Part II – Galois Theory

Based on lectures by Dr C. Brookes

Notes taken by Bhavik Mehta

Michaelmas 2017

0 Introduction

The primary motivation of this course is to study the solutions of polynomial equations in one variable to wander whether there is a formula involving roots, a solution by radicals. Quadratics were typically studied in school, while the solution in radicals for cubics and quartics has been known for a long time and studied in particular in 1770 by Lagrange.

In 1799, Ruffini claimed that there were some quintics that can't be solved by radicals, that is, there is no general formula, but it took until 1824 before Abel used existing ideas about permutations to produce the first accepted proof of insolubility, before dying in 1829. Galois' main contribution was in 1831, when he gave the first explanation as to why some polynomials are soluble by radicals and others are not. He made use of the group of permutations of the roots of a polynomial, and realised in particular the importance of *normal* subgroups.

Galois' work was not known generally in his lifetime - it was only published by Liouville in 1846, who realised that it tied in well with the work of Cauchy on permutations. Galois had submitted his work for various competitions and for entry into the Ecole Polytechnique in Paris. Unfortunately Galois died in a duel in 1832, leaving a six and a half page letter indicating his thoughts about the future development of his theory.

0.1 Course overview

Most of this course is Galois Theory, but presented in a more modern fashion- in terms of field extensions. Recall from GRM that if $f(t)$ is an irreducible polynomial in $k[t]$ where k is a field, then $k[t]/(f(t))$ is a field, where $(f(t))$ denotes the ideal of $k[t]$ generated by $f(t)$, and this new field contains k. In this way, we can see the field $k[t]/(f(t))$ as a field extension of k.

Prerequisites Quite a lot of the Groups, Rings and Modules course, but no modules except in one place where it's useful to know the structure of finite abelian groups. The DPMMS website has a Galois Theory page with a long history of example sheets and notes, in particular see Tony Scholl's 2013-4 course page.

1 Field Extensions

Definition 1.1. 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 . (in L) to K gives the + and . of K.

Example.

(i) $\mathbb{Q} \leq \mathbb{R}$

(ii) $\mathbb{R} \leq \mathbb{C}$

(iii) $\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}) = \{ \lambda + \mu\sqrt{2} \mid \lambda, \mu \in \mathbb{Q} \}$

(iv) $\{ \lambda + \mu i \mid \lambda, \mu \in \mathbb{Q} \} = \mathbb{Q}(i) \leq \mathbb{C}$

Suppose $K \leq L$ is a field extension. Then L is a K-vector space using the addition from the field structure and scalar multiplcation given by the multiplication in the field L.

Definition 1.2. 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**.

Example.

(i) $|\mathbb{C} : \mathbb{R}| = 2$, with $\mathbb{R}$-basis $1, i$

(ii) $|\mathbb{Q}(i) : \mathbb{Q}| = 2$, with $\mathbb{Q}$-basis $1, i$

(iii) $\mathbb{Q} \leq \mathbb{R}$ is an infinite extension.

Theorem 1.3 (Tower law)**.** Suppose $K \leq L \leq M$ are field extensions. Then $|M : K| = |M : L|\,|L : K|$.

Proof. Assume that $|M : L| < \infty$, and $|L : K| < \infty$. Take an L-basis of M, given by $\{ f_1, \ldots, f_b \}$, and a K-basis of L given by $\{ e_1, \ldots, e_a \}$. Take $m \in M$, so $m = \sum_{i=1}^{b} \mu_i f_i$ for some $\mu_i \in L$. Similarly, $\mu_i = \sum_{j=1}^{a} \lambda_{ij} e_j$ for some $\lambda_{ij} \in K$, so

$$m = \sum_{i=1}^{b} \sum_{j=1}^{a} \lambda_{ij} e_j f_i$$

Thus $\{ e_j f_i \mid 1 \leq j \leq a, 1 \leq i \leq a \}$ span M.

Linear independence: It's enough to show that if $0 = m = \sum \sum \lambda_{ij} e_j f_i$ then λ_{ij} are all zero. However if $m = 0$ the linear independence of f_i forces each $\mu_i = 0$. Then the linear indepedence of e_j forces λ_{ij} all to be zero, as required. □

The tower law will not be proved for infinite extensions, but observe that if M is an infinite extension of L then it is an infinite extension of K, and similarly if L is an infinite extension of K then the larger field M must also be an infinite extension of K.

1.1 Motivatory Example

Observe $\mathbb{Q} \leq \mathbb{Q}\left(\sqrt{2}\right) \leq \mathbb{Q}\left(\sqrt{2}, i\right)$

(i) $\mathbb{Q}\left(\sqrt{2}\right)$ has basis $1, \sqrt{2}$ over $\mathbb{Q}$.

(ii) $\mathbb{Q}\left(\sqrt{2}, i\right)$ has basis $1, i$ as a $\mathbb{Q}\left(\sqrt{2}\right)$–vector space.

(iii) $\mathbb{Q}\left(\sqrt{2}, i\right)$ has basis $1, \sqrt{2}, i, i\sqrt{2}$ over $\mathbb{Q}$.

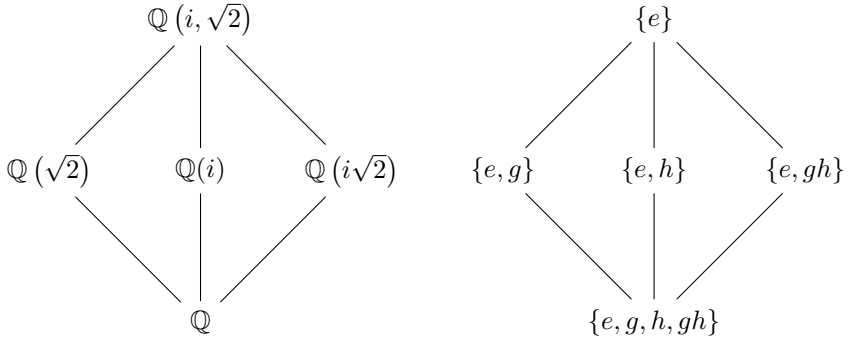
$$\left|\mathbb{Q}\left(i, \sqrt{2}\right) : \mathbb{Q}\right| = 4 = 2 \cdot 2 = \left|\mathbb{Q}\left(i, \sqrt{2}\right) : \mathbb{Q}\left(\sqrt{2}\right)\right| \left|\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right|$$

Any intermediate field strictly between $\mathbb{Q}$ and $\mathbb{Q}\left(\sqrt{2}, i\right)$ must be of degree 2 by the tower law. What are these intermediate fields? There are $\mathbb{Q}\left(\sqrt{2}\right)$, $\mathbb{Q}(i)$ and $\mathbb{Q}\left(i\sqrt{2}\right)$, but are these all?

The Galois correspodence arising in the Fundamental Theorem of Galois theory gives an order reversing bijection between the lattice of intermediate subfields and the subgroups of a group of ring automorphisms of the big field (in this case $\mathbb{Q}\left(i, \sqrt{2}\right)$) that fix the smaller field elementwise. For instance, consider the ring automorphisms of $\mathbb{Q}\left(i, \sqrt{2}\right)$ that fix $\mathbb{Q}$:

$$\begin{aligned} e : \sqrt{2} &\mapsto \sqrt{2} \\ i &\mapsto i \\ g : \sqrt{2} &\mapsto \sqrt{2} \\ i &\mapsto -i \\ h : \sqrt{2} &\mapsto -\sqrt{2} \\ i &\mapsto i \\ gh : \sqrt{2} &\mapsto -\sqrt{2} \\ i &\mapsto -i \end{aligned}$$

Notice that i and $-i$ play the same role in the field $\mathbb{Q}\left(\sqrt{2}, i\right)$, both roots of $t^2 + 1 = 0$, similarly $\sqrt{2}$ and $-\sqrt{2}$ are both roots of $t^2 - 2 = 0$. The automorphism e is seen to be identity, and g is conjugation. These four form the group of order $4 = \left|\mathbb{Q}\left(\sqrt{2}, i\right) : \mathbb{Q}\right|$.



The recipe for producing an intermediate subfield from a subgroup is to take the elements of $\mathbb{Q}\left(i, \sqrt{2}\right)$ which are fixed by all elements of the subgroup. For instance, $\mathbb{Q}\left(i\sqrt{2}\right)$ is the field of elements fixed by both e and gh.

This correspondence doesn't always work for all finite field extensions. It works for Galois extensions. In the correspondence, normal extensions correspond to normal subgroups. In this example, all subgroups are normal and the extensions are normal. We'll also prove the Primitive Element Theorem, which in the context of finite extensions of $\mathbb{Q}$ tells us that they are necessarily of the form $\mathbb{Q}(\alpha)$ for some α, for instance $\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(i + \sqrt{2})$.

1.2 Review of GRM

Definition 1.4. 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 $\alpha \in L$.

Remark. We can see I_α is an ideal of $K[t]$ since it is the kernel of the ring homomorphism $K[t] \to L$ given by $f(t) \mapsto f(\alpha)$.

Example.

(i) $\sqrt{2}$ is algebraic over $\mathbb{Q}$

(ii) π is algebraic over $\mathbb{Q}$

Lemma 1.5. Let $K \leq L$ be a finite field extension. Then L is algebraic over K.

Proof. Let $|L : K| = n$, and take $\alpha \in L$. Consider $1, \alpha, \alpha^2, \ldots, \alpha^n$, which must be linearly dependent in the n-dimensional K–vector space L. So, $\sum_{i=0}^{n} \lambda_i \alpha^i = 0$ for some $\lambda \in K$ not all zero, and hence α is a root of $f(t) = \sum_{i=0}^{n} \lambda_i t^i$, so α is algebraic over K. α was arbitrary, so L is algebraic over K. □

Definition 1.6. 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.

Remark. Multiplication by α within the field L gives a K–linear map $L \to L$, an automorphism (if $\alpha \neq 0$). In GRM, we have seen the minimal polynomial of a linear map is unique.

Example.

(1) The minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $t^2 - 2$.

(2) The minimal polynomial of $\sqrt{2}$ over $\mathbb{R}$ is $t - \sqrt{2}$.

Lemma 1.7. Suppose $K \leq L$ is a field extension, $\alpha \in L$ and α is 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.

Proof. Suppose $f_\alpha(t) = p(t)q(t)$. We aim to show $p(t)$ or $q(t)$ is a unit in $K[t]$. But $0 = f_\alpha(\alpha) = p(\alpha)q(\alpha)$, so $p(\alpha) = 0$ or $q(\alpha) = 0$, without loss of generality take $p(\alpha) = 0$, thus $p(t) \in I_\alpha$. But $I_\alpha = (f_\alpha(t))$, so $p(t) = f_\alpha(t)r(t)$, giving $f_\alpha(t) = f_\alpha(t)r(t)q(t)$ and so $r(t)q(t) = 1$ in $K[t]$, and $q(t)$ is a unit, as required. Recall from GRM that irreducible elements of $K[t]$ are prime and hence generate prime ideals of $K[t]$. So I_α is a prime ideal. □

Definition 1.8. 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 $\beta \in L$.