

Part II — Galois Theory

Theorems

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	8
2.9	Finite fields	8
3	Solutions to polynomial equations	9
3.1	Cyclotomic extensions	9
3.2	Kummer extensions	9
3.3	Radical extensions	10
3.4	Solubility of groups, extensions and polynomials	10
3.5	Insolubility of general equations of degree 5 or more	10
4	Computational techniques	12
4.1	Reduction mod p	12
4.2	Trace, norm and discriminant	12

0 Introduction

1 Solving equations

2 Field extensions

2.1 Field extensions

Theorem (Tower Law). Let $F/L/K$ be field extensions. Then

$$[F : K] = [F : L][L : K]$$

Lemma. Let L/K be a finite extension. Then L is algebraic over K .

Proposition. Let L/K be a field extension, $\alpha \in L$ algebraic over K , and P_α the minimal polynomial. Then P_α is irreducible in $K[t]$.

Theorem. Let L/K a field extension, $\alpha \in L$ algebraic. Then

- (i) $K(\alpha)$ is the image of the (ring) homomorphism $\phi : K[t] \rightarrow L$ defined by $f \mapsto f(\alpha)$.
- (ii) $[K(\alpha) : K] = \deg P_\alpha$, where P_α is the minimal polynomial of α over K .

Corollary. Let L/K be a field extension, $\alpha \in L$. Then α is algebraic over K if and only if $K(\alpha)/K$ is a finite extension.

Theorem. Suppose that L/K is a field extension.

- (i) If $\alpha_1, \dots, \alpha_n \in L$ are algebraic over K , then $K(\alpha_1, \dots, \alpha_n)/K$ is a finite extension.
- (ii) If we have field extensions $L/F/K$ and F/K is a finite extension, then $F = K(\alpha_1, \dots, \alpha_n)$ for some $\alpha_1, \dots, \alpha_n \in L$.

Proposition (Eisenstein's criterion). Let $f = a_n t^n + \dots + a_1 t + a_0 \in \mathbb{Z}[t]$. Assume that there is some prime number p such that

- (i) $p \mid a_i$ for all $i < n$.
- (ii) $p \nmid a_n$
- (iii) $p^2 \nmid a_0$.

Then f is irreducible in $\mathbb{Q}[t]$.

2.2 Ruler and compass constructions

Theorem. Let $S \subseteq \mathbb{R}^2$ be finite. Then

- (i) If R is 1-step constructible from S , then $[\mathbb{Q}(S \cup \{R\}) : \mathbb{Q}(S)] = 1$ or 2 .
- (ii) If $T \subseteq \mathbb{R}^2$ is finite, $S \subseteq T$, and the points in T are constructible from S , Then $[\mathbb{Q}(S \cup T) : \mathbb{Q}(S)] = 2^k$ for some k (where k can be 0).

Corollary. It is impossible to “double the cube”.

2.3 K -homomorphisms and the Galois Group

2.4 Splitting fields

Lemma. Let L/K be a field extension, $f \in K[t]$ irreducible, $\deg f > 0$. Then there is a 1-to-1 correspondence

$$\text{Root}_f(L) \longleftrightarrow \text{Hom}_K(K[t]/\langle f \rangle, L).$$

Corollary. Let L/K be a field extension, $f \in K[t]$ irreducible, $\deg f > 0$. Then

$$|\text{Hom}_K(K[t]/\langle f \rangle, L)| \leq \deg f.$$

In particular, if $E = K[t]/\langle f \rangle$, then

$$|\text{Aut}_K(E)| = |\text{Root}_f(E)| \leq \deg f = [E : K].$$

So E/K is a Galois extension iff $|\text{Root}_f(E)| = \deg f$.

Theorem. Let K be a field, $f \in K[t]$. Then

- (i) There is a splitting field of f .
- (ii) The splitting field is unique (up to K -isomorphism).

2.5 Algebraic closures

Lemma. If R is a commutative ring, then it has a maximal ideal. In particular, if I is an ideal of R , then there is a maximal ideal that contains I .

Theorem (Existence of algebraic closure). Any field K has an algebraic closure.

Theorem (Uniqueness of algebraic closure). Any field K has a unique algebraic closure up to K -isomorphism.

2.6 Separable extensions

Lemma. Let K be a field, $f, g \in K[t]$. Then

- (i) $(f + g)' = f' + g'$, $(fg)' = fg' + f'g$.
- (ii) Assume $f \neq 0$ and L is a splitting field of f . Then f has a repeated root in L if and only if f and f' have a common (non-constant) irreducible factor in $K[t]$ (if and only if f and f' have a common root in L).

Corollary. Let K be a field, $f \in K[t]$ non-zero irreducible. Then

- (i) If $\text{char } K = 0$, then f is separable.
- (ii) If $\text{char } K = p > 0$, then f is not separable iff $\deg f > 0$ and $f \in K[t^p]$. For example, $t^{2p} + 3t^p + 1$ is not separable.

Lemma. Let $L/F/K$ be finite extensions, and E/K be a field extension. Then for all $\alpha \in L$, we have

$$|\text{Hom}_K(F(\alpha), E)| \leq [F(\alpha) : F] |\text{Hom}_K(F, E)|.$$

Theorem. Let L/K and E/K be field extensions. Then

- (i) $|\text{Hom}_K(L, E)| \leq [L : K]$. In particular, $|\text{Aut}_K(L)| \leq [L : K]$.
- (ii) If equality holds in (i), then for any intermediate field $K \subseteq F \subseteq L$:
 - (a) We also have $|\text{Hom}_K(F, E)| = [F : K]$.
 - (b) The map $\text{Hom}_K(L, E) \rightarrow \text{Hom}_K(F, E)$ by restriction is surjective.

Theorem. Let L/K be a finite field extension. Then the following are equivalent:

- (i) There is some extension E of K such that $|\text{Hom}_K(L, E)| = [L : K]$.
- (ii) L/K is separable.
- (iii) $L = K(\alpha_1, \dots, \alpha_n)$ such that P_{α_i} , the minimal polynomial of α_i over K , is separable for all i .
- (iv) $L = K(\alpha_1, \dots, \alpha_n)$ such that R_{α_i} , the minimal polynomial of α_i over $K(\alpha_1, \dots, \alpha_{i-1})$ is separable for all i for all i .

Lemma. Let L be a field, $L^* \setminus \{0\}$ be the multiplicative group of L . If G is a finite subgroup of L^* , then G is cyclic.

Theorem (Primitive element theorem). Assume L/K is a finite and separable extension. Then L/K is simple, i.e. there is some $\alpha \in L$ such that $L = K(\alpha)$.

Corollary. Any finite extension L/K of field of characteristic 0 is simple, i.e. $L = K(\alpha)$ for some $\alpha \in L$.

Proposition. Let L/K be an extension of finite fields. Then the extension is separable.

2.7 Normal extensions

Lemma. Let $L/F/K$ be finite extensions, and \bar{K} is the algebraic closure of K . Then any $\psi \in \text{Hom}_K(F, \bar{K})$ extends to some $\phi \in \text{Hom}_K(L, \bar{K})$.

Theorem. Let L/K be a finite extension. Then L/K is a normal extension if and only if L is the splitting field of some $f \in K[t]$.

Theorem. Let L/K be a finite extension. Then the following are equivalent:

- (i) L/K is a Galois extension.
- (ii) L/K is separable and normal.
- (iii) $L = K(\alpha_1, \dots, \alpha_n)$ and P_{α_i} , the minimal polynomial of α_i over K , is separable and splits over L for all i .

Corollary. Let K be a field and $f \in K[t]$ be a separable polynomial. Then the splitting field of f is Galois.

2.8 The fundamental theorem of Galois theory

Lemma (Artin's lemma). Let L/K be a field extension and $H \leq \text{Aut}_K(L)$ a finite subgroup. Then L/L^H is a Galois extension with $\text{Aut}_{L^H}(L) = H$.

Theorem. Let L/K be a finite field extension. Then L/K is Galois if and only if $L^H = K$, where $H = \text{Aut}_K(L)$.

Theorem (Fundamental theorem of Galois theory). Assume L/K is a (finite) Galois extension. Then

- (i) There is a one-to-one correspondence

$$H \leq \text{Aut}_K(L) \longleftrightarrow \text{intermediate fields } K \subseteq F \subseteq L.$$

This is given by the maps $H \mapsto L^H$ and $F \mapsto \text{Aut}_F(L)$ respectively. Moreover, $|\text{Aut}_K(L) : H| = [L^H : K]$.

- (ii) $H \leq \text{Aut}_K(L)$ is normal (as a subgroup) if and only if L^H/K is a normal extension if and only if L^H/K is a Galois extension.
- (iii) If $H \triangleleft \text{Aut}_K(L)$, then the map $\text{Aut}_K(L) \rightarrow \text{Aut}_K(L^H)$ by the restriction map is well-defined and surjective with kernel isomorphic to H , i.e.

$$\frac{\text{Aut}_K(L)}{H} = \text{Aut}_K(L^H).$$

2.9 Finite fields

Lemma. Let X be a finite field with $q = |K|$ element. Then

- (i) $q = p^d$ for some $d \in \mathbb{N}$, where $p = \text{char } K > 0$.
- (ii) Let $f = t^q - t$. Then $f(\alpha) = 0$ for all $\alpha \in K$. Moreover, K is the splitting field of f over \mathbb{F}_p .

Lemma. Let $q = p^d$, $q' = p^{d'}$, where $d, d' \in \mathbb{N}$. Then

- (i) There is a finite field K with exactly q elements, which is unique up to isomorphism. We write this as \mathbb{F}_q .
- (ii) We can embed $\mathbb{F}_q \subseteq \mathbb{F}_{q'}$ iff $d \mid d'$.

Theorem. Consider $\mathbb{F}_{q^n}/\mathbb{F}_q$. Then Fr_q is an element of order n as an element of $\text{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$.

Theorem. The extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ is Galois with Galois group $\text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) = \text{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^n}) \cong \mathbb{Z}/n\mathbb{Z}$, generated by Fr_q .

3 Solutions to polynomial equations

3.1 Cyclotomic extensions

Theorem. For each $d \in \mathbb{N}$, there exists a d th cyclotomic monic polynomial $\phi_d \in \mathbb{Z}[t]$ satisfying:

- (i) For each $n \in \mathbb{N}$, we have

$$t^n - 1 = \prod_{d|n} \phi_d.$$

- (ii) Assume $\text{char } K = 0$ or $0 < \text{char } K \nmid n$. Then

$$\text{Root}_{\phi_n}(L) = \{n\text{th primitive roots of unity}\}.$$

Note that here we have an abuse of notation, since ϕ_n is a polynomial in $\mathbb{Z}[t]$, not $K[t]$, but we can just use the canonical map $\mathbb{Z}[t] \rightarrow K[t]$ mapping 1 to 1 and t to t .

Theorem. Let K be a field with $\text{char } K = 0$ or $0 < \text{char } K \nmid n$. Let L be the n th cyclotomic extension of K . Then L/K is a Galois extension, and there is an injective homomorphism $\theta : \text{Gal}(L/K) \rightarrow (\mathbb{Z}/n\mathbb{Z})^\times$.

In addition, every irreducible factor of ϕ_n (in $K[t]$) has degree $[L : K]$.

Lemma. Under the notation and assumptions of the previous theorem, ϕ_n is irreducible in $K[t]$ if and only if θ is an isomorphism.

Theorem. ϕ_n is irreducible in $\mathbb{Q}[t]$. In particular, it is also irreducible in $\mathbb{Z}[t]$.

Corollary. Let $K = \mathbb{Q}$ and L be the n th cyclotomic extension of \mathbb{Q} . Then the injection $\theta : \text{Gal}(L/\mathbb{Q}) \rightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ is an isomorphism.

3.2 Kummer extensions

Theorem. Let K be a field, $\lambda \in K$ non-zero, $n \in \mathbb{N}$, $\text{char } K = 0$ or $0 < \text{char } K \nmid n$. Let L be the splitting field of $t^n - \lambda$. Then

- (i) L contains an n th primitive root of unity, say μ .
- (ii) $L/K(\mu)$ is a cyclic (and in particular Galois) extension with degree $[L : K(\mu)] \mid n$.
- (iii) $[L : K(\mu)] = n$ if and only if $t^n - \lambda$ is irreducible in $K(\mu)[t]$.

Lemma. Assume L/K is a field extension. Then $\text{Hom}_K(L, L)$ is linearly independent. More concretely, let $\lambda_1, \dots, \lambda_n \in L$ and $\phi_1, \dots, \phi_n \in \text{Hom}_K(L, L)$ distinct. Suppose for all $\alpha \in L$, we have

$$\lambda_1 \phi_1(\alpha) + \dots + \lambda_n \phi_n(\alpha) = 0.$$

Then $\lambda_i = 0$ for all i .

Theorem. Let K be a field, $n \in \mathbb{N}$, $\text{char } K = 0$ or $0 < \text{char } K \nmid n$. Suppose K contains an n th primitive root of unity, and L/K is a cyclic extension of degree $[L : K] = n$. Then L/K is a Kummer extension.

3.3 Radical extensions

Lemma. Let L/K be a Galois extension, $\text{char } K = 0$, $\gamma \in L$ and F the splitting field of $t^n - \gamma$ over L . Then there exists a further extension E/F such that E/L is radical and E/K is Galois.

Theorem. Suppose L/K is a radical extension and $\text{char } K = 0$. Then there is an extension E/L such that E/K is Galois and there is a sequence

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

where $E_i \subseteq E_{i+1}$ is cyclotomic or Kummer.

3.4 Solubility of groups, extensions and polynomials

Lemma. Let G be a finite group. Then

- (i) If G is soluble, then any subgroup of G is soluble.
- (ii) If $A \triangleleft G$ is a normal subgroup, then G is soluble if and only if A and G/A are both soluble.

Lemma. Let L/K be a Galois extension. Then L/K is soluble if and only if $\text{Gal}(L/K)$ is soluble.

Theorem. Let K be a field with $\text{char } K = 0$, and L/K is a radical extension. Then L/K is a soluble extension.

Corollary. Let K be a field with $\text{char } K = 0$, and $f \in K[t]$. If f can be solved by radicals, then $\text{Gal}(L/K)$ is soluble, where L is the splitting field of f over K .

Lemma. Let K be a field, $f \in K[t]$ of degree n with no repeated roots. Let L be the splitting field of f over K . Then L/K is Galois and there exist an injective group homomorphism

$$\text{Gal}(L/K) \rightarrow S_n.$$

Lemma. Let p be a prime, and $\sigma \in S_p$ have order p . Then σ is a p -cycle.

Theorem. Let $f \in \mathbb{Q}[t]$ be irreducible and $\deg f = p$ prime. Let $L \subseteq \mathbb{C}$ be the splitting field of f over \mathbb{Q} . Let

$$\text{Root}_f(L) = \{\alpha_1, \alpha_2, \dots, \alpha_{p-2}, \alpha_{p-1}, \alpha_p\}.$$

Suppose that $\alpha_1, \alpha_2, \dots, \alpha_{p-2}$ are all real numbers, but α_{p-1} and α_p are not. In particular, $\alpha_{p-1} = \bar{\alpha}_p$. Then the homomorphism $\beta : \text{Gal}(L/\mathbb{Q}) \rightarrow S_n$ is an isomorphism.

3.5 Insolubility of general equations of degree 5 or more

Theorem (Symmetric rational function theorem). Let K be a field, $L = K(x_1, \dots, x_n)$. Let F the field fixed by the automorphisms that permute the x_i . Then

(i) L is the splitting field of

$$f = t^n - e_1 t^{n-1} + \cdots + (-1)^n e_n$$

over F .

(ii) $F = L^{S_n} \subseteq L$ is a Galois group with $\text{Gal}(L/F)$ isomorphic to S_n .

(iii) $F = K(e_1, \dots, e_n)$.

Theorem. Let K be a field with $\text{char } K = 0$. Then the general polynomial over K of degree n cannot be solved by radicals if $n \geq 5$.

Theorem. Let K be a field with $\text{char } K = 0$. If L/K is a soluble extension, then it is a radical extension.

Corollary. Let K be a field with $\text{char } K = 0$ and $h \in K[t]$. Let L be the splitting of h over K . Then h can be solved by radicals if and only if $\text{Gal}(L/K)$ is soluble.

Corollary. Let K be a field with $\text{char } K = 0$. Let $f \in K[t]$ have $\deg f \leq 4$. Then f can be solved by radicals.

4 Computational techniques

4.1 Reduction mod p

Theorem.

$$G = \{\lambda \in S_n : \lambda \text{ preserves the irreducible factor corresponding to } G\}. \quad (\dagger)$$

Theorem. Let $f \in \mathbb{Z}[t]$ be monic with no repeated roots. Let E be the splitting field of f over \mathbb{Q} , and take $\bar{f} \in \mathbb{F}_p[t]$ be the obvious polynomial obtained by reducing the coefficients of f mod p . We also assume this has no repeated roots, and let \bar{E} be the splitting field of \bar{f} .

Then there is an injective homomorphism

$$\bar{G} = \text{Gal}(\bar{E}/\mathbb{F}_p) \hookrightarrow G = \text{Gal}(E/\mathbb{Q}).$$

Moreover, if \bar{f} factors as a product of irreducibles of length n_1, n_2, \dots, n_r , then $\text{Gal}(f)$ contains an element of cycle type (n_1, \dots, n_r) .

4.2 Trace, norm and discriminant

Lemma. Let $L/F/K$ be finite field extensions. Then

$$\text{tr}_{L/K} = \text{tr}_{F/K} \circ \text{tr}_{L/F}, \quad N_{L/K} = N_{F/K} \circ N_{L/F}.$$

Lemma. Let F/K be a field extension, and V an F -vector space. Let $T : V \rightarrow V$ be an F -linear map. Then it is in particular a K -linear map. Then

$$\det_K T = N_{F/K}(\det_F T), \quad \text{tr}_K T = \text{tr}_{F/K}(\text{tr}_F T).$$

Corollary. Let L/K be a finite field extension, and $\alpha \in L$. Let $r = [L : K(\alpha)]$ and let P_α be the minimal polynomial of α over K , say

$$P_\alpha = t^n + a_{n-1}t^{n-1} + \dots + a_0.$$

with $a_i \in K$. Then

$$\text{tr}_{L/K}(\alpha) = -ra_{n-1}$$

and

$$N_{L/K}(\alpha) = (-1)^{nr} a_0^r.$$

Theorem. Let L/K be a finite but not separable extension. Then $\text{tr}_{L/K}(\alpha) = 0$ for all $\alpha \in L$.

Theorem. Let L/K be a finite separable extension. Pick a further extension E/L such that E/K is normal and

$$|\text{Hom}_K(L, E)| = [L : K].$$

Write $\text{Hom}_K(L, E) = \{\varphi_1, \dots, \varphi_n\}$. Then

$$\text{tr}_{L/K}(\alpha) = \sum_{i=1}^n \varphi_i(\alpha), \quad N_{L/K}(\alpha) = \prod_{i=1}^n \varphi_i(\alpha)$$

for all $\alpha \in L$.

Corollary. Let L/K be a finite separable extension. Then there is some $\alpha \in L$ such that $\text{tr}_{L/K}(\alpha) \neq 0$.

Theorem. Let K be a field and $f \in K[t]$, L is the splitting field of f over K . Suppose $D_f \neq 0$ and $\text{char } K \neq 2$. Then

- (i) $D_f \in K$.
- (ii) Let $G = \text{Gal}(L/K)$, and $\theta : G \rightarrow S_n$ be the embedding given by the permutation of the roots. Then $\text{im } \theta \subseteq A_n$ if and only if $\Delta_f \in K$ (if and only if D_f is a square in K).

Theorem. Let K be a field, and $f \in K[t]$ be an n -degree monic irreducible polynomial with no repeated roots. Let L be the splitting field of f over K , and let $\alpha \in \text{Root}_F(L)$. Then

$$D_f = (-1)^{n(n-1)/2} N_{K(\alpha)/K}(f'(\alpha)).$$