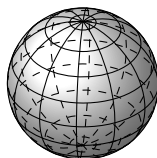


UNIVERSITY OF WATERLOO



PMATH 348
FIELDS AND GALOIS THEORY

PROF. YU-RU LIU • WINTER 2018



Contents

1	INTRODUCTION	1
1.1	Polynomial Equations	1
1.2	Cubic Equations	1
1.3	Quartic Equations	1
1.4	Quintic Equations	1
2	FIELD EXTENSIONS	2
2.1	Degree of Extensions	2
2.2	Algebraic and Transcendental Extensions	3



1 Introduction

1.1 Polynomial Equations

Consider the quadratic equation. Let $ax^2 + bx + c = 0$ with the leading coefficient $a \neq 0$, then we have that,

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

We notice immediately that there are a couple of operations that are involved in this equation.

Definition 1.1.1. An expression involving only addition, subtraction, multiplication, division and radicals is called a radical. These operations are denoted by $+$, $-$, \times , \div and $\sqrt[n]{}$.

The natural question that is raised is the extension to higher dimensions.

1.2 Cubic Equations

All cubic equations can be reduced to the following equation,

$$x^3 + px = q$$

for some $p, q \in \mathbb{C}$. A solution to the above equation is of the form

$$x = \sqrt[3]{\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \sqrt[3]{\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} \quad (\text{Cardano's Formula})$$

1.3 Quartic Equations

A radical solution can be obtained by reducing a quartic to a cubic equation.

1.4 Quintic Equations

- General radical solutions were attempted by Euler, Bézout and Lagrange without success
- In 1799, Ruffini gave a 516 page proof about the unsolvability of quintic equations. His Proof was “almost right”
- In 1824, Abel filled the gap in Ruffini’s proof.

We can now ask ourselves, given a quintic equation, is it solvable by radicals? This question seems to be too hard, so we ask, suppose that a radical solution exists. How does its associated quintic equation look like?

Two main steps in Galois Theory

1. Link a root of a quintic equation, say α to $\mathbb{Q}(\alpha)$, the smallest field containing \mathbb{Q} and α . $\mathbb{Q}(\alpha)$ is a field. So it has more structures to be played with than α ; however, our knowledge of $\mathbb{Q}(\alpha)$ is still too little to answer the question. For example, we do not know how many intermediate fields, E between \mathbb{Q} and $\mathbb{Q}(\alpha)$. What we mean is how many fields E satisfy

$$\mathbb{Q} \subseteq E \subseteq \mathbb{Q}(\alpha).$$

2. Link the field $\mathbb{Q}(\alpha)$ to a group. More precisely, we associate $\mathbb{Q}(\alpha)/\mathbb{Q}$ to the group

$$\text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha)) = \left\{ \Psi : \mathbb{Q}(\alpha) \rightarrow \mathbb{Q}(\alpha) \text{ an isomorphism and } \Psi|_{\mathbb{Q}} = 1_{\mathbb{Q}} \right\}$$

It can be shown that if α is “good”, say algebraic, $\text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha))$ is finite. If α is “very good”, say constructable, the order of $\text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha))$ is in certain forms. Moreover, there is a one-to-one correspondence between the intermediate fields between $\mathbb{Q}(\alpha)$ and \mathbb{Q} and the subgroups of $\text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha))$.

It follows that given some “good” α , we have that the intermediate fields of $\mathbb{Q}(\alpha)$ and \mathbb{Q} are indeed finitely many. This introduces Galois Theory; the interplay between fields and groups.

2 Field Extensions

2.1 Degree of Extensions

Definition 2.1.1. If E is a field containing another field F , we say E is a field extension of F , denoted by E/F .

If E/F is a field extension, we can view E as a vector space over F .

1. Addition: For $e_1, e_2 \in E$, $e_1 + e_2 := e_1 + e_2$ (addition in E)
2. Scalar Multiplication: For $c \in F, e \in E$, $c \cdot e := ce$ (multiplication in E)

Definition 2.1.2. The dimension of E over F (viewed as a vector space) called the degree of E over F , denoted by $[E : F]$. If $[E : F] < \infty$, we say E/F is a finite extension. Otherwise, E/F is an infinite extension.

Example 2.1.3. $[\mathbb{C} : \mathbb{R}] = 2$ is a finite extension since $\mathbb{C} \cong \mathbb{R} + \mathbb{R}i$, with $i^2 = -1$.

Example 2.1.4. Let F be a field. Then $[F(x) : F] = \infty$ since $1, x, x^2, \dots$ are linearly independent over F .

Remark. $F[x] = \{f(x) = a_0 + a_1x + \dots + a_nx^n : a_i \in F, n \in \mathbb{N} \cup \{0\}\}$

Remark. $F(x) = \{\frac{f(x)}{g(x)} : f(x), g(x) \in F[x]\}$

Theorem 1. The E/K and K/F are finite field extensions, then E/F is a finite field extension and

$$[E : F] = [E : K][K : F]$$

In particular, K is an intermediate field of an field extension E/F , then $[K : F] \mid [E : F]$.

Proof. Suppose $[E : K] = m$ and $[K : F] = n$. Let $\{a_i, \dots, a_m\}$ be a basis of E/K and $\{b_1, \dots, b_n\}$ be a basis of K/F . It suffices to show $\{a_ib_j : 1 \leq i \leq m, 1 \leq j \leq n\}$ is a basis of E/F .

Claim. Every element of E is a linear combination of $\{a_ib_j\}$ over F .

For $e \in E$, we have

$$e = \sum_{i=1}^m k_i a_i$$

with $k_i \in K$. Also, for each $k_i \in K$, we have

$$k_i = \sum_{j=1}^n c_{ij} b_j$$

with $c_{ij} \in F$. Thus,

$$e = \sum_{i=1}^m \sum_{j=1}^n c_{ij} b_j a_i.$$

Claim. *The set $\{a_i b_j : 1 \leq i \leq m, 1 \leq j \leq n\}$ is linearly independent over F .*

Suppose that

$$\sum_{i=1}^m \sum_{j=1}^n c_{ij} b_j a_i = 0$$

with $c_{ij} \in F$. Since $\sum_{j=1}^n c_{ij} b_j \in K$ and $\{a_1, \dots, a_m\}$ are independent over K . We have

$$\sum_{j=1}^n c_{ij} b_j = 0.$$

Since $\{b_1, \dots, b_n\}$ are independent over F , we have $c_{ij} = 0$.

Combining both claims, we see that $\{a_i b_j, 1 \leq i \leq m, 1 \leq j \leq n\}$ is a basis of E/F and we have $[E : F] = [E : K][K : F]$. \square

2.2 Algebraic and Transcendental Extensions

Definition 2.2.1. Let E/F be a field extension and $\alpha \in E$. We say α is algebraic over F if there exists $f(x) \in F[x] \setminus \{0\}$ with $f(\alpha) = 0$. Otherwise, α is transcendental over F .

Example 2.2.2. $\frac{e}{d} \in \mathbb{Q}$, $\sqrt{2}$, $\sqrt[3]{7} + 2i$ are algebraic over \mathbb{Q} (see Assignment 1) but e (Hermite, 1873) and π (Lindemann, 1882) are transcendental over \mathbb{Q} .

Let E/F be a field extension and $\alpha \in E$. Let $F[\alpha]$ denote the smallest subfield of E containing F and α . For $\alpha, \beta \in E$, we define $F[\alpha, \beta]$ and $F(\alpha, \beta)$ similarly.

Definition 2.2.3. If $F = F(\alpha)$ for some $\alpha \in E$, we say E is a simple extension of F .

Definition 2.2.4. Let R_1 and R_2 be two rings which contain a field F . A ring homomorphism $\Psi : R_1 \rightarrow R_2$ is said to be a F -homomorphism if $\Psi|_F = 1_F$.

Theorem 2. Let E/F be a field extension and $\alpha \in E$. If α is transcendental over F , then

$$F[\alpha] \cong F[x] \quad \text{and} \quad F(\alpha) \cong F(x)$$

In particular, $F[\alpha] \neq F(\alpha)$.

Remark. In fact, if α is algebraic, indeed $F[\alpha] = F(\alpha)$.

Proof. Let $\Psi : F(x) \rightarrow F(\alpha)$ be the unique F -homomorphism defined by $\Psi(x) = \alpha$. Thus, for $f(x), g(x) \in F[x], g(x) \neq 0$,

$$\Psi\left(\frac{f(x)}{g(x)}\right) = \frac{f(\alpha)}{g(\alpha)} \in F(\alpha).$$

Notice that this is indeed a well-defined map as $g(x) \neq 0$ implies $g(\alpha) \neq 0$ since α is transcendental. Since $F(x)$ is a field and $\ker(\Psi)$ is an ideal of $F(x)$, we have $\ker(\Psi) = F(x)$ or trivial. This $\Psi = 0$ or Ψ is injective. Since $\Psi(x) = \alpha \neq 0$, Ψ must be injective. Also, since $F(x)$ is a field, $\text{Im}\Psi$ contains a field generated by F and α , in other words, $F(\alpha) \subseteq \text{Im}\Psi$. Thus, $\text{Im}\Psi = F(\alpha)$ and Ψ is surjective. It follows that Ψ is an isomorphism and we have

$$F[\alpha] \cong F[x] \quad \text{and} \quad F(\alpha) \cong F(x)$$

□

Theorem 3. Let E/F be a field extension and $\alpha \in E$. If α is algebraic over F , there exists a unique monic irreducible polynomial $p(x) \in F[x]$ such that there exists a F -homomorphism

$$\Psi : F[x]/\langle p(x) \rangle \rightarrow F[\alpha] \quad \text{with } \Psi(x) = \alpha$$

from which we conclude $F[\alpha] \cong F(\alpha)$.

Proof. Consider the unique F -homomorphism $\Psi : F[x] \rightarrow F[\alpha]$ defined by $\Psi(x) = \alpha$. Thus, for $f(x) \in F[x]$, we have $\Psi(f) = f(\alpha)$. Since $F[x]$ is a ring, $\text{Im}\Psi$ contains a ring generated by F and α , in other words, $F[\alpha] \subseteq \text{Im}\Psi$. Thus, $\text{Im}\Psi = F[\alpha]$.

Let

$$I = \text{Ker}\Psi = \{f(x) \in F[x] : f(\alpha) = 0\}.$$

Since α is algebraic, $I \neq \{0\}$. We have $F[x]/I \cong \text{Im}\Psi = F[\alpha] \subseteq F(\alpha)$, a subring of a field $F(\alpha)$. Thus, $F[x]/I$ is an integral domain so I is a prime ideal. It follows that $I = \langle p(x) \rangle$, where $p(x)$ is irreducible. If we assume $p(x)$ is monic, then it is unique. It follows that

$$F[x]/\langle p(x) \rangle \cong F[\alpha].$$

Since $p(x)$ is irreducible, $F[x]/\langle p(x) \rangle$ is a field. So $F[\alpha]$ is a field. It follows that $F[\alpha] = F(\alpha)$. □

Definition 2.2.5. If α is algebraic over a field F , the unique monic polynomial irreducible polynomial $p(x)$ in Theorem 3 is called the minimal polynomial of α over F .

Remark. From the proof of Theorem 3, if $f(x) \in F[x]$ with $f(\alpha) = 0$, then $p(x) \mid f(x)$.

Theorem 4. Let E/F be a field extension and $\alpha \in E$.

1. α is transcendental over F if and only if $[F(\alpha) : F]$ is ∞ .

2. α is algebraic over F if and only if $[F(\alpha) : F] < \infty$.

Moreover, if $p(x)$ is the minimal polynomial of α over F , we have $[F(\alpha) : F] = \deg(p)$ and $\{1, \alpha, \alpha^2, \dots, \alpha^{\deg(p)-1}\}$ is a basis of $F(\alpha)/F$.

Proof. It suffices to prove the forward direction for each statement as the inverse direction implies the other statement.

(1) **Forwards:** From Theorem 2, if α is transcendental over F , then $F(x) \cong F(\alpha)$. In $F(x)$, the elements $\{1, x, x^2, \dots\}$ are linearly independent over F . Thus, $[F(\alpha) : F]$ is ∞ .

(2) **Forwards:** From Theorem 3, if α is algebraic over F , $F[x]/\langle p(x) \rangle \cong F(x)$ with the map $x \mapsto \alpha$. Note that,

$$F[x]/\langle p(x) \rangle \cong \{r(x) \in F[x] : \deg(r) < \deg(p)\} \quad (\deg(0) = -\infty)$$

Thus, $\{1, x, x^2, \dots, x^{\deg(p)-1}\}$ forms a basis for $F[x]/\langle p(x) \rangle$. It follows that $[F(\alpha) : F] = \deg(p)$ and $\{1, \alpha, \alpha^2, \dots, \alpha^{\deg(p)-1}\}$ is a basis of $F(\alpha)/F$. \square

Theorem 5. Let E/F be a field extension. If $[E : F] < \infty$, then there exists $\alpha_1, \dots, \alpha_n \in E$ such that

$$F \subsetneq F(\alpha_1) \subsetneq \dots \subsetneq F(\alpha_1, \dots, \alpha_n) = E.$$