Algebra III Lecture 04.05.2026

Last time:

Prop 4.4.10 Let $K \subset L$ be a field extension, $\alpha \in L$, $f \in K[x]$. TFAE:

(1) α is a multiple root of f

(2) $f(\alpha) = 0$ and $\frac{\partial}{\partial x} f(\alpha) = 0$

(3) $(x-\alpha) \mid \gcd\left(f, \frac{\partial}{\partial x} f\right)$.

Example $x^5 - 1$ over $\mathbb{C}$ then $\frac{\partial}{\partial x}(x^5 - 1) = 5x^4$

$\gcd(x^5 - 1, x^4) = 1 \Rightarrow$ No multiple roots in $\mathbb{C}$

Corollary 4.4.12 If $f \in K[x]$ is irreducible then

f has a multiple root in some field extension $L \supset K$ $\iff$ $\frac{\partial}{\partial x} f = 0$

Pf. "$\Leftarrow$" Let $g = \gcd(f, \frac{\partial}{\partial x} f)$ if $\frac{\partial}{\partial x} f \neq 0$

then $\gcd(f, \frac{\partial}{\partial x} f) = g \Rightarrow \exists$ a multi. root in the splitting field.

"$\Rightarrow$" f is irreducible $\Rightarrow$

either $\gcd(f, \partial_x f) = 1$

or: $\gcd(f, \partial_x f) \sim f$

If we assume that f has a multiple root

we get that $\gcd(f, \partial_x f) \sim f$

in particular $\deg \gcd(f, \partial_x f) = \deg f$.

But since $\deg(\partial_x f) \leq \deg(f) - 1$

$\Rightarrow \partial_x f = 0$ ∎

Example $f(x) = x^2 + x + 1$ over $\mathbb{F}_2$

↖ irreducible since $f(x) \neq 0$ $\forall\, x \in \mathbb{F}_2$

$\frac{\partial}{\partial x} f = 1 \neq 0 \Rightarrow$

f does not have multiple roots in any field extension.

Today:

- Fundamental thm of finite fields
  - ↳ classification of f. fields
- Simple / Separable extensions:

  Primitive element thm.

  finite Separable ⇒ simple
- (Galois theory)

4.4.3 Fundamental theorem for finite fields

Recall Exponent of finite abelian group!

Def. G - finite ab. group then $\exp(G)$ is the smallest $m \in \mathbb{N}$ s.t. $g^m = e \ \forall g \in G$

Prop G - finite ab of order n then $\exp(G) \mid n$ with the equality for cyclic groups

Proof We can write $G \cong \prod_{i=1}^{s} \mathbb{Z}/n_i\mathbb{Z}$

So prop. is a direct calculation.

Theorem 4.4.17 Fundamental theorem of finite fields

- **Restriction of the order:**

(1) If L is a finite field then

$$|L| = p^n \quad \text{with } p \text{ prime}, n \geq 1$$

Usually we denote p^n by q.

Uniqueness and properties: (Fix $q = p^n$)

(2) A field with q-elements is unique up to isomorphism

(denote it by $\mathbb{F}_q$)

(3) $\mathbb{F}_q$ is the splitting field of $x^q - x \in \mathbb{F}_p[x]$

(4) Every element of $\mathbb{F}_q$ is a root of $x^q - x$

(5) The extension $\mathbb{F}_p \subset \mathbb{F}_q$ is simple

(6) For any irred. poly $f \in \mathbb{F}_p[x]$ of deg n

$\mathbb{F}_q \simeq \mathbb{F}_p[x]/(f)$

(7) multiplicative group $\mathbb{F}_q^*$ is isomorphic to $\mathbb{Z}/(q-1)\mathbb{Z}$

Proof (1) If F is finite $\Rightarrow$

$\Rightarrow$ $\mathrm{char}(F) = p > 0$ $\Rightarrow$

$$\begin{array}{ccc} \mathbb{F}_p & \hookrightarrow & F \\ \downarrow & & \\ r + p\mathbb{Z} & \longmapsto & \underbrace{1 + \cdots + 1}_{r\text{-times}} \end{array}$$

So F is an extension of $\mathbb{F}_p$

$\Rightarrow$ F is $\mathbb{F}_p$-vector space if $\dim_{\mathbb{F}_p} F = n$

$\Rightarrow$ $|F| = p^n$

Now we fix $q = p^n$

- First Assume $|F| = q \Rightarrow$

$\Rightarrow |F^\times| = q-1 \Rightarrow \forall \alpha \in F^\times$ we have

$|F^\times|$ = F wo 0

$\alpha^{q-1} = 1 \Rightarrow$

$\Rightarrow \forall \alpha \in F$ we have

$\alpha^q - \alpha = 0 \Rightarrow$

$\Rightarrow$ Every element of F is a root of $x^q - x$.

Let L denote the splitting field of $x^q - x$ over $\mathbb{F}_p$ then

If field with q elements exists then it is equal to L.

It is enough to show that

- Every element of L is a root of $x^q - x$
- $|L| = q$

For the first: Let $E \subset L$ be set of roots of $x^q - x$

$\Rightarrow L = \mathbb{F}_p(E)$ so it is enough to show that E is a field so $\mathbb{F}_p(E) = E$.

$0 \in E$ since $0^q + 0 = 0$

$\alpha, \beta \in E \Rightarrow \alpha + \beta \in E : (\alpha+\beta)^q = \alpha^q + \beta^q = \alpha + \beta$

$\alpha \in E \Rightarrow -\alpha \in E : (-\alpha)^q = (-1)^q \cdot \alpha^q = -\alpha$

if q is odd $(-1)^q = -1$

if $q = 2^n$ so $\operatorname{char} L = 2 \Rightarrow 1 = -1$

$\vdots$

For the second:

$$\frac{\partial}{\partial x}\left(x^q - x\right) = -1 \qquad \gcd\left(x^q - x, \frac{\partial}{\partial x}(x^q - x)\right)$$

$$= \underline{1}$$

$\Rightarrow$ No multiple roots in the splitting field

$\Rightarrow$ $|L| = \deg(x^q - x) = q$.

So we proved so far:

Splitting field of $x^q - x$ has exactly q - elements and any other field with q - elements is isomorphic to it.

We left with properties (5) and (7)

Now let us denote by $\mathbb{F}_q$ the unique field with q - elements

For #1)

$\mathbb{F}_q^\times$ finite ab. group let $r = \exp(\mathbb{F}_q^\times)$

$\Rightarrow$ $r \mid q-1$ also $\alpha^r = 1$ for $\alpha \in \mathbb{F}_q^\times$

So every $\alpha \in \mathbb{F}_q$ is a root of

$x^{r+1} - x$ but since $\deg(x^{r+1} - x)$

$= r+1$

it has at most $r+1$ roots

$\Rightarrow$ $q \leq r+1$ $\Rightarrow$ $r = q-1 \Rightarrow \mathbb{F}_q^\times$ - cyclic.

(5) $\mathbb{F}_p \subset \mathbb{F}_q$ is simple ;

take any generator α of $\mathbb{F}_q^* \simeq \mathbb{Z}/(q-1)\mathbb{Z}$

then any element of $\mathbb{F}_q^*$ is

equal to α^i for some $i = 0 \dots q-1$

$\Rightarrow$ $\mathbb{F}_q = \mathbb{F}_p(\alpha)$ it is simple

extension

∎

Remark We showed that all $\alpha \in \mathbb{F}_q^*$ are $(q-1)$-st roots of unity.

Remark Even though all fields with q elements are isomorphic there is no canonical isomorphism $\mathrm{Aut}(\mathbb{F}_q)$ is a non-trivial group

Corollary 4.4.22 Let $\mathbb{F}_{p^s}$ and $\mathbb{F}_{p^r}$ be finite fields then we have an extension $\mathbb{F}_{p^s} \subset \mathbb{F}_{p^r}$ iff $s|r$. Moreover in this case there is unique subfield of $\mathbb{F}_{p^r}$ isomorphic to $\mathbb{F}_{p^s}$.

4.5 Simple and Separable extensions

Def 4.5.2 (1) K - field $f \in K[x]$ is called separable if it has $\deg(f)$ distinct roots in the splitting field.

(2) $K \subset L$ - field extension and $\alpha \in L$ is algebraic $/K$ then α is called separable if $m_{\alpha,K}$ is separable.

(3) $K \subset L$ - algebraic extension called Separable if $\forall x \in L$ is separable

(4) K is called perfect field if all Algebraic extensions are Separable.

(5) K is in perfect if it is not perfect.

Lemma 4.5.3 TFAE:

(1) K is perfect

(2) $\forall$ finite deg extension $K \subseteq L$ is separable

(3) $\forall$ simple alg. extension is separable

(4) Every irreducible polynomial is separable

Proof (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4) $\Rightarrow$ (1)

bijection irr $f \longrightarrow K[x]/(f)$? $x \mapsto (f)$

Lemma 4.5.4 $f \in K[x]$ TFAE:

(1) f is separable

(2) f has $\deg(f)$ distinct roots in some extension of K

(3) f has no mult. roots in the splitting field

(4) $\forall$ alg. extension $K \subset L$ f has no mult. roots

Example Every finite field is perfect

$K = \mathbb{F}_q$ for $q = p^n$

Let $K \subset L = K(\alpha)$ be a simple extension

Let $L \subset E$ splitting field of $m_{\alpha,K}$

We know $\alpha^{p^r} - \alpha = 0$ for some r $|L| < \infty$

$\Rightarrow m_{\alpha,K} \mid \alpha^{p^r} - \alpha$ is separable since no mult. roots

$\Rightarrow m_{\alpha,K}$ has no mult. roots $\Rightarrow$ sep. ∎

Characterisation of perfect fields

Recall Let $\mathrm{char}(F) = p > 0$ then

$$F^p = \{\alpha^p \mid \alpha \in F\}$$ is a subfield of F

Proof F^p is closed under arithmetic operations!

$$\alpha^p + \beta^p = (\alpha + \beta)^p$$

$\vdots$

$\blacksquare$

Prop 4.5.7 Let K be a field TFAE:

(1) K is perfect

(2) for every irred. f

$$\partial/\partial x\, f \neq 0$$

(3) Either $\operatorname{char}(K) = 0$

or $\operatorname{char}(K) = p > 0$ and

$$K^p = K.$$

Proof: (2) $\Rightarrow$ (1) If f is irreducible then f has mult. roots $\Leftrightarrow \frac{\partial}{\partial x} f = 0$

$\Rightarrow$ If for any irreducible f

$$\frac{\partial}{\partial x} f \neq 0 \Rightarrow f \text{ is sep.}$$

$\Rightarrow k$ is perfect.

(1) $\Rightarrow$ (2) Assume counter positive

let f irreducible s.t $\frac{\partial}{\partial x} f = 0$

Then consider $L = K[x]/(f)$

then $\alpha = x + (f) \in L$ is a root

of f.

But since $\frac{\partial}{\partial x} f = 0$ α is a root

of $\frac{\partial}{\partial x} f \Rightarrow$ it is a multiple

root of $f \Rightarrow L > k$ is

not separable. Contradiction ∎

To show equivalence with (3)

First notice in Char = 0

$\frac{\partial}{\partial x} f \neq 0$ for any irr f.

So any char 0 field is perfect.

Assume char $K = p > 0$.

(1) $\Rightarrow$ (3) Assume $K^p \neq K$.

Let $\alpha \in K \setminus K^p$

Denote by L the splitting field of $x^p - \alpha$

$L \setminus K \neq \emptyset$ so there exists

a root $\beta \in L \setminus K$ of $x^p - \alpha$

$\Rightarrow m_{\beta,K} \mid x^p - \alpha$ $\Rightarrow$ so $m_{\beta,K}$

"$(x-\beta)^p = x^p - \beta^p$" is not separable.

Contradiction

(3) $\Rightarrow$ (2) Assume $K = K^p$ and f

is s.t. $\frac{\partial}{\partial x} f = 0 \Rightarrow$

$$\Rightarrow f(x) = \sum_{i=1}^{n} a_i x^{i \cdot p} \quad \text{but } K^p = K$$

$$\Rightarrow \exists\ b_i \in K \text{ s.t. } b_i^p = a_i \text{ for any } i$$

$$\Rightarrow f(x) = \left(\sum_{i=1}^{n} b_i x^i \right)^p \quad \text{so } f(x)$$

is not irreducible

∎

Example For any F with

$$\operatorname{char}(F) = p > 0$$

the $F(t)$ is not perfect:

$$F(t)^p = F(t^p) \subsetneq F(t).$$

Theorem 4.5.9. (Primitive element thm)

Every finite separable extension is simple.

Example By fundamental theorem of finite fields every finite extension of finite field is separable and simple.