Algebraic Equations

Martin Azpillaga

December 23, 2013

Contents

Part I

Definitions

Chapter 1.

Roots of unity, Extensions and Galois Group

In this first chapter, we discuss the definitions involved in the subsequent three sections:

1. Roots of the unity who form cyclotomic polynomials and cyclotomic fields.

2. Algebraic and Transcendent extensions over fields. Normal extensions.

3. Galois Group of an algebraic extension.

Section 1.1

Roots of unity

nth root of unity

Let:

- K field
- $n \in \mathbb{N}$
- $x \in \mathbb{K}$

Then, x is a nth root of unity in K if:

- $x^n = 1$

We denote:

- $\{x \in \mathbb{K} \mid x^n = 1\} \,:\, \mu_n(\mathbb{K})$
- $\{x \in \mathbb{K} \mid \exists\, n \in \mathbb{N} \;\shortparallel\; x^n = 1\} \,:\, \mu(K)$

nth Primitive root of unity

Let:

- K field
- $x \in \mu_n(K)$

Then, x is a primitive root of unity in K if:

- $o(x) = n$

We denote:

- $\{x \in \mu_n(\mathbb{K}) \mid o(x) = n\} \,:\, \mu_n^*(K)$

nth Cyclotomic Polynomial

Let:

- $n \in \mathbb{N}$

We call nth Cyclotomic Polynomial to:

$$f(X) = \prod_{\zeta \in \mu_n^*(\mathbb{K})} (X - \zeta) \in \mathbb{C}[X]$$

We denote:

- $f(X) \,:\, \Phi_n(X)$

Mobius' function

We call Mobius' function to:

$$\begin{aligned} f \,:\mathbb{N} &\longrightarrow \{0, +1, -1\} \\ x &\longmapsto \begin{cases} +1, & n = 1 \\ +0, & \exists\, p \in \mathbb{N} \;\text{" } p \text{ prime } \wedge a^2 | n \\ -1, & * \end{cases} \end{aligned}$$

We denote:

- $f \,:\, \mu$

Section 1.2

Classification of Field Extensions

Field Extension

Let:

- K, k fields

Then, K is an extension of k if:

- $k \subset K$

We denote:

- $k \subset K \;:\; K|k$

Algebraic extension

Let:

- $K|k$ field extension

Then, $\theta \in K$ is an algebraic element over k if:

- $\exists\, f \;_{''}\, (X) \in k[X] \;_{''}\, f(\theta) = 0$

Then, $K|k$ is an algebraic extension if:

- $\forall\, \theta \in K$:

  θ algebraic over k

We denote:

- $K|k$ no algebraic extension : $K|k$ transcendent extension

Cyclotomic Extension

Let:

- $n \in \mathbb{N}$
- $\zeta \in \mu_n^*(\mathbb{C})$

We call nth cyclotomic field to:

$$Q(\zeta) \mid \mathbb{Q}$$

Quadratic extension

Let:

- k field „ $car(k) \neq 2$
- $K|k$ field extension

Then, $K|k$ is a quadratic extension if:

- $[K:k] = 2$

Normal Extension

Let:

- $K|k$ algebraic extension

Then, $K|k$ is a normal extension over k if:

- $\exists\ f(X) \in k(X)$ irreductible „ $f(X)$ splits in K

Separable extension

Let:

- $K|k$ algebraic extension

Then, $\theta \in K$ is a separable element over k if:

- $\exists\ f(X) \in k[X]$,, $f(\theta) = 0\ \wedge\ f(X)$ separable in $K[X]$

Then, $K|k$ is a separable extension if:

- $\forall\ \theta \in K$:

  θ separable over k

Simple extension

Let:

- $K \mid k$ field extension
-

Then, $K \mid k$ is a simple extension if:

- $\exists\ \theta \in K$,, $K = k(\theta)$

We denote:

- θ : primitive element of $K \mid k$

Galois extension

Let:

- $K \mid k$ algebraic extension

Then, $K \mid k$ is a Galois extension if:

- $K \mid k$ normal extension
- $K \mid k$ separable extension

Section 1.3

Properties of field extensions

Evaluation function

Let:

- $K|k$ field extension
- $\theta \in K$

We call Evaluation function of θ over k to:

$$\begin{array}{rcl} f\ : k[X] & \longrightarrow & K \\ p(X) & \longmapsto & p(\theta) \end{array}$$

We denote:

- $f\ :\ \Psi_\theta$
- $Im\, \psi_\theta\ :\ k[\theta]$
- fraction field of $k[\theta]\ :\ k(\theta)$

Minimal Polynomial

Let:

- $K|k$ field extension
- $\theta \in K$ algebraic over k

We call Minimal Polynomial of θ in $K|k$ to:

$$f(X) \in k[X] \;\; " \;\; \wedge \begin{cases} f(X) \neq 0 \\ f(X) \text{ irreducible} \\ f(\theta) = 0 \end{cases}$$

We denote:

- $f(X) \; : \; Irr(\theta, k)(X)$

Extension Degree

Let:

- $K|k$ field extension

We call degree of $K|k$ to:

$$\dim_k K \in \mathbb{N} \cup \{\infty\}$$

We denote:

- $\dim_k K \; : \; [K : k]$
- $[K : k] \in \mathbb{N} : K|k$ finite extension

Splitting field

Let:

- k field
- $f \in k[X]$
- $\{\theta_i\}_{i=1}^n$ roots of f

We call splitting field of f to:

$$k(\theta_i)_{i=1}^n$$

Field Composition

Let:

- $K_1|k, K_2|k$ field extensions

We call the composition of K_1 and K_2 to:

$$< K_1, K_2 >$$

We denote:

- $< K_1, K_2 >:\ K_1K_2$

Separability degree

Let:

- $k|k$ algebraic extension
- $\overline{k}$ algebraic closure of k

We call separability degree of $K|k$ to:

$$\#\{\sigma \in \mathcal{F}(K, \overline{k}) \mid \sigma \text{ } k\text{-immersion}\}$$

We denote:

- $\#\{\sigma \in \mathcal{F}(K, \overline{k}) \mid \sigma \text{ } k\text{-immersion}\} \ : \ [K : k]_s$

Section 1.4

Galois Group

Fixed Field

Let:

- K_1, K_2 fields
- $\sigma \ : \ K_1 \to K_2$

We call the fixed field of k_1 by σ to:

$$\{x \in K_1 \mid \sigma(x) = x\}$$

We denote:

- $\{x \in K_1 \mid \sigma(x) = x\} \ : \ K_1^\sigma$

k-Immersion

Let:

- $K_1|k, K_2|k$ field extensions

- $\sigma : K_1 \to K_2$

Then, σ is a k-immersion if:

- $k \subset K_1^\sigma$

We denote:

- σ k-immersion $\wedge$ σ automorphism : σ k-automorphism

k-Automorphism

Let:

- $K \mid k$ field extensions

- $\sigma : K \to K$

Then, σ is a k-automorphism if:

- σ k-immersion

- σ isomorphism

We denote:

- σ k-immersion $\wedge$ σ automorphism : σ k-automorphism

Galois Group

Let:

- $K|k$ field extension

We call Galois group of $K|k$ to:

$$\{\sigma \in \mathcal{F}(K,K) \mid \sigma \ k\text{-autmorphism } \}$$

We denote:

- $\{\sigma \in \mathcal{F}(K,K) \mid \sigma \ k \text{ autmorphism } \} \ : \ Gal(K|k)$

Section 1.5

Finite Fields

Finite Field

Let:

- k field

Then, k is a finite field if:

- $\#k \in \mathbb{N}$

We denote:

- $\exists\, p, n \in \mathbb{N} \;\shortparallel\; p$ prime $\wedge \#k = p^n \;:\; \mathbb{F}_{p^n}$

Frobenius' Automorphism

Let:

- $\mathbb{F}_{p^n}$ finite field

We call Frobenius' automorphism of $\mathbb{F}_{p^n}$ to:

$$\begin{aligned} f : \mathbb{F}_{p^n} &\longrightarrow \mathbb{F}_{p^n} \\ x &\longmapsto x^p \end{aligned}$$

We denote:

- $f \;:\; \varphi_p$

Section 1.6

Separability

Section 1.7

Norm and trace

Norm

Let:

- $K|k$ finite extension

We call Norm of $K|k$ to:

$$\begin{array}{rcl} f : K & \longrightarrow & k \\ \theta & \longmapsto & det(m_\theta) \end{array}$$

We denote:

- $f \ : \ N_{K|k}$

Trace

Let:

- $K|k$ finite extension

We call trace of $K|k$ to:

$$\begin{array}{rcl} f : K & \longrightarrow & k \\ \theta & \longmapsto & tr(m_\theta) \end{array}$$

We denote:

- $f \ : \ Tr_{K|k}$

Cyclic extension

Let:

· $K|k$ Galois extension

Then, $K|k$ is a cyclic extension if:

· $Gal(K|k)$ cyclic

Abelian extension

Let:

· $K|k$ Galois extension

Then, $K|k$ is an abelian extension if:

· $Gal(K|k)$ abelian

Resoluble by radicals

Let:

· k field

· $f(X) \in k[X]$

Then, $f(X)$ is resoluble by radicals if:

· $\exists\ K|k$ „ $K|k$radical extension

We denote:

· *property* : *notation*

·

Part II

Propositions

Chapter 2.

Roots of unity, Field extensions and Galois Group

Basic propositions over:

1. Roots of unity.
2. Field extensions.
3. Galois Group

Section 2.1

Roots of unity

The Group of Roots of Unity

Let:

- K field

Then, holds:

- $\mu(K) < K^*$

Demonstration:

$$\forall\ x, y \in \mu(K) :$$

$$1$$

$$\mu(K) < K^*$$

The group of nth roots

Let:

- K field
- $n \in N$

Then, holds:

- $\mu_m(K) \triangleleft K^*$

Demonstration:

Follow 3 steps

Step 1: $\mu_n(K) \subset K^*$:

$$\mu_n(K) \subset \mu(K) \subset K^*$$

Step 2: Define a group morphism :

$$\begin{aligned} \phi_n : K^* &\longrightarrow K^* \\ x &\longmapsto x^n \end{aligned}$$

$\forall\ x, y \in K^*$:

$$\phi_n(x)\phi_n(y) = x^n y^n = (xy)^n = \phi_n(xy)$$

Step 3: Identify $\mu_n(K)$ with the kernel :

$$Ker\phi_n = \mu_n(K)$$

Finite subgroups of the multiplicative group

Let:

- $\cdot$ K field
- $\cdot$ $G < K^*$ finite

Then, holds:

- $\circ$ $\exists\, m \in \mathbb{N}$ „ $G = \mu_m(K)$
- $\circ$ G cyclic

Demonstration:

Follow 2 steps

Step 1: Find m :

$$m := \max\{o(x) \mid x \in G\} \in \mathbb{N}$$

$$\forall\, x \in G :$$

$$o(x) \mid m \to x^m = 1$$

$$x \in \mu(K)$$

$$G = \mu_m(K)$$

Step 2: G cyclic :

$$\exists\, \zeta \in G \text{ „ } o(\zeta) = m$$

$$<\zeta> \subset G = \mu_m(K)$$

$$\left.\begin{cases} \# G \geq o(\zeta) = m \\ \# G \leq \# \mu_m(K) \leq m \end{cases}\right\} \to \# G = m$$

$$G = <\zeta> \to G \text{ cyclic}$$

Characterization of nth roots by cyclotomic polynomials

Let:

- $n \in \mathbb{N}$

Then, holds:

- $X^n - 1 = \prod_{d|n} \Phi_d(X)$

Demonstration:

$f(X) := X^n - 1 \in \mathbb{C}[X]$

$g(X) := \prod_{d|n} \Phi_d(X) \in \mathbb{C}[X]$

Follow 3 steps

Step 1: $f(X)$ and $g(X)$ have the same roots :

$\forall\ x \in \mathbb{C}$ 〃 $f(x) = 0$:

$x \in \mu_n(\mathbb{C})$

$d := o(x) \in \mathbb{N}$

$x \in \mu_d^*(\mathbb{C}) \rightarrow \Phi_d(x) = 0 \rightarrow g(x) = 0$

$\forall\ y \in \mathbb{C}$ 〃 $g(y) = 0$:

$\exists\ d \in \mathbb{N}$ 〃 $d|n \ \wedge\ \Phi_d(y) = 0$

$y \in \mu_d^*(\mathbb{C}) \rightarrow y^d = 1 \rightarrow y^n = 1 \rightarrow f(y) = 06$

Step 2: $f(X)$ and $g(X)$ are monic :

f monic

$\forall\ d \in \mathbb{N}$ „ $d \mid n$:

$\Phi_d(X)$ monic

$g(X)$ monic

Step 3: $f(X)$ and $g(X)$ are separable :

$D(f(X)) = nX^{n-1}$

$mcd\{X^n - 1, nX^{n-1}\} = 1$

$f(X)$ separable

$\forall\ x \in \mathbb{C}$ „ $x \in \mu_d^*(\mathbb{C})$:

$\forall\ d' \in \mathbb{N}$ „ $d \mid n \ \wedge\ d' \neq d$:

$x \notin \mu_{d'}^*(\mathbb{C})$

$g(X)$ separable

$f(X) = g(X)$

Mobius' lemma

Let:

- $n \in \mathbb{N}$

Then, holds:

- $\sum_{d|n} \mu(d) = 0$

Demonstration:

$\exists \ \{p_i\}_{i=1}^{r}, \{a_i\}_{i=1}^{r} \subset \mathbb{N}$ „ $\prod_{i=1}^{r} p_i^{a_i}$ prime factorization of n

$\forall \ d \in \mathbb{N}$ „ $d \mid n$:

$\exists \ \{b_i\}_{i=1}^{r} \subset \mathbb{N}$ „ $\forall \ i \in [1, r]_{\mathbb{N}}$:

$b_i \leq a_i$

$\prod_{i=1}^{r} p_i^{b_i}$ prime factorization of n

$\mu(d) \neq 0 \leftrightarrow \forall \ i \in [1, r]_{\mathbb{N}}$:

$b_i \in \{0, 1\}$

$\sum_{d|n} \mu(d) = \sum_{k=0}^{r} \binom{r}{k}(-1)^k = \sum_{k=0}^{r} \binom{r}{k}(-1)^k 1^{r-k} = (-1 + 1)^r = 0$

Recursive formula for cyclotomic polynomials

Let:

- $n \in \mathbb{N}$

Then, holds:

- $\Phi_n(X) = \prod_{d \mid n}(X^d - 1)^{\mu(\frac{n}{d})}$

Demonstration:

$\prod_{d|n}(X^d - 1)^{\mu(\frac{n}{d})} =$

$= \prod_{d|n}(X^{\frac{n}{d}} - 1)^{\mu(d)} =$

$= \prod_{d|n} \prod_{\delta|\frac{n}{d}} \Phi_\delta(X)^{\mu(d)}$

$= \prod_{\delta|n} \prod_{d|\frac{n}{\delta}} \Phi_\delta(X)^{\mu(d)} =$

$= \prod_{\delta|n} \Phi_\delta(X)^{\sum_{d|\frac{n}{\delta}} \mu(d)}$

$\sum_{d|\frac{n}{\delta}} \mu(d) \neq 0 \leftrightarrow \delta = n$

$\prod_{\delta|n} \Phi_\delta(X)^{\sum_{d|\frac{n}{\delta}} \mu(d)} = \Phi_n(X)^1 = \Phi_n(X)$

Classification of cyclotomic polynomials

Let:

- $n \in \mathbb{N}$

Then, holds:

- $\Phi_n(X) \in \mathbb{Z}[X]$

Demonstration:

$$\Phi_n(X) = \prod_{d|n}(X^{\frac{n}{d}} - 1)^{\mu(d)}$$

$$\mu(d) = 1 \leftrightarrow d = 1 \rightarrow \Phi_n(X) = \frac{X^n - 1}{\prod_{1<d|n}(X^{\frac{n}{d}} - 1)^{\mu(d)}}$$

$$f(X) \ := \ X^n - 1$$

$$g(X) \ := \ \prod_{1<d|n}(X^{\frac{n}{d}} - 1)^{\mu(d)}$$

$$\Phi_1(X) = X - 1 \in \mathbb{Z}[X] \rightarrow \text{induction} \rightarrow g(X) \in \mathbb{Z}[X]$$

$$\left\{ \begin{array}{l} f(X), g(X) \text{ monics} \\ f(X), g(X) \in \mathbb{Z}[X] \end{array} \right\} \rightarrow \Phi_n(X) = \frac{f(X)}{g(X)} \in \mathbb{Z}[X]$$

Irreductibility of cyclotomic polynomials

Let:

- $n \in \mathbb{N}$

Then, holds:

- $\Phi_n(X)$ irreductible over $\mathbb{Q}[X]$

Demonstration:

$Idontwanttodothis$

Section 2.2

Extensionesdecuerpos

Classification of the image of the evaluation function

Let:

- $K \mid k$ field extension
- $\theta \in K$

Then, holds:

- θ algebraic over $k \to k[\theta] = k(\theta)$
- θ transcendent over $k \to k[\theta] \simeq k(\theta)$

Demonstration:

Separate 2 cases:

Case θ algebraic over k :

k field $\to k$ PID $\to k[X]$ PID

$Ker(\Phi_\theta)$ principal $\to \exists\ f(X) \in k[X]$ „ $Ker(\Phi_\theta) = (f(X))$

K field $\to K$ integral domain

$k[\theta] \subset K \to k[\theta]$ integral domain

Isomorphy theorem :$k[X]/f(X) \simeq k[\theta]$

$$\left.\begin{cases} k[X]/f(X) \simeq k[\theta] \\ k[\theta] \text{ integral domain} \end{cases}\right\} \to (f(X)) \text{ prime ideal}$$

$k[X]$ UFD $\rightarrow (f(X))$ irreductible ideal $\rightarrow (f(X))$ maximal ideal

$k[X]/(f(X))$ field $\rightarrow k[\theta]$ field

$k[\theta] = k(\theta)$

Case θ transcendent over k :

$Ker(\Psi_\theta) = (0)$

Isomorphy theorem: $k[\theta] \simeq k[X]/(0) \simeq k[X]$

Inclusion of finite extensions in algebraic extensions

Let:

- $\cdot$ $K \mid k$ finite field extension

Then, holds:

- $\circ$ $K \mid k$ algebraic extension

Demonstration:

$\forall\ \theta \in K$:

$n := dim_k K \in \mathbb{N}$

$\{\theta^i\}_{i=0}^{n}$linearly dependent

$\exists\ \{a_i\}_{i=0}^{n} \subset k$ " $\exists\ i \in [1,n]_{\mathbb{N}}$ " $\sum_{i=0}^{n} a_i\theta^i = 0$

$f(X) := \sum_{i=0}^{n} a_i\theta^i \in k[X]$

$f(X) \neq 0 \ \wedge\ f(\theta) = 0 \rightarrow \theta$ algebraic over k

$K \mid k$ algebraic extension

Degree behaviour in extension towers

Let:

- $K \mid k, L \mid K$ field extensions

Then, holds:

- $[L : k] = [L : K][K : k]$

Demonstration:

$\exists \ \{\theta_i\}_{i\in I} \subset K$ k-base of K

$\exists \ \{\theta'_j\}_{j\in J} \subset K$ K-base of L

$\forall \ \theta \in K$:

$\exists \ \{a'_k\}_{j\in J} \subset K \ \ \shortparallel \ \theta = \sum_{j\in J} a'_j \theta'_j$

$\forall \ j \in J$:

$\exists \ \{a_{i,j}\}_{i\in I} \subset k \ \ \shortparallel \ a'_j = \sum_{i\in I} a'_{i,j} \theta_i$

$\theta = \sum_{(i,j)\in(I,J)} a_{i,j} \theta_i \theta'_j$

$\{\theta_i \theta'_j\}_{(i,j)\in I\times J}$ $k-$base of L

$[L : k] = dim_k L = \#(I \times J) = \#I \cdot \#J = [K : k][L : K]$

Degree behaviour in base exchanges

Let:

- $K \mid k, L \mid k$ finite extensions

Then, holds:

- $[KL : K] \leq [L : k]$

Demonstration:

$$n := dim_k L \in \mathbb{N}$$

$$\exists \{\theta_i\}_{i=1}^n \subset L \text{ " } L = k(\theta_i)_{i=1}^n$$

$$KL = K(\theta_i)_{i=1}^n$$

$$[KL : K] = \prod_{r=1}^{n-1} [K(\theta_i)_{i=1}^{r+1} : K(\theta_i)_{i=1}^r]$$

$$[L : k] = \prod_{r=1}^{n-1} [k(\theta_i)_{i=1}^{r+1} : k(\theta_i)_{i=1}^r]$$

$\forall\ r \in [1, n-1]_{\mathbb{N}}$:

$$k \subset K \to k(\theta_i)_{i=1}^r \subset K(\theta_i)_{i=1}^r$$

$$[K(\theta_i)_{i=1}^{r+1} : K(\theta_i)_{i=1}^r] \leq [k(\theta_i)_{i=1}^{r+1} : k(\theta_i)_{i=1}^r$$

$$[KL : K] \leq [L : k]$$

Section 2.3

Classification of field extensions

Invariancy of Cyclotomic prime extensions by composition and intersection

Let:

- $n, m \in \mathbb{N}$ „ $mcd(n,m) = 1$
- $\mathbb{Q}(\zeta_n) \mid \mathbb{Q}(\zeta_m)$ cyclotomic extensions

Then, holds:

- $\mathbb{Q}(\zeta_n, \zeta_m) = \mathbb{Q}(\zeta_n \zeta_m) \mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}$

Demonstration:

Follow 2 steps

Step 1: $\mathbb{Q}(\zeta_n, \zeta_m)$ cyclotomic extension :

$\subset)$:

$o(\zeta_n \zeta_m) = o(\zeta_n) o(\zeta_m) = \varphi(n)\varphi(m)$

$mcd(m,n) = 1 \to \varphi(n)\varphi(m) = \varphi(nm) \to \zeta_n \zeta_m \in \mu_{nm}(\mathbb{C})$

$\zeta := \zeta_n \zeta_m \in \mu_{nm}(\mathbb{C})$

$(\zeta^m)^n = 1 \to \zeta^m \in \mu_n(\mathbb{C})$

$\exists\, r \in \mathbb{N}$ „ $(\zeta^m)^r = \zeta_n$

$\zeta_n \in \mathbb{Q}(\zeta)$

Similarly: $\zeta_m \in \mathbb{Q}(\zeta)$

$$\mathbb{Q}(\zeta_n, \zeta_m) \subset \mathbb{Q}(\zeta)$$

$\supset)$:

$$\zeta_n, \zeta_m \in \mathbb{Q}(\zeta_n, \zeta_m) \to \zeta_n\zeta_m \in \mathbb{Q}(\zeta_n, \zeta_m)$$

Step 2: $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}$:

$$[\mathbb{Q}(\zeta_n, \zeta_m) : \mathbb{Q}] = [\mathbb{Q}(\zeta_m, \zeta_n) : \mathbb{Q}(\zeta_n)][\mathbb{Q}(\zeta_n) : \mathbb{Q}]$$

$$\varphi(mn) = [\mathbb{Q}(\zeta_m, \zeta_n) : \mathbb{Q}(\zeta_n)]\varphi(n)$$

$$[\mathbb{Q}(\zeta_m, \zeta_n) : \mathbb{Q}(\zeta_n)] = \varphi(m)$$

$$[\mathbb{Q}(\zeta_m, \zeta_n) : \mathbb{Q}(\zeta_n)] \leq [\mathbb{Q}(\zeta_m) : \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n)] \leq [\mathbb{Q}(\zeta_m) : \mathbb{Q}]$$

$$\varphi(m) \leq [\mathbb{Q}(\zeta_m) : \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n)] \leq \varphi(m)$$

$$[\mathbb{Q}(\zeta_m) : \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n)] = \varphi(m)$$

$$[\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) : \mathbb{Q}] = \frac{\varphi(m)}{\varphi(m)} = 1$$

$$\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$$

Inclusion of Quadratic extensions in Simple extensions

Let:

- $K \mid k$ quadratic extension

Then, holds:

- $K \mid k$ simple extension

Demonstration:

$$[K:k] = 2 \rightarrow \exists\ \theta \in K \ \shortparallel\ \theta \notin k$$

$$k \subset k(\theta) \subset K$$

$$2 = [K:k] = [K:k(\theta)][k(\theta):k]$$

$$\theta \notin k \rightarrow [k(\theta):k] \geq 2$$

$$[K:k(\theta)] = 1 \rightarrow K = k(\theta)$$

$K \mid k$ simple extension

Inclusion of Quadratic extensions in Normal extensions

Let:

- $K \mid k$ quadratic extension

Then, holds:

- $K \mid k$ normal extension

Demonstration:

$K \mid k$ quadratic extension $\rightarrow K \mid k$ simple extension

$\exists\ \theta \in K \ _{''}\ \theta \notin k\ \wedge\ K = k(\theta)$

$\{1, \theta\} k$-base of K

$\{1, \theta, \theta^2\}$ linearly dependent $\rightarrow \exists\ b, c \in k\ _{''}\ \theta^2 + b\theta + c = 0$

$\eta\ :=\ 2\eta + b \in K$

$\eta^2 = 4\eta^2 + b^2 + 4b\eta = b^2 - 4c \in k$

$f(X)\ :=\ X^2 - \eta^2 \in k[X]$

$\eta, -\eta \notin k \rightarrow f(X)$ irreductible over $k[X]$

$\eta, -\eta \in K \rightarrow f(X)$ splits over $K[X]$

$k(\theta)$ splitting field of $f(X)$

$K \mid k$ normal extension

Section 2.4

Galois Group

Determination of automorphisms by minimal polynomial root images

Let:

- $K \mid k$ algebraic extension
- $f(X)$ irreductible over $k[X]$
- $\theta, \theta' \in K$ roots of $f(X)$

Then, holds:

- $\exists\,!\,\sigma \;:\; k(\theta) \to k(\theta') \;\;_{''}\; \sigma$ k-automorphism $\wedge\, \sigma(\theta) = \theta'$

Demonstration:

Follow 2 steps

Step 1: Existence of σ :

$\exists \rho : k[X]/(Irr(\theta, k)(X)) \to k(\theta)$ isomorphism

$\exists \rho' : k[X]/(Irr(\theta', k)(X)) \to k(\theta')$ isomorphism

$\sigma \;:=\; \rho' \circ \rho^{-1} \in \mathcal{F}(k(\theta), k(\theta'))$

σ isomorphism

Step 2: σ determined by θ's image :

$\forall\; \sigma' \;:\; k(\theta) \to k(\theta') \;\;_{''}\; \sigma'$ k-isomorphism $\wedge\, \sigma'(\theta) = \theta'$:

$$\forall\ x \in k(\theta)\ :$$

$$\exists\ \{a_i\}_{i=1}^{r} \subset k \ \ \text{"}\ x = \sum_{i=1}^{r} a_i \theta^i$$

$$\sigma'(x) = \sum_{i=1}^{r} \sigma'(a_i)\sigma'(\theta)^i = \sum_{i=1}^{r} a_i {\theta'}^i$$

$$\sigma(x) = \sigma'(x)$$

$$\sigma' = \sigma$$

Inclusion of immersions in automorphims

Let:

- $K \mid k$ algebraic extension
- $\sigma : K \to K k$-immersion

Then, holds:

- $\sigma \in Aut(K)$

Demonstration:

demonstration

Fundamental theorem of Galois theory

Let:

- $K \mid k$ algebraic extension
- $S(Gal(K \mid k))$ set of all subgroups of $Gal(K \mid k)$
- $C(K \mid k)$ set of all subfields between $K \mid k$

Then, holds:

- $\exists\, \phi \in \mathcal{F}(S(Gal(K \mid k), C(K \mid k)) \;_{\shortparallel}\; \phi$ biyective

Demonstration:

demonstration

Section 2.5

Finite Fields

Fermat's little theorem

Let:

- $\mathbb{F}_{p^n}$ finite field

Then, holds:

- $\forall\ x \in \mathbb{F}$,, $x \neq 0$:

$$x^{p^n - 1} = 1$$

- $\forall\ x \in \mathbb{F}$:

$$x^{p^n} = x$$

Demonstration:

Separate 2 cases:

Case $x = 0$:

$$0^{p^n} = 0$$

Case $x \neq 0$:

$$o(x) \mid \# F^* = p^n - 1$$

$$x^{p^n - 1} = 1 \rightarrow x^p = x$$

Polynomials over finite prime fields

Let:

- $\cdot$ $\mathbb{F}_p$ finite field
- $\cdot$ $f(X) \in \mathbb{F}_p[X]$

Then, holds:

- $\circ$ $f(X)^p = f(X^p)$

Demonstration:

$\forall\ i \in \{k\}_{k=1}^{p-1} \subset \mathbb{N}$:

$$p \mid \binom{p}{i} \rightarrow \binom{p}{i} \overset{p}{\equiv} 0$$

$\forall\ a, b \in \mathbb{F}_p$:

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i} \overset{p}{\equiv} a^p + b^p$$

$n \ := \ gr(f(X)) \in \mathbb{N}$

$\exists\ \{a_i\}_{i=0}^{n} \subset \mathbb{F}_p$ „ $f(X) = \sum_{i=0}^{n} a_i X^i$

$$f(X)^p = \sum_{i=0}^{n} a_i^p X^{pi}$$

Fermat's little theorem$\rightarrow f(X)^p \overset{p}{\equiv} \sum_{i=0}^{n} a_i (X^p)^i \overset{p}{\equiv} f(X^p)$

Classification of characteristic and order

Let:

- $\cdot$ $\mathbb{F}$ finite field

Then, holds:

- $\exists\, p \in \mathbb{N}$ „ p prime $\wedge\, car(\mathbb{F}) = p$
- $\exists\, r \in \mathbb{N}$ „ $\#\mathbb{F} = p^r$

Demonstration:

demonstration

Cyclotomic finite fields

Let:

- · *let*
- ·

Then, holds:

- ∘ *proposition*
- ∘

Demonstration:

demonstration

Determination of Galois group over Finite fields

Let:

- $q \in \mathbb{N}$ prime power
- $n \in \mathbb{N}$

Then, holds:

- $Gal(\mathbb{F}_{q^n} \mid \mathbb{F}_q) = < \varphi_q >$

Demonstration:

demonstration