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

Definition 1.1 (Field extension)**.** A **field extension** $K \leq L$ is the inclusion of a field K into another field L with the same 0, 1, and where the restriction of $+$ and $\cdot$ (in L) to K gives the $+$ and $\cdot$ of K.

Definition 1.2 (Degree)**.** The **degree** of L over K is $\dim_K L$, the K-vector space dimension of L. This may not be finite. We typically denote this by $|L : K|$. If $|L : K| < \infty$, then the extension is **finite**, otherwise the extension is **infinite**.

1.1 Motivatory Example

1.2 Review of GRM

Definition 1.3 (Algebraic)**.** Suppose $K \leq L$ is a field extension. Take $\alpha \in L$ and define

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

We say α is **algebraic** over K if $I_\alpha \neq 0$. Otherwise α is **transcendental**. We say L is algebraic over K if α is algebraic over K for all $\alpha \in L$.

Definition 1.4 (Minimal polynomial)**.** The non-zero ideal I_α (where α is algebraic over K) is principal since $K[t]$ is a principal ideal domain. In particular, we can say $I_\alpha = (f_\alpha(t))$ where $f_\alpha(t)$ can be assumed to be monic. Such a monic $f_\alpha(t)$ is the **minimal polynomial** of α over K.

Definition 1.5 (Simple extension)**.** Suppose $K \leq L$ is a field extension and $\alpha \in L$. $K(\alpha)$ is defined to be the smallest subfield of L containing K and α. It's called the field **generated** by K and α. We say that L is a **simple extension** if $L = K(\beta)$ for some $\beta \in L$.

Given $\alpha_1, \ldots, \alpha_n \in L$, $K \leq L$. $K(\alpha_1, \ldots \alpha_n)$ is the smallest field containing $\alpha_1, \ldots, \alpha_n$. It is the field generated by K and $\alpha_1, \ldots, \alpha_n$.

On the other hand $K[\alpha]$ is the ring generated by K and α, in particular the image of $K[t]$ under the map $f(t) \mapsto f(\alpha)$.

1.3 Digression on (Non-)Constructibility

Definition 1.6 (Constructible)**.** The points of intersection of any two distinct lines or circles drawn using these operations are **constructible in one step** from P_0. More generally, a point $\mathbf{r} \in \mathbb{R}^2$ is **constructible** from P_0 if there is a finite sequence $\mathbf{r_1}, \mathbf{r_2}, \ldots, \mathbf{r_n} = \mathbf{r}$ such that $\mathbf{r_i}$ is constructible in one step from $P_0 \cup \{\mathbf{r_1}, \ldots, \mathbf{r_{i-1}}\}$.

1.4 Return to theory development

Definition 1.7 (Homomorphism over a field)**.** Suppose $K \leq L$, $K \leq L'$ are field extensions. A K-**homomorphism** $\phi : L \to L'$ is a ring homomorphism such that $\phi|_K = \mathrm{id}$.

A K-homomorphism is a K-isomorphism if it is a ring isomorphism.

Definition 1.8 (Splitting)**.** Let $K \leq L$ be a field extension and $f(t) \in K[t]$. We say f **splits over** L if

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

where $a \in K$ and $\alpha_1, \ldots, \alpha_n \in L$.

We say L is a **splitting field for** f **over** K if $L = K(\alpha_1, \ldots, \alpha_n)$.

Definition 1.9 (Normal extension)**.** A field extension $K \leq L$ is **normal** if for every $\alpha \in L$ the minimal polynomial $f_\alpha(t)$ of α over K splits over L.

2 Separable, normal and Galois extensions

Definition 2.1 (Separable polynomial)**.** Let K be a field and $f(t) \in K[t]$. Suppose $f(t)$ is irreducible in $K[t]$ and L is a splitting field for $f(t)$ over K. Then $f(t)$ is **separable** over K if $f(t)$ has no repeated roots in L.

For general $f(t)$ we say $f(t)$ is separable over K if every irreducible factor in $K[t]$ is separable over K.

All constant polynomials are separable.

Definition 2.2 (Formal differentiation)**.** If K is a field then **formal differentiation**

$$\begin{aligned} D : K[t] &\to K[t] \\ t^n &\mapsto nt^{n-1} \end{aligned}$$

is a K-linear map. We denote this by $D(f(t)) = f'(t)$.

Definition 2.3 (Separable extension)**.** We say $\alpha \in L$ **is separable over** K if its minimal polynomial is separable over K.

L **is separable over** K if all $\alpha \in L$ are separable over K.

If $f_\alpha(t) = (t-\alpha)^n = t^n - \alpha^n$ where n is a power of $p(= \operatorname{char} K)$, we say that α is **purely inseparable over** K.

Definition 2.4 (Separably generated)**.** We say $M = K(\alpha_1, \dots, \alpha_r)$ is **separably generated** by $\alpha_1, \dots, \alpha_r$ over K if each α_i is separable over K.

2.1 Trace and Norm

Definition 2.5 (Trace and norm)**.** Let $K \leq M$ be a finite field extension, and $\alpha \in M$. Multiplication by α gives a K-linear map $\theta_\alpha : M \to M$.

Then we define

Trace of α **over** K is given by $\operatorname{Tr}_{M/K}(\alpha) = \text{trace of } \theta_\alpha \in K$.

Norm of α **over** K is given by $N_{M/K}(\alpha) = \text{determinant of } \theta_\alpha \in K$.

Note these are dependent on the field extension.

2.2 Normal extensions

Definition 2.6 (Automorphism group)**.** Let $K \leq M$ be a finite field extension. Its **K-automorphism** group is $\operatorname{Aut}_K(M) = \{ \phi \mid \phi \text{ a } K\text{-homomorphism } M \to M \}$.

Definition 2.7 (Galois extension)**.** A finite field extension that is normal and separable is a **Galois extension**.

Definition 2.8 (Galois group)**.** Let $K \leq M$ be a Galois extension. Then, the K-automorphism group of M is the **Galois group** of M over K. Write this as $\operatorname{Gal}(M/K)$.

3 Fundamental Theorem of Galois Theory

3.1 Artin's Theorem

Definition 3.1 (Fixed field)**.** Let $K \leq L$ be a field extension and $H \leq \mathrm{Aut}_K(L)$. The **fixed field** of H is,

$$L^H := \{\, \alpha \in L \mid \sigma(\alpha) = \alpha \text{ for all } \sigma \in H \,\}$$

3.2 Galois groups of polynomials

Definition 3.2 (Galois group of polynomial)**.** Let $f(t)$ be a separable polynomial $\in K[t]$ and let $K \leq L$ with L a splitting field for $f(t)$. Then the **Galois group of** $f(t)$ over K is

$$\mathrm{Gal}(f) := \mathrm{Gal}(L/K).$$

Definition 3.3 (Discriminant)**.** Let $f(t) \in K[t]$ with distinct roots $\alpha_1, \ldots, \alpha_n$ in a splitting field (with $f(t)$ not necessarily irreducible). Let

$$\Delta = \prod_{i<j} (\alpha_i - \alpha_j).$$

Then the **discriminant** $D = D(f)$ of f is

$$\begin{aligned} D = \Delta^2 &= \prod_{i<j} (\alpha_i - \alpha_j)^2 \\ &= (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j} (\alpha_i - \alpha_j). \end{aligned}$$

3.3 Galois Theory of Finite Fields

Definition 3.4 (Frobenius automorphism)**.** Let $\mathbb{F}$ be a finite field of characteristic p. Then the **Frobenius automorphism** of $\mathbb{F}$ is

$$\begin{aligned} \phi : \mathbb{F} &\longrightarrow \mathbb{F} \\ \alpha &\longmapsto \alpha^p. \end{aligned}$$

4 Cyclotomic and Kummer extensions

4.1 Cyclotomic extensions

Definition 4.1 (Cyclotomic extension)**.** Suppose $\operatorname{char} K = 0$ or p prime where $p \nmid m$. The mth **cyclotomic extension** of K is the splitting field L of $t^m - 1$.

Definition 4.2 (Primitive mth root of unity)**.** An element $\xi \in \mu_m$ is a **primitive mth root of unity** if $\mu_m = \langle \xi \rangle$.

Definition 4.3 (Group of roots of unity)**.**

$$\theta : G \longrightarrow (\mathbb{Z}/m\mathbb{Z})^\times$$

This is a group homomorphism: If $\sigma(\xi) = \xi^c, \phi(\xi) = \xi^j$ then $(\sigma\phi)(\xi) = \sigma(\xi^j) = \xi^{ij}$. Hence G is abelian.

Thus we regard G as a subgroup of $(\mathbb{Z}/m\mathbb{Z})^\times$.

Definition 4.4 (Cyclotomic polynomial)**.** The mth **cyclotomic polynomial** is

$$\Phi_m(t) = \prod_{i \in (\mathbb{Z}/m\mathbb{Z})^\times} (t - \xi^i),$$

the product of the linear factors of $t^m - 1$ corresponding to the primitive mth roots of unity.

Definition 4.5 (Cyclic, abelian extension)**.** An extension $K \leq L$ is **cyclic** if the extension is Galois and $\operatorname{Gal}(L/K)$ is cyclic. Similarly, it is called **abelian** if $\operatorname{Gal}(L/K)$ is abelian.

4.2 Kummer Theory

Definition 4.6 (Kummer extension)**.** A cyclic extension $K \leq L$ with $|L : K| = m$, where $\operatorname{char} K \nmid m$ and K contains a primitive mth root of unity is a **Kummer extension**.

Definition 4.7 (Extension by radicals)**.** A field extension $K \leq L$ is an **extension by radicals** if $\exists K = L_0 \leq L_1 \leq \cdots \leq L_n = L$ such that each $L_i \leq L_{i+1}$ is either cyclotomic or Kummer extension. A polynomial $f(t) \in K[t]$ is **soluble by radicals** if its splitting field lies in an extension by radicals.

4.3 Cubics

4.4 Quartics

4.5 Solubility by radicals

Definition 4.8 (Soluble group)**.** A group is **soluble** if there is a chain of subgroups

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

with G_i/G_{i+1} abelian.

Definition 4.9 (Derived subgroup)**.** The **derived subgroup** G' of a group G is the subgroup generated by all the commutators $g_1 g_2 g_1^{-1} g_2^{-1}$ for $g_1, g_2 \in G$.

Definition 4.10 (Derived series)**.** The **derived series** $\{G^{(m)}\}$ of G is defined inductively:

$$\begin{aligned} G^{(0)} &= G \\ G^{(1)} &= G' \\ G^{(2)} &= (G')' \\ G^{(j+1)} &= (G^{(j)})' \end{aligned}$$

Thus $G = G^{(0)} \triangleright G^{(1)} \triangleright G^{(2)} \triangleright \cdots$ with $G^{(j)}/G^{(j+1)}$ abelian.

5 Final Thoughts

5.1 Algebraic closure

Definition 5.1 (Algebraically closed)**.** A field L is **algebraically closed** if any $f(t) \in L[t]$ splits into a product of linear factors in $L[t]$.

Definition 5.2 (Algebraic closure)**.** An extension $K \leq L$ is an algebraic closure of K if $K \leq L$ is algebraic and L is algebraically closed.

Definition 5.3 (Partial order)**.** $(\mathcal{S}, \leq)$ is a **partial order** on $\mathcal{S}$ if

(i) $\forall x \in \mathcal{S}\ x \leq x$

(ii) $x \leq y$ and $y \leq z \implies x \leq z$.

(iii) if $x \leq y$ and $y \leq x$ then $x = y$.

$\mathcal{S}$ is **totally ordered** if for any $x, y \in S$ either $x \leq y$ or $y \leq x$. A **chain** is a partially ordered set $(\mathcal{S}, \leq)$ that is a totally ordered subset.

5.2 Symmetric polynomials and invariant theory

Definition 5.4 (Elementary symmetric polynomials)**.** These s_i are the elementary symmetric polynomials.

Definition 5.5. $\alpha_1, \ldots, \alpha_n$ are **algebraically independent** over K if the ring homomorphism $K[Y_1, \ldots, Y_n] \to K[\alpha_1, \ldots, \alpha_n] \leq L$ is an isomorphism where $K[Y_1, \ldots, Y_n]$ is the polynomial ring in $Y_1, \ldots, Y_n$.