3rd Presentation

Leandro Jorge Fernández Vega

22.3 Primitive Elements:

22.3.1 Proposition: Let K be a finite field extension of k. Then $\exists_1\, \alpha \in K / K = k(\alpha) \iff \exists$ only finitely many fields between K and k

Def: A single element $\alpha \in K / K = k(\alpha)$ is a primitive element for K over k.

22.3.3 Corollary: Let K be a finite separable extension of k. Then, there are finitely-many fields between K and k, and K can be generated by a single element over k.

22.4 Normal Field Extensions:

Def: A finite extension K over k is normal $\iff$ All k-algebra homomorphisms $\sigma : K \longrightarrow \bar{k}$ have the same image.

22.4.2 Example: To illustrate that normal extensions are arguably atypical, note that the field extension $\mathbb{Q}(\sqrt[3]{2})$ of $\mathbb{Q}$ is *not* normal

Let $\sigma_i : \mathbb{Q}(\sqrt[3]{2}) \longrightarrow \bar{\mathbb{Q}} \subseteq \mathbb{C}$ be a $\mathbb{Q}$-algebra homomorph.

We can see $\sqrt[3]{2} = \{\sqrt[3]{2} \cdot e^{\frac{2k\pi}{3}} / k = 0..2\} = \{\sqrt[3]{2}, \sqrt[3]{2}\, e^{\frac{2\pi}{3}i}, \sqrt[3]{2}\, e^{\frac{4\pi}{3}i}\}$

Then, $\exists$ 3 $\mathbb{Q}$-algebra hom. / $\sigma_1(\sqrt[3]{2}) = \sqrt[3]{2}$, $\sigma_2(\sqrt[3]{2}) = \sqrt[3]{2}\, e^{\frac{2\pi}{3}i}$, $\sigma_3(\sqrt[3]{2}) = \sqrt[3]{2}\, e^{\frac{4\pi}{3}i}$

$\Rightarrow \mathbb{Q}(\sqrt[3]{2})$ isn't normal over $\mathbb{Q}$.

22.4.3 Example: All cyclotomic extensions of $\mathbb{Q}$ are normal.

Let ζ be a primitive n^{th} root of unity, $n \in \mathbb{N}$. We know every primitive n^{th} root of unity is of the form ζ^k, $\gcd(n,k)=1$.

Let $\sigma: \mathbb{Q}(\zeta) \to \overline{\mathbb{Q}}$ be a $\mathbb{Q}$-algebra homomorph. / $\sigma(\zeta) = \zeta^k$

Let $B = \{\zeta^k / \mathrm{mcd}(n,k)=1\}$ be a base of $\mathbb{Q}(\zeta)$. Let's see $\sigma(B) = B$

- $\sigma(B) \subseteq B$ trivial

We know $B \cong \sigma(B) \subseteq B$, as $\mathbb{Q}$-algebra homomorph. are also ring homomorph.

$\Rightarrow$ necessarily σ is injective and $\sigma(B) = B$

$\Rightarrow$ $\mathbb{Q}(\zeta)$ is a normal extension over $\mathbb{Q}$.

22.4.5 Proposition: Let $f(x)$ be minimal polynomial of a generator α of a finite field extension $k \subseteq k(\alpha)$. Then $k \subseteq k(\alpha)$ normal $\iff$ every root of $f(x)$ lies in $k(\alpha)$ $\iff$ $f(x)$ factors into lineal factors in $k(\alpha)[x]$

22.4.6 Proposition: If $k \subseteq L$ is a finite normal extension and $k \subseteq K \subseteq L \Rightarrow K \subseteq L$ normal.

22.4.7 Remark: $k \subseteq K$ isn't necessarily normal.

22.4.8 Proposition: A finite extension $k \subseteq K$ is normal $\iff$ [$\forall f \in k[x]$ irreducible polynomial, f has one linear factor in $K[x] \Rightarrow$ it factors completely into linear factors in $K[x]$].

22.4.9 Proposition: Let $f \in k[x]$, $\overline{k}$ the algebraic closure of k. Then, $K = k(\text{all roots of } f \text{ in } \overline{k})$ is normal over k.

22.4.10 Proposition: Let $k \subseteq K$ be a normal extension, f irreducible in $k[x]$, $\alpha, \beta \in K$ roots of f. Then, $\exists \sigma: K \to K$ k-algebra automorphism / $\sigma(\alpha) = \beta$

22.4.11 Remark: If $k \subseteq K$, $K \subseteq L$ normal, it doesn't necessarily mean $k \subseteq L$ normal.

22.6 Conjugate, Trace, Norm:

Let $k \subseteq K$ be a Galois extension with Galois Group G, $\alpha \in K$.

Def: The Galois conjugates of α over k are the images $\sigma(\alpha)$, $\sigma \in G$

Def: The Galois Trace from K to k is the map $\mathrm{trace}_{K/k}(\alpha) = \mathrm{tr}_{K/k}(\alpha) = \sum_{\sigma \in G} \sigma(\alpha)$

Def: The Galois Norm from K to k is the map $\mathrm{norm}_{K/k}(\alpha) = N_{K/k}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha)$

Proposition: When K is the splitting field over k of the minimal polynomial $f \in k[x]$, with α separable, algebraic over k. Then:

$$f(x) = \prod_{\sigma \in G} (x - \sigma\alpha) = x^n - \underset{\in k}{\mathrm{tr}_{K/k}(\alpha)}\, x^{n-1} + \dots + (-1)^n \underset{\in k}{N_{K/k}(\alpha)}, \quad n = [K:k]$$

Additional Exercises

4.8 Let R be a commutative ring with unit. Suppose R contains an *idempotent* element r other than 0 or 1. (That is, $r^2 = r$.) Show that every prime ideal in R contains an idempotent other than 0 or 1.

Let I be a prime ideal in $R \Rightarrow 0 \in I$, $r - r^2 = r - r = 0 \in I$

$r - r^2 = r(1-r) = 0 \Rightarrow r \in I \vee 1-r \in I$. Let's see $1-r$ is idempotent.

$(1-r)^2 = 1 + r^2 - 2r = 1 + r - 2r = 1 - r$

- $1 - r = 0 \Rightarrow r = 1$!!!
- $1 - r = 1 \Rightarrow r = 0$!!!

As a conclusion, I contains r or $1-r$, which are idempotent and $\neq 0, 1$

6.3 Find a polynomial with rational coefficients having a root $\sqrt{2} + \sqrt{3}$.

First we'll find a polynomial with root $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$

$x - (\sqrt{2} + \sqrt{3}) = 0 \Leftrightarrow (x - \sqrt{2})^2 = (\sqrt{3})^2 \Leftrightarrow x^2 - 2\sqrt{2}x - 1 = 0$

$(x^2 - 1)^2 = (2\sqrt{2}x)^2 \Leftrightarrow x^4 - 10x^2 + 1 = 0$, which is the polynomial we were looking for.

6.5 Let γ be a root of $x^5 - x + 1 = 0$ in an algebraic closure of $\mathbb{Q}$. Find a polynomial with rational coefficients of which $\gamma + \sqrt{2}$ is a root.

Let $\alpha = \gamma + \sqrt{2} \Rightarrow \gamma = \alpha - \sqrt{2} \Rightarrow (\alpha - \sqrt{2})^5 - (\alpha - \sqrt{2}) + 1 = 0 \Leftrightarrow$

$\alpha^5 - 5\sqrt{2}\alpha^4 + 20\alpha^3 - 20\sqrt{2}\alpha^2 + 20\alpha - 4\sqrt{2} - \alpha + \sqrt{2} + 1 = 0 \Leftrightarrow$

$[\alpha^5 + 20\alpha^3 + 19\alpha + 1]^2 = [\sqrt{2}(5\alpha^4 + 20\alpha^2 + 3)]^2 \Leftrightarrow$

$\alpha^{10} + 40\alpha^8 + 438\alpha^6 + 2\alpha^5 + 760\alpha^4 + 40\alpha^3 + 361\alpha^2 + 38\alpha + 1 = 50\alpha^8 + 400\alpha^6 + 860\alpha^4 + 240\alpha^2 + 18$

$\Leftrightarrow \alpha^{10} - 10\alpha^8 + 38\alpha^6 + 2\alpha^5 - 100\alpha^4 + 40\alpha^3 + 121\alpha^2 + 38\alpha - 17 = 0$

which is the polynomial we were looking for.

7.5 Show that the ideal generated by $x^2 - x + 1$ and 13 in $\mathbb{Z}[x]$ is *not* maximal.

Let $I = \langle 13, x^2 - x + 1 \rangle$ be an ideal. We consider the quotient $\mathbb{Z}[x]/I$

We know $\mathbb{Z}[x]/\langle 13 \rangle \cong \mathbb{Z}_{13}[x]$, where $x^2 - x + 1 = x^2 + 12x + 1 = (x+3)(x+9)$

therefore, the quotient $\mathbb{Z}_{13}[x]/\langle x^2 - x + 1 \rangle$ has proper zero divisors $\bar{x}+3$, $\bar{x}+9$, where $\bar{x}$ is the image of x in the quotient $\Rightarrow$ $\mathbb{Z}[x]/I$ isn't an Integral Domain $\Rightarrow$ it isn't a field $\Rightarrow$ I isn't a maximal ideal, as we know that if R is a commutative ring with 1, I an ideal, R/I is field $\Leftrightarrow$ I is maximal.

22.19 Show that the Galois trace $\sigma : \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_q$ is

$$\sigma(\alpha) \;=\; \alpha + \alpha^q + \alpha^{q^2} + \ldots + \alpha^{q^{n-1}}$$

To prove this we are going to make use of some theorems:

Theorem: Let $\mathbb{F}_q \leq \mathbb{F}_{q^n}$ be a finite group extension. Then, $Aut_{\mathbb{F}_q}(\mathbb{F}_{q^n})$ is cyclic of order n with generator ϕ, defined as $\phi(\alpha) = \alpha^q$. Besides, $\mathbb{F}_{q^n}$ is the spliting field of $f(x) = x^{q^n} - x$.

Theorem: Let $f \in \mathbb{F}_q[x]$ irreducible of degree n. Then, its splitting field is $\mathbb{F}_{q^n}$. Besides, if $\alpha \in \mathbb{F}_{q^n}$ is a root of f, the rest of its roots are $\alpha^q \ldots \alpha^{q^{n-1}}$.

We can now easily affirm $\mathbb{F}_q \leq \mathbb{F}_{q^n}$ is finite, normal and separable $\Longrightarrow$ $\mathbb{F}_q \leq \mathbb{F}_{q^n}$ is a Galois Extension with Galois Group $G = Aut_{\mathbb{F}_q}(\mathbb{F}_{q^n})$.

As G is cyclic of order n, we consider all powers of the generator ϕ, for composition:

$$\phi^i(\alpha) = \underbrace{\phi(\ldots\phi}_{i}(\alpha)\ldots) = \alpha^{q^i} \qquad i = 0 \ldots n-1$$

$$\text{Finally,} \quad tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = \sigma(\alpha) = \sum_{\phi \in G} \phi(\alpha) = \sum_{i=0}^{n} \alpha^{q^i}$$

22.20 Show that the Galois norm $\nu : \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_q$ is

$$\nu(\alpha) \;=\; \alpha^{\frac{q^n-1}{q-1}}$$

Based on the previous exercise, we can easily compute:

$$N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = \nu(\alpha) = \prod_{\sigma \in G} \sigma(\alpha) = \prod_{i=0}^{n-1} \alpha^i = \alpha^{\sum_{i=0}^{n-1} q^i} \underset{\text{Geometric series}}{=} \alpha^{\frac{q^n-1}{q-1}}$$