *does not divide* a_0. *Then* $f(x)$ *is irreducible in* $\mathbb{Q}[x]$.

See rings.pdf for a proof.

Remark: Sometimes it helps to make a change of variables $x \to y = x + a$ in the polynomial and then apply the Eisenstein criterion. If $f(x) = g(x)h(x)$, then $\tilde{f}(y) = \tilde{g}(y)\tilde{h}(y)$. If $\tilde{f}(y)$ is irreducible, so is $f(x)$.

Examples of irreducible polynomials

1. $g(x) = 2x^3 + 4x^2 + 11x + 1 \in \mathbb{Q}[x]$.

If $\frac{r}{s}$ is a root $\Rightarrow$ r divides $1 = a_0$, s divides $2 = a_n$ $\Rightarrow$ $r \in \{\pm 1\}$, $s \in \{\pm 1, \pm 2\}$

$\Rightarrow \frac{r}{s} \in \{\pm \frac{1}{2}, \pm 1\}$ $\Rightarrow$ Check $g(\pm 1) \neq 0$, $g(\pm \frac{1}{2}) \neq 0$, $\deg g = 3$

$\Rightarrow$ it is irreducible

2. $f(x) = 7x^5 + 12x^4 + 18x^3 - 9x + 15 \in \mathbb{Q}[x]$.

$3 \nmid 7$ $3 \mid 12$ $3 \mid 18$ $3 \mid -9$ $3 \mid 15$

$9 \nmid 15$ $\Rightarrow$ By Eisenstein irreducible.

3. $h(x) = x^k - p \in \mathbb{Q}[x]$, p a prime

$p \nmid 1$ $p \mid p$, $p^2 \nmid p$ irreducible by Eisenstein $\forall k \geq 1$

Consider $x^{2k} - p^2 = (x^k - p)(x^k + p)$ is not irreducible

$p^2 \mid p^2$ $\Rightarrow$ Eisenstein is not applicable

Quotients of polynomial rings

Proposition

1. *If $f(x) \in F[x]$, F a field, is irreducible of degree n, then any element of $K = F[x]/(f(x))$ is of the form*

$$a_0 + a_1\overline{x} + \ldots + a_{n-1}\overline{x}^{n-1},$$

where $a_i \in F$, $\overline{x}^i = \{x^i + f(x)g(x)\}_{g(x)\in F[x]}$ is a representative of a congruence class modulo $f(x)$.

2. *If F is a finite field with $|F| = q$ and $f(x)$ is irreducible in $F[x]$ of degree n, then the field $K = F[x]/(f(x))$ has q^n elements.*

Idea: $a(x) = \underbrace{f(x)q(x)}_{\in (f(x))} + r(x)$ $\quad \deg r < \deg f$

$\deg r \leq n-1$

(2) follows from (1)

Quotients of polynomial rings: examples

(1) Let $F = \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ and $f(x) = x^3 + x^2 + 1 \in \mathbb{F}_2[x]$.

Consider $K = \mathbb{F}_2[x]/(f(x))$. is a field ← is it irreducible?

$f(0) = 0+0+1 = 1$
$f(1) = 1+1+1 = 1$
no roots, deg = 3 => $f(x)$ is irreducible.

$\Rightarrow \quad |K| = 2^3 = 8$

elements of the form $a\overline{x}^2 + b\overline{x} + c$, $a, b, c \in \mathbb{F}_2$

$\{0, 1, \overline{x}, \overline{x}^2, \overline{x}+1, \overline{x}^2+1, \overline{x}^2+\overline{x}, \overline{x}^2+\overline{x}+1\}$ all nonzero elements are invertible in K.

Inverse of $\overline{x}$ in K = ?

$\gcd(x, x^3+x^2+1) = 1 \Rightarrow \exists\, h(x), g(x) : x \cdot g(x) + (x^3+x^2+1) \cdot h(x) = 1$

$x \cdot (x^2+x) + (x^3+x^2+1) = 1$ over $\mathbb{F}_2 = \{0, 1\}$

$\Rightarrow (\overline{x})^{-1} = (\overline{x}^2+\overline{x}) \in K$

(2) Let $F = \mathbb{R}$, $f(x) = x^2 + 1$, consider $\mathbb{R}[x]/(f(x))$. = M is a field

$f(x)$ irreducible over $\mathbb{R}$ no roots, deg = 2

$\{a + b\overline{x}\}_{a,b \in \mathbb{R}}$ and $\overline{x} : \overline{x}^2 + 1 = 0 \Rightarrow \mathbb{R}[x]/(x^2+1) \simeq \mathbb{C}$.

Finite fields - easy facts

1. If a field K is finite, then $\mathrm{char}(K) = p$, a prime.

   $\tau: \mathbb{Z} \to K \quad \tau(1) = 1, \ \tau(m) = m \cdot 1 \neq 0 \ \forall m \in \mathbb{N} \Rightarrow K$ is infinite
   $\Rightarrow \tau(p) = 0$ for p a prime

2. If K is a finite field of characteristic p, then K contains a subfield isomorphic to $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

   $\tau: \mathbb{Z} \to K \Rightarrow \tau(p) = 0 \Rightarrow \mathbb{Z}/p\mathbb{Z} \xrightarrow{\tau} K$ injective $\Rightarrow \tau(\mathbb{Z}/p\mathbb{Z}) \subset K$

3. If K is a field with $|K| = p$, then $K \simeq \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$

   $\mathbb{Z}/p\mathbb{Z} \subset K \Rightarrow |K| = p \Rightarrow \mathbb{Z}/p\mathbb{Z} = K$

4. If K is a finite field of characteristic p, then $|K| = p^n$ for some $n \in \mathbb{N}_+$.

   Since K is a vector space over $\mathbb{Z}/p\mathbb{Z}$ $\quad \mathrm{char}\, K = p$.

Units in a finite field

Proposition

The group of units of a finite field is cyclic.

Proof: $|K^*| = n$, K^* is a finite abelian gp $\Rightarrow K^* \simeq C_{d_1} \times C_{d_2} \times \dots \times C_{d_s}$
gp of units
$d_1 | d_2 \dots | d_s$
invariant factors

Then $m = d_s$ is the max order of an elt in K^*
order of an elt $\leq$ order of $K^* \Rightarrow m \leq n$

We have $t^m = 1 \quad \forall t \in K^* \Rightarrow$ the elts of K^* are solutions of $t^m - 1 = 0$ of degree m. A polynomial of degree m has at most m roots in a field (Euclidean division: $t^m - 1 = (t-\alpha) h^{m-1}(t) + r$
α is a root, deg $= m$, deg $= 1$, $\alpha^m - 1 = 0 = (t-\alpha) h^{m-1}(t)$, deg $r < 1 \Rightarrow r = \text{const}$

$$\Rightarrow \underset{\deg = m}{(t^m - 1)} = \underset{\deg = 1}{(t-\alpha)} \underset{\deg = m-1}{h^{m-1}(t)}$$

$\Rightarrow n \leq m \Rightarrow n = m \Rightarrow K^* \simeq C_{d_s} = C_m$ ▨

Units in a commutative ring

Remark: The Proposition fails in general for commutative rings. In particular, a polynomial of degree m with coefficients in a commutative ring can have more than m roots.

Ex. $\mathbb{Z}/8\mathbb{Z}$: $x^2 - 1 = 0$ has 4 roots: $\{1, 7, 3, 5\}$

degree = 2

The gp of units $(\mathbb{Z}/8\mathbb{Z})^*$ is not cyclic $= \{1, 7, 3, 5\} = (\mathbb{Z}/8\mathbb{Z})^* \simeq C_2 \times C_2$

$\{(1,1), (1,t), (q,1), (q,t)\} \simeq C_2 \times C_2$

1 3 5 7

$q^2 = t^2 = 1$.

Units in a finite field: example

Let $f(x) = x^3 + x^2 + 1 \in \mathbb{F}_2[x]$ and $K = \mathbb{F}_2[x]/(f(x))$.

K^* is cyclic, $|K| = 8 \Rightarrow |K^*| = 8 - 1 = 7 \Rightarrow K^* \simeq C_7$

Since 7 is a prime $\Rightarrow$ any nonzero elt of K is a generator of $C_7 \simeq K^*$ as a group.

for example, $\bar{x} \in K^*$ is a generator

$$\{\bar{x}, \underbrace{\bar{x}^2}_{\bar{x}^2}, \underbrace{\bar{x}^2+1}_{\bar{x}^3}, \underbrace{\bar{x}^2+\bar{x}+1}_{\bar{x}^4}, \underbrace{\bar{x}+1}_{\bar{x}^5}, \underbrace{\bar{x}^2+\bar{x}}_{\bar{x}^6}, \underbrace{1}_{\bar{x}^7}\} = K^*$$

$$\bar{x}^3 = \bar{x}^2 + 1 \mod (x^3 + x^2 + 1)$$

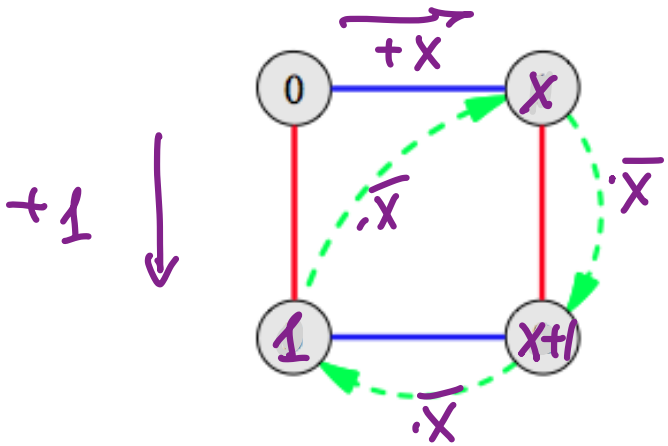
$$\bar{x}^3 + \bar{x} = x^2 + \bar{x} + 1 \mod (x^3 + x^2 + 1)$$

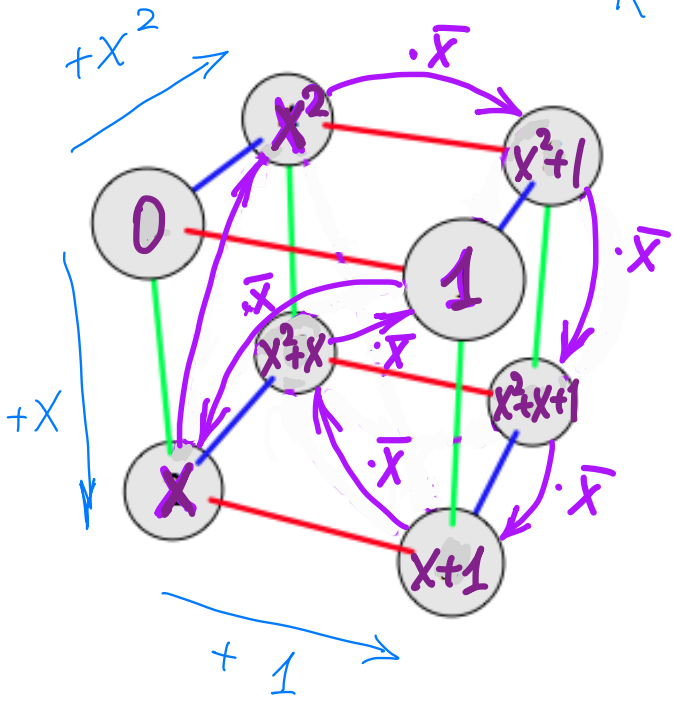
Visualization of finite fields

Addition along straight lines,
multiplication along curvy lines

K, $|K| = 8$ $\quad \operatorname{char} K = 2$.

$K = \mathbb{F}_2[x] / \langle x^3 + x^2 + 1 \rangle$





Exercise: $\mathbb{F}_2[x] / \langle x^2 + x + 1 \rangle \simeq L$

field of 4 elements, $\operatorname{char}(L) = 2$

$L = \{0, 1, \bar{x}, \bar{x}+1\}$

Classification of finite fields

Theorem

Let p be a prime, $n \in \mathbb{N}^*$. Then there exists a field K with $|K| = p^n$, and an irreducible polynomial $f(x) \in \mathbb{F}_p[x]$ such that $\mathbb{F}_p[x]/(f(x)) \simeq K$.

If $g(x)$ is another irreducible polynomial of degree n over $\mathbb{F}_p$, then

$$K \simeq \mathbb{F}_p[x]/(f(x)) \simeq \mathbb{F}_p[x]/(g(x)).$$

See rings.pdf

Example: $f(x) = x^3 + x^2 + 1 \in \mathbb{F}_2[x]$ and $g(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$.

$$\Longrightarrow \quad \mathbb{F}_2[x]/(f(x)) \simeq \mathbb{F}_2[x]/(g(x)).$$ [PS 13]

Irreducible polynomials over $\mathbb{F}_p$

Corollary

Over $\mathbb{F}_p$ there exist an irreducible polynomial of any degree $n \in \mathbb{N}^*$.

This fails for fields of characteristic 0.

over $\mathbb{R}$, the only irreducible polynomials are of degree 1 or 2
over $\mathbb{C}$ the only irreducible polynomials are of degree 1.

Definition

A field where the only irreducible polynomials are of degree 1 is called algebraically closed.

Ex. $\mathbb{C}$ is algebraically closed, but $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is not.

Poll: Irreducible polynomials

Which of the following polynomials is NOT irreducible? $\mathbb{F}_3 = \{0, 1, -1\} = \{0, 1, 2\}$

A: $x^3 + x^2 - 1$ over $\mathbb{F}_3$ deg = 3, no roots in $\mathbb{F}_3$ $\Rightarrow$ irreducible

B: $x^4 - x^2 + 1$ over $\mathbb{F}_3$ not irreducible: $(x^2+1)(x^2+1) = x^2+2x+1 = x^2-x+1$

C: $3x^5 + 4x^4 - 6x^2 + 8x - 10$ over $\mathbb{Q}$ irreducible by Eisenstein
(2 ∤ 3, 2 | 4, 2 | −6, 2 | 8, 2 | −10, 4 ∤ −10)

D: $x^2 + x - 1$ over $\mathbb{F}_3$ deg = 3, no roots in $\mathbb{F}_3$ $\Rightarrow$ irreducible

E: $x^3 + 2x + 7$ over $\mathbb{Q}$ deg = 3, if $\alpha = \frac{r}{s} \in \mathbb{Q}$ a root $\Rightarrow$ $s \mid 1$, $r \mid 7$ $\Rightarrow$ $\frac{r}{s} \in \{\pm 1, \pm 7\}$
$f(\pm 1) \neq 0$, $f(\pm 7) \neq 0$ $\Rightarrow$ irreducible

Conclusions: finite fields

1. For any prime p, any $n \in \mathbb{N}^*$ there exist a unique finite field $\mathbb{F}_{p^n}$ of p^n elements, with $\mathrm{char}(\mathbb{F}_{p^n}) = p$.

2. For $n = 1$, this finite field is isomorphic to $\mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$.

3. For $n > 1$, this unique field can be constructed as a quotient

$$\mathbb{F}_{p^n} \simeq \mathbb{F}_p[x]/(f(x)),$$

where $f(x) \in \mathbb{F}_p[x]$ is an irreducible polynomial of degree n.

Remark on finite fields

$\mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$ but $\mathbb{F}_{p^n} \not\simeq \mathbb{Z}/p^n\mathbb{Z}$. $n \geq 2$

$n = 1$

unique field of p^n elts

ring with zero divisors

$[p^s] \cdot [p^t] = [0]$ in $\mathbb{Z}/p\mathbb{Z}$

$s + t = n$

The end.