Algebra MATH-310

Lecture 12

Anna Lachowska

December 8, 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 5

(a) When is A/I a field?

(b) When is $F[x]/(f(x))$ a field?

(c) Irreducible elements in polynomial rings

(d) Finite fields

Recall: When is A/I a field?

1. Maximal ideal: $I \subsetneq A$ is maximal if there is no ideal $J \subsetneq A$ 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 not a unit, and if $p = ab \Rightarrow$ either a or b is a unit.
3. Let A be a PID. Then
   $I \subset A$ is maximal $\iff A/I$ is a field
   $\iff I = (d)$, $d \in A$ is irreducible.
4. Let F be a field. Then $F[x]$ is a Euclidean domain $\implies$ a PID.
   $F[x]/(f(x))$ 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 *or* 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) $f(x) = g(x)h(x)$, $\deg = 1$

$\deg f = \deg g + \deg h$ $\Rightarrow$ exactly one of $g(x), h(x)$ is a nonzero constant.

$1 = 1 + 0$

$0 + 1$ $\Rightarrow$ by def $f(x)$ is irreducible.

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

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

$2, 3$ non-constants has degree 1 $\Rightarrow g(x) = ax + b = a(x + \frac{b}{a})$

$\Rightarrow f(-\frac{b}{a}) = 0$.

(3) $f(\frac{r}{s}) \cdot s^n = a_n r^n + a_{n-1} r^{n-1} s + \ldots + a_1 r s^{n-1} + a_0 s^n = 0$ $\Rightarrow$ r divides a_0, s divides a_n

(r divides the first terms; s divides the last terms)

In particular, in $\mathbb{Q}$ roots of monic polynomials with integer coefficients 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_Math310.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. $g(x) = 2x^3 + 4x^2 + 11x + 1 \in \mathbb{Q}[x]$.

deg = 3 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 $g(\pm 1) \neq 0$, $g(\pm\frac{1}{2}) \neq 0$ $\Rightarrow g(x)$ is irreducible.

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

3 ✗ 3 | 3 | 3 | 3 | 9 ✗ $\Rightarrow$ By Eisenstein irreducible

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

$p \nmid 1$ $p \mid p$, $p^2 \nmid p$ p is a prime $\Rightarrow$ By Eisenstein irreducible $\forall k \geq 1$

On the other hand, consider $X^{2k} - p^2 = (x^k - p)(x^k + p)$ not irreducible

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

Quotients of polynomial rings

Proposition

1. *If F is a field and $f(x) \in F[x]$ 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.*

(1) Idea: $a(x) = \underbrace{f(x)\,q(x)}_{\in (f(x))} + r(x)$ $\quad \deg r < \deg f \Rightarrow \deg r \leq n-1$

(2) Follows from (1)

Quotients of polynomial rings: examples

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

deg = 3

$f(0) = 0+0+1 = 1 \neq 0$

$f(1) = 1+1+1 = 1$

$\Rightarrow f(x)$ is irreducible

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

$|K| = 2^3 = 8$, of the form $a\bar{x}^2 + b\bar{x} + c$, $a, b, c \in \mathbb{F}_2$

$\{0, 1, \bar{x}, \bar{x}+1, \bar{x}^2, \bar{x}^2+1, \bar{x}^2+\bar{x}, \bar{x}^2+\bar{x}+1\}$ all nonzero elts are invertible in K

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

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

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

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

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

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

Finite fields - easy facts

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

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

   $\Rightarrow \tau(p) = 0$, p is a prime (proved char of a field is 0 or a prime)

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

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

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

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

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 $\mathbb{Z}/p\mathbb{Z}$

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 $\Rightarrow K^* \simeq C_{d_1} \times C_{d_2} \times \dots \times C_{d_s}$, $d_1 | d_2 | \dots | d_s$ (invariant factors)

gp of units

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 $t^m = 1$ $\forall t \in K^*$ $\Rightarrow$ the elts of K^* are solutions of $t^m - 1 = 0$

A polynomial of deg $= m$ has at most m roots in a field

Euclidean division: $t^m - 1 = (t-\alpha) h^{m-1}(t) + r$, $\deg r < 1$ $\Rightarrow \alpha^m - 1 = (\alpha - \alpha) h^{m-1}(\alpha) + r = 0$ $\Rightarrow r = 0$

(α is a root; $\deg = 1$)

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

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

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. $\mathbb{Z}/8\mathbb{Z}$: $x^2 - 1 = 0$ (degree $= 2$) roots: $\{1, 7, 3, 5\}$

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

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

$q^2 = t^2 = 1$

$1 \quad 3 \quad 5 \quad 7$

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, $|K| = 8 \Rightarrow |K^*| = 7 \Rightarrow K^* \simeq C_7$

Since 7 is a prime $\Rightarrow$ any nontrivial elt of K^* is a generator of K^*

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

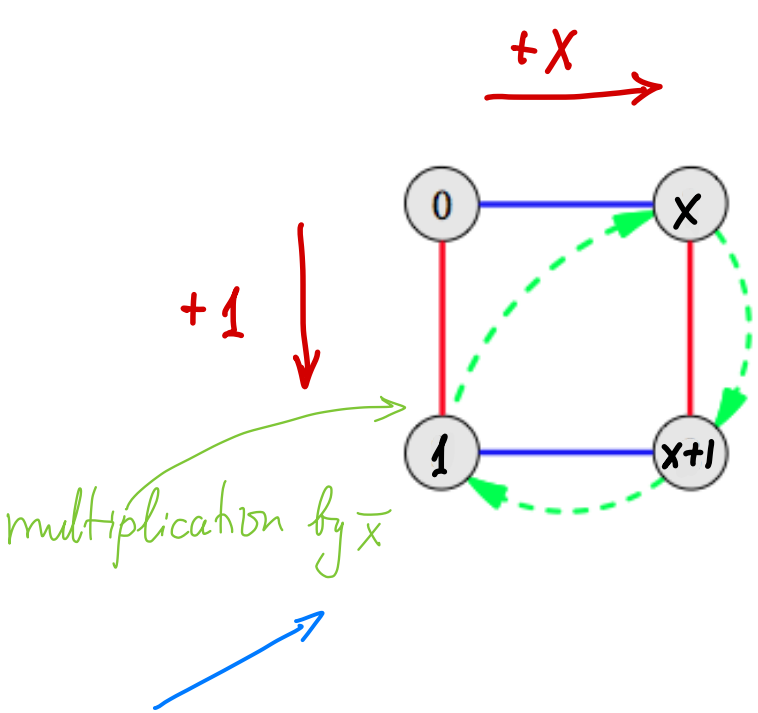
$$\{\bar{x}, \underbrace{\bar{x}^2}_{\bar{x}^2}, \underbrace{\bar{x}^2+1}_{\bar{x}^3}, \underbrace{\bar{x}^2+\bar{x}+1}_{\bar{x}^4}, \underbrace{\bar{x}+1}_{\bar{x}^5}, \underbrace{\bar{x}^2+\bar{x}}_{\bar{x}^6}, \underbrace{1}_{\bar{x}^7}\} = K^*$$

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

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

Visualization of finite fields

(Addition along straight lines)

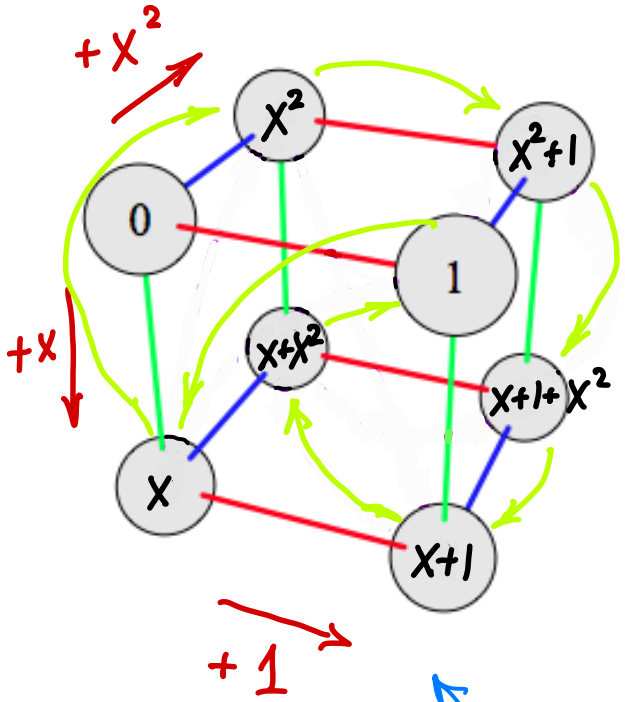


$\mathbb{F}_2[x]/\langle x^2+x+1\rangle \simeq L$

field of 4 elements

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

$L^* \simeq C_3$



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

field of 8 elements

$K^* \simeq C_7$

Exercise: draw the multiplication by $\bar{x}$ with arrows

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_Math 310

It works because in K^* all elts satisfy $x^{p^n-1} - 1 = 0$, $x^{p^n} - x = 0$

all elts of $\overline{K}$ satisfy this

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

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

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; $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is not

Poll: Irreducible polynomials

Which of the following polynomials is NOT irreducible?

A: $x^3 + 2x + 11$ over $\mathbb{Q}$ irred.

deg = 3, if $\alpha = \frac{r}{s}$ a root $\Rightarrow$ $s \mid 1$, $r \mid 11$ $\Rightarrow$ no roots

$\frac{r}{s} \in \{\pm 1, \pm 11\}$

B: $x^3 + x^2 - 1$ over $\mathbb{F}_3$ irred.

deg = 3, check $f(1) \neq 0$, $f(-1) \neq 0$, $f(0) \neq 0$

C: $x^4 + x^3 + x - 1$ over $\mathbb{F}_3$ not irred: $(x^2+1)(x^2+x-1) = x^4 + x^2 + x^3 + x - x^2 - 1$

D: $15x^4 + 8x^3 - 6x^2 + 2x - 6$ over $\mathbb{Q}$ by Eisenstein $\Rightarrow$ irred.

2 ✗ 2 ✓ 2 ✓ 2 ✓ 2 ✓, 4 ✗

E: $5x^3 + 2x + 1$ over $\mathbb{Q}$

deg = 3, $\frac{r}{s}$, $s \mid 5$ and $r \mid 1$ $\Rightarrow \frac{r}{s} \in \{\pm 1, \pm \frac{1}{5}\}$

$\Rightarrow$ no roots

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

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

unique field of p elts

unique field of p^n elts

ring with zero divisors:
$[p^s]\cdot[p^t] = [0]$
$s+t=n$

The end :)