

Part II — Galois Theory

Definitions

Based on lectures by C. Birkar

Notes taken by Dexter Chua

Michaelmas 2015

These notes are not endorsed by the lecturers, and I have modified them (often significantly) after lectures. They are nowhere near accurate representations of what was actually lectured, and in particular, all errors are almost surely mine.

Groups, Rings and Modules is essential

Field extensions, tower law, algebraic extensions; irreducible polynomials and relation with simple algebraic extensions. Finite multiplicative subgroups of a field are cyclic. Existence and uniqueness of splitting fields. [6]

Existence and uniqueness of algebraic closure. [1]

Separability. Theorem of primitive element. Trace and norm. [3]

Normal and Galois extensions, automorphic groups. Fundamental theorem of Galois theory. [3]

Galois theory of finite fields. Reduction mod p . [2]

Cyclotomic polynomials, Kummer theory, cyclic extensions. Symmetric functions. Galois theory of cubics and quartics. [4]

Solubility by radicals. Insolubility of general quintic equations and other classical problems. [3]

Artin's theorem on the subfield fixed by a finite group of automorphisms. Polynomial invariants of a finite group; examples. [2]

Contents

0	Introduction	3
1	Solving equations	4
2	Field extensions	5
2.1	Field extensions	5
2.2	Ruler and compass constructions	5
2.3	K -homomorphisms and the Galois Group	6
2.4	Splitting fields	6
2.5	Algebraic closures	6
2.6	Separable extensions	6
2.7	Normal extensions	7
2.8	The fundamental theorem of Galois theory	7
2.9	Finite fields	7
3	Solutions to polynomial equations	8
3.1	Cyclotomic extensions	8
3.2	Kummer extensions	8
3.3	Radical extensions	8
3.4	Solubility of groups, extensions and polynomials	8
3.5	Insolubility of general equations of degree 5 or more	8
4	Computational techniques	10
4.1	Reduction mod p	10
4.2	Trace, norm and discriminant	10

0 Introduction

1 Solving equations

2 Field extensions

2.1 Field extensions

Definition (Field extension). A *field extension* is an inclusion of a field $K \subseteq L$, where K inherits the algebraic operations from L . We also write this as L/K . Alternatively, we can define this by a injective homomorphism $K \rightarrow L$. We say L is an *extension* of K , and K is a *subfield* of L .

Definition (Degree of field extension). The *degree* of L over K is $[L : K]$ is the dimension of L as a vector space over K . The extension is *finite* if the degree is finite.

Definition (Algebraic number). Let L/K be a field extension, $\alpha \in L$. We define

$$I_\alpha = \{f \in K[t] : f(\alpha) = 0\} \subseteq K[t]$$

This is the set of polynomials for which α is a root. It is easy to show that I_α is an ideal, since it is the kernel of the ring homomorphism $K[t] \rightarrow L$ by $g \mapsto g(\alpha)$.

We say α is *algebraic* over K if $I_\alpha \neq 0$. Otherwise, α is *transcendental* over K .

We say L is *algebraic* over K if every element of L is algebraic.

Definition (Minimal polynomial). Let L/K be a field extension, $\alpha \in L$. The *minimal polynomial* of α over K is a monic polynomial P_α such that $I_\alpha = \langle P_\alpha \rangle$.

Definition (Field generated by α). Let L/K be a field extension, $\alpha \in L$. We define $K(\alpha)$ to be the smallest subfield of L containing K and α . We call $K(\alpha)$ the *field generated by α over K* .

Definition (Field generated by elements). Let L/K be a field extension, $\alpha_1, \dots, \alpha_n \subseteq L$. We define $K(\alpha_1, \dots, \alpha_n)$ to be the smallest subfield of L containing K and $\alpha_1, \dots, \alpha_n$.

We call $K(\alpha_1, \dots, \alpha_n)$ the *field generated by $\alpha_1, \dots, \alpha_n$ over K* .

2.2 Ruler and compass constructions

Definition (Constructible points). Let $S \subseteq \mathbb{R}^2$ be a set of (usually finite) points in the plane.

A “ruler” allows us to do the following: if $P, Q \in S$, then we can draw the line passing through P and Q .

A “compass” allows us to do the following: if $P, Q, Q' \in S$, then we can draw the circle with center at P and radius of length QQ' .

Any point $R \in \mathbb{R}^2$ is *1-step constructible* from S if R belongs to the intersection of two distinct lines or circles constructed from S using rulers and compasses.

A point $R \in \mathbb{R}^2$ is *constructible* from S if there is some $R_1, \dots, R_n = R \in \mathbb{R}^2$ such that R_{i+1} is 1-step constructible from $S \cup \{R_1, \dots, R_i\}$ for each i .

Definition (Field of S). Let $S \subseteq \mathbb{R}^2$ be finite. Define the *field of S* by

$$\mathbb{Q}(S) = \mathbb{Q}(\{\text{coordinates of points in } S\}) \subseteq \mathbb{R},$$

where we put in the x coordinate and y coordinate separately into the generating set.

2.3 K -homomorphisms and the Galois Group

Definition (K -homomorphism). Let L/K and L'/K be field extensions. A K -homomorphism $\phi : L \rightarrow L'$ is a ring homomorphism such that $\phi|_K = \text{id}$, i.e. it fixes everything in K . We write $\text{Hom}_K(L, L')$ for the set of all K -homomorphisms $L \rightarrow L'$.

A K -isomorphism is a K -homomorphism which is an isomorphism of rings. A K -automorphism is a K -isomorphism $L \rightarrow L$. We write $\text{Aut}_K(L)$ for the set of all K -automorphisms $L \rightarrow L$.

Definition (Galois extension). Let L/K be a finite field extension. This is a *Galois extension* if $|\text{Aut}_K(L)| = [L : K]$.

Definition (Galois group). The *Galois group* of a Galois extension L/K is defined as $\text{Gal}(L/K) = \text{Aut}_K(L)$. The group operation is defined by function composition. It is easy to see that this is indeed a group.

2.4 Splitting fields

Notation. Let L/K be a field extension, $f \in K[t]$. We write $\text{Root}_f(L)$ for the roots of f in L .

Definition (Splitting field). Let L/K be a field extension, $f \in K[t]$. We say f *splits* over L if we can factor f as

$$f = a(t - \alpha_1) \cdots (t - \alpha_n)$$

for some $a \in K$ and $\alpha_j \in L$. Alternatively, this says that L contains all roots of f .

We say L is a *splitting field* of f if $L = K(\alpha_1, \dots, \alpha_n)$. This is the smallest field where f has all its roots.

2.5 Algebraic closures

Definition (Algebraically closed field). A field L is *algebraically closed* if for all $f \in L[t]$, we have

$$f = a(t - \alpha_1)(t - \alpha_2) \cdots (t - \alpha_n)$$

for some $a, \alpha_i \in L$. In other words, L contains all roots of its polynomials.

Let L/K be a field extension. We say L is an algebraic closure of K if

- L is algebraic over K
- L is algebraically closed.

2.6 Separable extensions

Definition (Separable polynomial). Let K be a field, $f \in K[t]$ non-zero, and L a splitting field of f . For an irreducible f , we say it is *separable* if f has no repeated roots, i.e. $|\text{Root}_f(L)| = \deg f$. For a general polynomial f , we say it is *separable* if all its irreducible factors in $K[t]$ are separable.

Definition (Formal derivative). Let K be a field, $f \in K[t]$. (*Formal*) *differentiation* the K -linear map $K[t] \rightarrow K[t]$ defined by $t^n \mapsto nt^{n-1}$.

The image of a polynomial f is the *derivative* of f , written f' .

Definition (Separable elements and extensions). Let $K \subseteq L$ be an algebraic field extension. We say $\alpha \in L$ is *separable* over K if P_α is separable, where P_α is the minimal polynomial of α over K .

We say L is *separable* over K (or $L \subseteq L$ is *separable*) if all $\alpha \in L$ are separable.

2.7 Normal extensions

Definition (Normal extension). Let $K \subseteq L$ be an algebraic extension. We say L/K is *normal* if for all $\alpha \in L$, the minimal polynomial of α over K splits over L .

2.8 The fundamental theorem of Galois theory

Definition (Fixed field). Let L/K be a field extension, $H \leq \text{Aut}_K(L)$ a subgroup. We define the *fixed field* of H as

$$L^H = \{\alpha \in L : \phi(\alpha) = \alpha \text{ for all } \phi \in H\}.$$

It is easy to see that L^H is an intermediate field $K \subseteq L^H \subseteq L$.

2.9 Finite fields

Definition. Consider the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$, where q is a power of p . The *Frobenius* $\text{Fr}_q : \mathbb{F}_{q^n} \rightarrow \mathbb{F}_{q^n}$ is defined by $\alpha \mapsto \alpha^q$.

3 Solutions to polynomial equations

3.1 Cyclotomic extensions

Definition (Cyclotomic extension). For a field K , we define the n th *cyclotomic extension* to be the splitting field of $t^n - 1$.

Definition (Primitive root of unity). The n th *primitive root of unity* is an element of order n in $\text{Root}_{t^n - 1}(L)$.

3.2 Kummer extensions

Definition (Cyclic extension). We say a Galois extension L/K is *cyclic* if $\text{Gal}(L/K)$ is a cyclic group.

Definition (Kummer extension). Let K be a field, $\lambda \in K$ non-zero, $n \in \mathbb{N}$, $\text{char } K = 0$ or $0 < \text{char } K \nmid n$. Suppose K contains an n th primitive root of unity, and L is a splitting field of $t^n - \lambda$. If $\deg[L : K] = n$, we say L/K is a *Kummer extension*.

3.3 Radical extensions

Definition (Radical extension). A field extension L/K is *radical* if there is some further extension E/L and with a sequence

$$K = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_r = E,$$

such that each $E_i \subseteq E_{i+1}$ is a cyclotomic or Kummer extension, i.e. E_{i+1} is a splitting field of $t^n - \lambda_{i+1}$ over E_i for some $\lambda_{i+1} \in E_i$.

Definition (Solubility by radicals). Let K be a field, and $f \in K[t]$. f . We say f is *soluble by radicals* if the splitting field of f is a radical extension of K .

3.4 Solubility of groups, extensions and polynomials

Definition (Soluble group). A finite group G is *soluble* if there exists a sequence of subgroups

$$G_r = \{1\} \triangleleft \cdots \triangleleft G_1 \triangleleft G_0 = G,$$

where G_{i+1} is normal in G_i and G_i/G_{i+1} is cyclic.

Definition (Soluble extension). A finite field extension L/K is *soluble* if there is some extension $L \subseteq E$ such that $K \subseteq E$ is Galois and $\text{Gal}(E/K)$ is soluble.

3.5 Insolubility of general equations of degree 5 or more

Definition (Field of symmetric rational functions). Let K be a field, $L = K(x_1, \dots, x_n)$, the field of rational functions over K . Then there is an injective homomorphism $S_n \rightarrow \text{Aut}_K(L)$ given by permutations of x_i .

We define the *field of symmetric rational functions* $F = L^{S_n}$ to be the fixed field of S_n .

Definition (Elementary symmetric polynomials). The *elementary symmetric polynomials* are e_1, e_2, \dots, e_n defined by

$$e_i = \sum_{1 \leq l_1 < l_2 < \dots < l_i \leq n} x_{l_1} \cdots x_{l_i}.$$

Definition (General polynomial). Let K be a field, u_1, \dots, u_n variables. The *general polynomial over K* of degree n is

$$f = t^n + u_1 t^{n-1} + \cdots + u_n.$$

Technically, this is a polynomial in the polynomial ring $K(u_1, \dots, u_n)[t]$. However, we say this is the general polynomial over K because we tend to think of these u_i as representing actual elements of K .

4 Computational techniques

4.1 Reduction mod p

4.2 Trace, norm and discriminant

Definition (Trace). Let K be a field. If $A = [a_{ij}]$ is an $n \times n$ matrix over K , we define the *trace* of A to be

$$\mathrm{tr}(A) = \sum_{i=1}^n a_{ii},$$

i.e. we take the sum of the diagonal terms.

Definition (Trace of linear map). Let V be a finite-dimensional vector space over K , and $\sigma : V \rightarrow V$ a K -linear map. Then we can define

$$\mathrm{tr}(\sigma) = \mathrm{tr}(\text{any matrix representing } \sigma).$$

Definition (Trace of element). Let $K \subseteq L$ be a finite field extension, and $\alpha \in L$. Consider the K -linear map $\sigma : L \rightarrow L$ given by multiplication with α , i.e. $\beta \mapsto \alpha\beta$. Then we define the *trace* of α to be

$$\mathrm{tr}_{L/K}(\alpha) = \mathrm{tr}(\sigma).$$

Definition (Norm of element). We define the *norm* of α to be

$$N_{L/K}(\alpha) = \det(\sigma),$$

where σ is, again, the multiplication-by- α map.

Definition (Discriminant). Let K be a field and $f \in K[t]$, L the splitting field of f over K . So we have

$$f = a(t - \alpha_1) \cdots (t - \alpha_n)$$

for some $a, \alpha_1, \dots, \alpha_n \in L$. We define

$$\Delta_f = \prod_{i < j} (\alpha_i - \alpha_j), \quad D_f = \Delta_f^2 = (-1)^{n(n-1)/2} \prod_{i \neq j} (\alpha_i - \alpha_j).$$

We call D_f the *discriminant* of f .