Part II – Galois Theory

Based on lectures by Dr C. Brookes
Notes taken by Bhavik Mehta

Michaelmas 2017

0 Introduction

0.1 Course overview

1 Field Extensions

Theorem 1.1 (Tower law)**.** Suppose $K \leq L \leq M$ are field extensions. Then $|M : K| = |M : L|\,|L : K|$.

1.1 Motivatory Example

1.2 Review of GRM

Lemma 1.2. Let $K \leq L$ be a finite field extension. Then L is algebraic over K.

Lemma 1.3. Suppose $K \leq L$ is a field extension, $\alpha \in L$ and α is algebraic over K. Then the minimal polynomial $f_\alpha(t)$ of α over K is irreducible in $K[t]$ and I_α is a prime ideal.

Theorem 1.4. Suppose $K \leq L$ is a field extension and $\alpha \in L$ is algebraic over K. Then

(i) $K(\alpha) = K[\alpha]$

(ii) $|K(\alpha) : K| = \deg f_\alpha(t)$ where $f_\alpha(t)$ is the minimal polynomial of α over K.

Corollary 1.5. If $K \leq L$ is a field extension and $\alpha \in L$, then α is algebraic over K if and only if $K \leq K(\alpha)$ is finite.

Corollary 1.6. Let $K \leq L$ be a field extension with $|L : K| = n$. Let $\alpha \in L$, then $\deg f_\alpha(t) \mid n$.

1.3 Digression on (Non-)Constructibility

Lemma 1.7. x_i, y_i are both roots in K_i of quadratic polynomials in $K_{i-1}[t]$.

Theorem 1.8. If $\mathbf{r} = (x, y)$ is constructible from a set P_0 of points in $\mathbb{R}^2$ and if K_0 is the subfield of $\mathbb{R}$ generated by $\mathbb{Q}$ and the coordinates of the points in P_0, then the degrees $|K_0(x) : K_0|$ and $|K_0(y) : K_0|$ are powers of two.

Theorem 1.9. Let $f(t)$ be a primitive integral polynomial. Then $f(t)$ is irreducible in $\mathbb{Q}[t]$ if and only if it is irreducible in $\mathbb{Z}[t]$.

Theorem 1.10 (Eisenstein's criterion)**.** Let $f(t) = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_0 \in \mathbb{Z}[t]$. Suppose there is a prime p such that

(i) $p \nmid a_n$

(ii) $p \mid a_{n-1}$, $p \mid a_{n-2}, \ldots, p \mid a_0$

(iii) $p^2 \nmid a_0$

Then $f(t)$ is irreducible in $\mathbb{Z}[t]$

Theorem 1.11. The cube cannot be duplicated by ruler and compasses.

Theorem 1.12. The circle cannot be squared using ruler and compasses.

1.4 Return to theory development

Lemma 1.13. Let $K \leq L$ be a field extension. Then

(i) $\alpha_1, \ldots, \alpha_n \in L$ are algebraic over K if and only if $K \leq K(\alpha_1, \ldots, \alpha_n)$ is a finite field extension.

(ii) If $K \leq M \leq L$ such that $K \leq M$ is finite, then there exist $\alpha_1, \ldots, \alpha_n \in L$ such that $K(\alpha_1, \ldots, \alpha_n) = M$.

Lemma 1.14. Suppose $K \leq L$, $K \leq L'$ are field extensions. Then

(i) Any K-homomorphism $\phi : L \to L'$ is injective and $K \leq \phi(L)$ is a field extension.

(ii) If $|L : K| = |L' : K| < \infty$ then any K-homomorphism $\phi : L \to L'$ is a K-isomorphism.

Theorem 1.15 (Existence of splitting fields)**.** Let K be a field and $f(t) \in K[t]$. Then there exists a splitting field for f over K.

Theorem 1.16 (Uniqueness of splitting fields)**.** If K is a field and $f(t) \in K[t]$, then the splitting field for f over K is unique up to K-isomorphism, that is, if there are two such splitting fields L and L', there is a K-isomorphism $\phi : L \to L'$.

Theorem 1.17. Let $K \leq L$ be a finite field extension. Then $K \leq L$ is normal $\iff$ L is the splitting field for some $f(t) \in K[t]$.

Theorem 1.18. Let G be a finite subgroup of the multiplicative group of a field K. Then G is cyclic. In particular, the multiplicative group of a finite field is cyclic.

2 Separable, normal and Galois extensions

Lemma 2.1. Let K be a field and $f(t), g(t) \in K[t]$. Then:

(a) $D(f(t)g(t)) = f'(t)g(t) + f(t)g'(t)$ (Leibniz' rule)

(b) Assume $f(t) \neq 0$. Then $f(t)$ has a repeated root in a splitting field L if and only if $f(t)$ and $f'(t)$ have a common irreducible factor in $K[t]$.

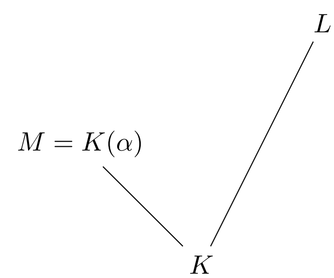
Corollary 2.2. If K is a field and $f(t) \in K[t]$ is irreducible:

(i) If the characteristic of K is 0, then $f(t)$ is separable over K.

(ii) If the characteristic of K is $p > 0$, then $f(t)$ is not separable if and only if $f(t) \in K[t^p]$.

Lemma 2.3. Let $M = K(\alpha)$, where α is algebraic over K and let $f_\alpha(t)$ be the minimal polynomial of α over K.

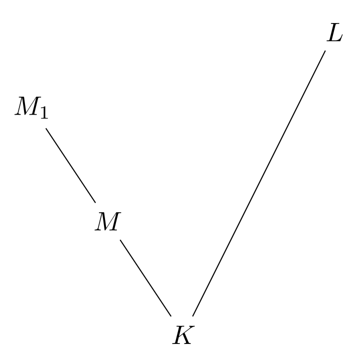
Then, for any field extension $K \leq L$, the number of K-homomorphisms of M to L is equal to the number of distinct roots of $f_\alpha(t)$ in L. Thus this number is $\leq \deg f_\alpha(t) = |K(\alpha) : K| = |M : K|$.



Corollary 2.4. The number of K-homomorphisms $K(\alpha) \to L = \deg f_\alpha(t) \iff L$ is large enough, in particular L contains a splitting field for $f_\alpha(t)$ and α is separable over K.

Lemma 2.5. Let $K \leq M$ be a field extension and $M_1 = M(\alpha_1)$ (where α_1 is algebraic over M). Let $f(t)$ be the minimal polynomial of α_1 over M and let $K \leq L$. Let $\phi : M \to L$ be a K-homomorphism. Then there is a correspondence

$$\{\text{Extensions } \phi_1 : M_1 \to L \text{ of } \phi\} \longleftrightarrow \{\text{roots of } \phi(f(t)) \in L\}.$$



Corollary 2.6. If L is large enough, the number of ϕ_1 which extend ϕ is equal to the number of distinct roots of $f(t)$ in L. This is equal to $|M_i : M| \iff \alpha$ is separable over M.

Corollary 2.7. Let $K \leq M \leq N$ be finite field extensions, $K \leq L$. Let $\phi : M \to L$ be a K-homomorphism. Then the number of extensions of ϕ to maps $\theta : N \to L$ is $\leq |N : M|$. Moreover, such a θ exists if L is large enough.

Lemma 2.8. Let $K \leq N$ be a field extension with $|N : K| = n$ and $N = K(\alpha_1, \dots, \alpha_r)$ say. Then the following are equivalent:

(i) N is separable over K.

(ii) Each α_i is separable over $K(\alpha_1, \dots, \alpha_{i-1})$.

(iii) If $K \leq L$ is large enough there are exactly n distinct K-homomorphisms $N \to L$.

Corollary 2.9. A finite extension is separable $\iff$ it is separably generated.

Lemma 2.10. If $K \leq M \leq L$ finite field extensions, $M \leq L$, then

$$K \leq M, \;\; M \leq L \text{ are both separable } \iff K \leq L \text{ is separable}$$

Theorem 2.11 (Primitive Element Theorem)**.** Any finite separable extension $K \leq M$ is a simple extension, that is, $M = K(\alpha)$ for some α, called a primitive element.

2.1 Trace and Norm

Theorem 2.12. With the above notation, suppose $f_\alpha(t) = t^s + a_{s-1}t^{s-1} + \cdots + a_0$ is the minimal polynomial for α over K. Let $r = |M : K(\alpha)|$, then the characteristic polynomial of θ_α is $(f_\alpha(t))^r$.

Note

$$|M : K| = |M : K(\alpha)| \, |K(\alpha) : K| = rs.$$

Then $\mathrm{Tr}_{M/K}(\alpha) = -ra_{s-1}$ and $N_{M/K} = ((-1)^s a_0)^r$.

Theorem 2.13. Let $K \leq M$ be a finite separable field extension and $|M : K| = n$, $\alpha \in M$. Let $K \leq L$ be large enough so that there are n distinct K-homomorphisms

$$\sigma_1, \sigma_2, \dots, \sigma_n : M \longrightarrow L.$$

Then the characteristic polynomial of $\theta_\alpha : M \to M$ (the multiplication map) is

$$\prod_{i=1}^{n} (t - \sigma_i(\alpha))$$

hence

$$\mathrm{Tr}_{M/K}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha) \qquad \text{and} \qquad N_{M/K}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha).$$

Theorem 2.14. Let $K \leq M$ be a finite separable extension. Then we define a K-bilinear form

$$\begin{aligned} T : M \times M &\to K \\ (x, y) &\longmapsto \mathrm{Tr}_{M/K}(xy). \end{aligned}$$

Then this is non-degenerate and in particular the K-linear map $\mathrm{Tr}_{M/K} : M \to K$ is non-zero, and hence surjective.

2.2 Normal extensions

Lemma 2.15.

$$\mathrm{Aut}_K(M) \leq |M : K| \, .$$

Theorem 2.16. Let $K \leq M$ be a finite field extension. Then $|\mathrm{Aut}_K(M)| = |M : K|$ iff the extension is both normal and separable.

3 Fundamental Theorem of Galois Theory

3.1 Artin's Theorem

Theorem 3.1 (Fundamental Theorem of Galois Theory)**.** Let $K \le L$ be a finite Galois extension. Then

(i) there is a 1 to 1 correspondence

$$\begin{aligned} \{\text{intermediate subfields } K \le M \le L\} &\longleftrightarrow \{\text{subgroups } H \text{ of } \operatorname{Gal}(L/K)\} \\ M &\longmapsto \operatorname{Aut}_M(L) \\ L^H &\longleftarrow\!\shortmid H \end{aligned}$$

This is called the Galois correspondence.

(ii) H is a normal subgroup of $\operatorname{Gal}(L/K)$ iff $K \le L^H$ is normal iff $K \le L^H$ is Galois.

(iii) If $H \triangleleft \operatorname{Gal}(L/K)$ then the map

$$\theta : \operatorname{Gal}(L/K) \longrightarrow \operatorname{Gal}(L^H/K)$$

given by restriction to L^H is a surjective group homomorphism with kernel H.

Theorem 3.2 (Artin's Theorem)**.** Let $K \le L$ be a field extension and H a finite subgroup of $\operatorname{Aut}_K(L)$. Let $M = L^H$. Then $M \le L$ is a finite Galois extension, and $H = \operatorname{Gal}(L/M)$.

Theorem 3.3. Let $K \le L$ be a finite field extension. Then the following are equivalent:

(i) $K \le L$ is Galois

(ii) $L^H = K$ when $H = \operatorname{Aut}_K(L)$

3.2 Galois groups of polynomials

Lemma 3.4. Suppose $f(t)$ is separable, $f(t) = g_1(t) \cdots g_s(t)$ with $g_i(t)$ irreducible in $K[t]$ is a factorisation in $K[t]$. Then the orbits of $\operatorname{Gal}(f)$ on the roots of $f(t)$ correspond to the factors $g_j(t)$.

$$\text{Two roots are in the same orbit} \iff \text{they are roots of the same } g_j(t).$$

In particular, if $f(t)$ is irreducible in $K[t]$ there is one orbit, i.e., $\operatorname{Gal}(f)$ acts transitively on the roots of $f(t)$.

Lemma 3.5. The transitive subgroups of S_n for $n \le 5$ are

$$\begin{aligned} n = 2&: \quad S_2\ (\cong C_2) \\ n = 3&: \quad A_3\ (\cong C_3),\ S_3 \\ n = 4&: \quad C_4,\ V_4,\ D_8,\ A_4,\ S_4 \\ n = 5&: \quad C_5,\ D_{10},\ H_{20},\ A_5,\ S_5 \end{aligned}$$

where H_{20} is generated by a 5-cycle and a 4-cycle.

Theorem 3.6. Let p be a prime, and $f(t)$ irreducible $\in \mathbb{Q}[t]$ of degree p. Suppose $f(t)$ has exactly 2 non-real roots in $\mathbb{C}$. Then $\operatorname{Gal}(f)$ over $\mathbb{Q} \cong S_p$.

Lemma 3.7. Let $f(t)$ be separable $\in K[t]$ of degree n with $\operatorname{char} K \neq 2$. Then

$$\operatorname{Gal}(f) \leq A_n \iff D(f) \text{ is a square in } K.$$

Theorem 3.8 (Mod p reduction)**.** Let $f(t) \in \mathbb{Z}[t]$ be monic of degree n with n distinct roots in a splitting field. Let p be a prime such that $\overline{f}(t)$, the reduction of $f(t)$ mod p also has n distinct roots in a splitting field. Let $\overline{f}(t) = \overline{g_1}(t) \cdots \overline{g_s}(t)$ be the factorisation into irreducibles in $\mathbb{F}_p[t]$ with $n_j = \deg \overline{g_j}(t)$. Then $\operatorname{Gal}(\overline{f}) \hookrightarrow \operatorname{Gal}(f)$ and has an element of cycle type $(n_1, n_2, \ldots, n_s)$.

3.3 Galois Theory of Finite Fields

Theorem 3.9 (Galois groups of finite fields)**.** Let $\mathbb{F}$ be a finite field with $|\mathbb{F}| = p^r$. Then $\mathbb{F}_p \leq \mathbb{F}$ is a Galois extension with $\operatorname{Gal}(\mathbb{F}/\mathbb{F}_p) = G$, a cyclic group with the Frobenius automorphism as generator.

Corollary 3.10. Let $\mathbb{F}_p \leq M \leq \mathbb{F}$ be finite fields. Then $\operatorname{Gal}(\mathbb{F}/M)$ is cyclic, generated by ϕ^u, where ϕ is the Frobenius automorphism and $|M| = p^u$ and M is the fixed field of $\langle \phi^u \rangle$.

Theorem 3.11 (Existence of finite fields)**.** Let p be a prime and $u \geq 1$. Then there is a field of order p^u, unique up to isomorphism.

4 Cyclotomic and Kummer extensions

4.1 Cyclotomic extensions

Lemma 4.1. $\Phi_m(t) \in \mathbb{Z}[t]$ if $\operatorname{char} K = 0$ (with $\mathbb{Q} \hookrightarrow K$, prime subfield). $\Phi_m(t) \in \mathbb{F}_p[t]$ if $\operatorname{char} K = p$ (with $\mathbb{F}_p \hookrightarrow K$, prime subfield).

Lemma 4.2. The homomorphism $\theta : G \to (\mathbb{Z}/m\mathbb{Z})^\times$ defined in **??** is an isomorphism iff $\Phi_m(t)$ is irreducible.

Theorem 4.3. Let L be the mth cyclotomic extension of finite field $\mathbb{F} = \mathbb{F}_q$ where $q = p^n$. Then the Galois group $G = \operatorname{Gal}(L/\mathbb{F})$ is isomorphic to the cyclic subgroup of $(\mathbb{Z}/m\mathbb{Z})^\times$ generated by q.

Theorem 4.4. For all $m > 0$, $\Phi_m(t)$ is irreducible in $\mathbb{Z}[t]$ and hence in $\mathbb{Q}[t]$. Thus θ in **??** is an isomorphism and thus $\operatorname{Gal}(\mathbb{Q}(\xi)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$ where $\xi =$ primitive mth root of unity.

4.2 Kummer Theory

Theorem 4.5. Let $f(t) = t^m - \lambda \in K[t]$ and $\operatorname{char} K \nmid m$. Then the splitting field L of $f(t)$ over K contains a primitive mth root of unity ξ and $\operatorname{Gal}(L/K(\xi))$ is cyclic of order dividing m. Moreover $f(t)$ is irreducible over $K(\xi)$ iff $|L : K(\xi)| = m$.

Theorem 4.6. Suppose $K \leq M$ is a cyclic extension with $|L : K| = m$, where $\operatorname{char} K \nmid m$ and that K contains a primitive mth root of unity. Then $\exists \lambda \in K$ such that $t^m - \lambda$ is irreducible over K and K is the splitting field of $t^m - \lambda$ over K. If β is a root of $t^m - \lambda$ in L, then $L = K(\beta)$.

Lemma 4.7. Let $\phi_1, \ldots, \phi_n$ be embeddings of a field K into a field L. Then there do not exist $\lambda_1, \ldots, \lambda_n$ not all zero such that $\lambda_1\phi_1(x) + \cdots + \lambda_n\phi_n(x) = 0\ \forall x \in K$.

4.3 Cubics

4.4 Quartics

4.5 Solubility by radicals

Lemma 4.8. A finite group G is soluble if and only if we have

$$\{e\} = G_m \lhd G_{m-1} \lhd \cdots \lhd G_1 \lhd G_0 = G$$

with G_i/G_{i+1} cyclic.

Lemma 4.9. Let $K \lhd G$. Then G/K abelian $\iff$ $G' \leq K$.

Lemma 4.10. For G finite, G is soluble $\iff$ $G^{(m)} = \{e\}$ for some m.

Lemma 4.11.

(i) Let $H \leq G$, G soluble. Then H soluble.

(ii) Let $H \lhd G$, then G soluble $\iff$ H and G/H both soluble.

Theorem 4.12. Let K be a field and $f(t) \in K[t]$. Assume $\operatorname{char} K = 0$. Then $f(t)$ is soluble by radicals over $K \iff \operatorname{Gal} f$ over K is soluble.

Corollary 4.13. If $f(t)$ is a monic irreducible polynomial $\in K[t]$ with $\operatorname{Gal}(f) \cong A_5$ or S_5 then $f(t)$ is not soluble by radicals (with $\operatorname{char} K = 0$).

Lemma 4.14. If $K \leq N$ is an extension by radicals then $\exists N'$ with $N \leq N'$ with $K \leq N'$ is an extension by radicals, with $K \leq N'$ a Galois extension.

5 Final Thoughts

5.1 Algebraic closure

Lemma 5.1. If $K \leq L$ is algebraic and every polynomial in $K[t]$ splits completely over L, then L is an algebraic closure of K.

Lemma 5.2 (Zorn's Lemma)**.** Let $(\mathcal{S}, \leq)$ be a non-empty partially ordered set. Suppose that any chain has an upper bound in $\mathcal{S}$. Then $\mathcal{S}$ has a maximal element.

Lemma 5.3. Let R be a ring. Then R has a maximal ideal.

Theorem 5.4 (Existence of algebraic closures)**.** For any field K there is an algebraic closure.

Theorem 5.5. Suppose $\theta : K \to L$ is a ring homomorphism and L is algebraically closed. Suppose $K \leq M$ is an algebraic extension. Then θ can be extended to a homomorphism $\theta : M \to L$ (i.e. $\phi|_K = \theta$).

Theorem 5.6 (Uniquness of algebraic closures)**.** If $K \leq L_1$, $L \leq L_2$ are two algebraic closures of K then there exists an isomorphism $\phi : L_1 \to L_2$.

5.2 Symmetric polynomials and invariant theory

Theorem 5.7. The fixed field $M = L^{s_n} = K(s_1, \ldots, s_n)$ and the $s_1, \ldots, s_n$ are algebraically independent over K (in L).