# Galois Theory

October 15, 2019

## 0 A Bit of History, Notation, and Revision

Historically the subject arose from looking at solutions to polynomial equations in one variable over $\mathbb{C}$. The question arose as to whether polynomials could be solved by a formula involving the coefficients and taking roots ("soluble by radicals"). From school, we know that we can solve quadratics in this way with $\frac{-b\pm\sqrt{b^2-4ac}}{2a}$. For a long time it has been known that cubics and quartics have similar, albeit more complicated, formulae for their roots. This was studied by Lagrange in the 1770s. In 1799 Ruffini claimed that there was no general formula in the case of quintics, however there was a gap in his proof. It wasn't until Abel in 1824 that there was a complete accepted proof, using permutations of roots of polynomials. This was the start of group theory.

Galois gave the first explanation of when a quintic was was soluble by radicals or not in 1831, using the structure of a group of permutations of the roots, in particular the importance of normal subgroups. Galois' work was not known until Liouville published his papers in 1846. Liouville realised the connection with Cauchy's work on permutations, but didn't realise the importance of the group-theoretic structure, and in fact few of the contemporary mathematicians did so.

Galois entered his papers for various competitions and also for the entrance process for the École Polytechnique in Paris. He didn't get in however, and went to another university in Paris, where he got involved in politics and eventually killed in a duel. Before the duel he left a 6½ page manuscript setting out his ideas about the future development of the theory. His papers have been carefully studied by Peter Neumann:

The Mathematical Writings of Évariste Galois
History of European Mathematics
European Mathematical Society

This course is presented in a more modern fashion. Rather than thinking about roots of polynomial equations we think about field extensions. Recall from GRM, if $\mathbb{K}$ is a field, and $f$ is an irreducible polynomial in $\mathbb{K}[x]$, then $\mathbb{K}[x]/f$ is also a field.[1]

### Books

There is a historical introduction in I. Stewart's Galois Theory, which is very readable but doesn't quite cover the syllabus. Other books are Artin's Galois Theory; Van der Waerden's Modern Algebra; Lang's Algebra; and Kaplansky's Fields and Rings.

[1] Alternative notation is to use $\mathbb{K}[x]/(f)$, where $(f)$ is the ideal generated by $f$

## Notation / Revision

In this course, a ***ring*** means a commutative ring with a **1**
A ***field*** means a ring in which all non-zero elements have multiplicative inverses, i.e. are units, e.g. $\mathbb{Q}, \mathbb{R}, \mathbb{Z}/\mathbb{Z}_p$ for $p$ prime.
For a ring $R$, $R^X$ is the set of units of $R$, so if $\mathbb{K}$ is a field, we have $\mathbb{K}^X = \mathbb{K} \setminus \{0\}$
$R[x]$ is the ring of polynomials with coefficients in $R$, with variable denoted by $x$[2].

UnderlineExercise: If $R$ is an integral domain then $R[x]$ is an integral domain.

If $\mathbb{K}$ is a field then $\mathbb{K}[x]$ is a Euclidean domain.
If $a, b \in \mathbb{K}[x]$ then $\exists q, r$ such that $a = qb + r$ with $\deg r < \deg b, b \neq 0$

**Corollary 0.1.**

1. $\mathbb{K}[x]$ *is a principal ideal domain (PID)*
2. $\mathbb{K}[x]$ *is a unique factorisation domain (UFD)*
3. *For* $f \in \mathbb{K}[x]$, $f$ *irreducible* $\iff$ $f$ *prime* $\iff$ $(f)$ *is maximal* $\iff$ $\mathbb{K}[x]/(f)$ *is a field*
4. *For* $a, b \in \mathbb{K}[x]$, $(a)+(b)$ *is an ideal and so is of the form* $(g)$ *for some* $g \in \mathbb{K}[x]$. $g = \gcd(a, b)$, *and is unique up to a unit.*
5. *If* $f \in \mathbb{K}[x] \setminus \{0\}$ *then* $f$ *has at most* $\deg f$ *roots in* $\mathbb{K}$.[3]

*Proof.* Left as an exercise □

$\mathbb{K}(x)$ is the ***fraction field*** of $\mathbb{K}[x] \coloneqq \{$equivalence classes $f/g$ where $f/g = r/s \iff fs = gr\}$

# 1 Field Extensions, Algebraic and Transcendental Numbers

## 1.1 Definitions

If $K \subseteq L$ is a subring that is also a field, the $L$ is an ***extension*** of $K$. We write this extension as $L/K$.
e.g. $\mathbb{C}/\mathbb{R}$, $\mathbb{R}/\mathbb{Q}$, $\mathbb{K}[x]/\mathbb{K}$, $L/K$ where $L = K[x]/(f)$, $f$ irreducible.
Observe that, if $L/K$ is a field extension then $L$ can be regarded as a vector space over $K$.

We then define $[L : K] = \dim_K L$, the dimension of the vector space of $L$ over $K$, to be the ***degree*** of the field extension $L/K$. If $[L : K] < \infty$, then it is called a finite field extension, otherwise an infinite field extension.
e.g. $[\mathbb{C} : \mathbb{R}] = 2$, $\mathbb{R}-$basis is $\{1, \mathrm{i}\}$

A field $\mathbb{K}$ always has a smallest subfield. There is a ring homomorphism $\mathbb{Z} \to \mathbb{K}; 1 \mapsto 1$. Either this is injective, in which case we get $\mathbb{Q} \subseteq \mathbb{K}$, and the ***characteristic*** of $\mathbb{K}$ is 0, written $\operatorname{char} \mathbb{K} = 0$, or it is not injective, in which case $1 + 1 + \ldots + 1 = 0$ for some prime number of 1s $p$, and we get $\mathbb{F}_p \subseteq \mathbb{K}$, and the ***characteristic*** of $\mathbb{K}$ is $p$. E.g. $\operatorname{char} \mathbb{F}_p(x) = p$, as $p \cdot 1 = 0$ in $\mathbb{F}_p \subseteq \mathbb{F}_p(x)$.

[2] $= \left\{\sum_{i \geq 0} r_i x^i\right\}$ where all but finitely many $r_i$ are non-zero
[3] We say $\alpha$ is a root of $f \iff f(\alpha) = 0$

$\mathbb{K}$ is a ***finite field*** if $\#\mathbb{K} < \infty$, where $\#\mathbb{K}$ denotes the number of elements of $\mathbb{K}$.

**Lemma 1.1.** *If $F$ is a finite field then* $\operatorname{char} F = p$ *for some prime $p$, and $\#F = p^n$ for some $n \geq 1$.*

*Proof.* If $\#F < \infty$ then the map $\mathbb{Z} \to F$ is not injective, so $\mathbb{F}_p \subseteq F$ and $F$ is a finite dimensional vector space over $\mathbb{F}_p$, and hence as a $\mathbb{F}_p$-vector pace $F \cong \mathbb{F}_p^n$, and hence has $p^n$ elements. □

We'll see later that in fact there is a unique field of $p^n$ elements for each prime $p$ and integer $n \geq 1$

Given a field extension $L/K$ and some $\alpha \in L$, we define $K[\alpha]$ to be the smallest subring of $L$ containing $K$ and $\alpha$, and $K(\alpha)$ to be the smallest such subfield. As such, $K[\alpha] = \{\sum_{i=1}^{N} r_i \alpha : r_i \in K, N \in \mathbb{N}\}$, whilst $K(\alpha) = \{f/g : f, g \in K[\alpha], g \neq 0\}$.

E.g.: $\mathbb{Q}[\mathfrak{i}] = \{a_0 + a_1\mathfrak{i} + a_2\mathfrak{i}^2 + \ldots + a_n\mathfrak{i}^n : a_i \in \mathbb{Q}\} = \{a_0 + a_1\mathfrak{i} : a_0, a_1 \in \mathbb{Q}\}$. This is already a field, so $\mathbb{Q}(\mathfrak{i}) = \mathbb{Q}[\mathfrak{i}]$.

NOTE: If $x$ an indeterminate then we can define a ring homomorphism $\phi : K[x] \to L; x \mapsto \alpha$, and $K[\alpha] = \operatorname{im} \phi$.

$\alpha$ is ***transcendental*** over $K$ if $\phi$ is injective. $\alpha$ is ***algebraic*** over $K$ if $\phi$ is not injective. If $\phi$ is not injective, then $\ker \phi$ is a non-zero ideal, hence $\ker \phi = (f)$ for some $f \in K[x]$ with $f(\alpha) = 0$. If $\phi$ is injective, then the preimage of 0 is exactly $\{0\}$, and so there is no polynomial over $K$ with root $\alpha$. Hence $\alpha$ algebraic over $K$ if and only if there is some polynomial over $K$ with root $\alpha$.

If $\ker \phi = (f)$, then $f$ is the polynomial of least degree such that $f(\alpha) = 0$. Sometimes we also require $f$ to be monic, and call it the ***minimal polynomial*** of $\alpha$ over $K$. We also define the ***degree*** of $\alpha$ over $K$ as $\deg_K \alpha = \deg f$.

$f$ is irreducible - if $f = gh$, then $f(\alpha) = g(\alpha)h(\alpha) = 0$, but $L$ is an integral domain so one of $g, h$ is a smaller polynomial with a zero at $\alpha$ ↯. As such, $f$ has non-zero constant term, and

**Proposition 1.2.** *$\alpha$ is transcendental over $K$ if and only if $\phi : K[x] \to K[\alpha]$ an isomorphism which extends to an isomorphism $K(x) \to K(\alpha)$. In particular, all transcendental extensions $K(\alpha)$ are mutually isomorphic, being isomorphic to $K(x)$.*

To summarise:

**Proposition 1.3.** *Given a field extension $L/K$ and $\alpha \in L$, the following are all equivalent:*

1. *$\alpha$ is algebraic over $K$*
2. *$[K(\alpha) : K] < \infty$*
3. *$\dim_K K(\alpha) < \infty$*
4. *$K[\alpha] = K(\alpha)$*
5. *$K[\alpha]$ is a field*

*When these hold,* $[K(\alpha) : K] = \deg_K \alpha$

*Proof.* Let $d = \deg_K \alpha = \deg f$, where $f$ is the minimal polynomial of $\alpha$ over $K$. Observe $1, \alpha, \alpha^2, \ldots, \alpha^d$ span $K(\alpha)$, and the minimality of the degree of $f$ imply that $1, \alpha, \ldots, \alpha^{d-1}$ are linearly independent. □

## Warnings

1. "Algebraic" and "transcendental" depend on $K$ - e.g. $2\pi\mathfrak{i} \in \mathbb{C}$ is algebraic over $\mathbb{R}$ with minimal polynomial $x^2 = -4\pi^2$, but is transcendental over $\mathbb{Q}$.
2. The minimal polynomial is dependent on $K$ - e.g. $\alpha = \sqrt{\mathfrak{i}} = (1+\mathfrak{i})\frac{\sqrt{2}}{2}$. The minimal polynomial of $\alpha$ over $\mathbb{Q}$ is $x^4+1$, whilst over $\mathbb{Q}(\mathfrak{i})$ it is $x^2 - \mathfrak{i}$. Note that in this example $[\mathbb{Q}(\mathfrak{i}) : \mathbb{Q}] = 2; [\mathbb{Q}(\alpha) : \mathbb{Q}(\mathfrak{i})] = 2; [\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$, and $2 \times 2 = 4$, illustrating the ***tower law***.

**Theorem 1.4** (Tower Law)**.** *Given field extensions $M/L/K$, then $M/L$ is finite if and only if $M/K$ and $L/K$ are finite. In that case, $[M : K] = [M : L][L : K]$.*

This can be deduced from the following proposition:

**Proposition 1.5.** *Suppose $L/K$ is a finite field extension, and $V$ is a vector space over $L$. Then $V$ is finite dimensional over $L$ if and only if $V$ is finite dimensional over $K$ and $\dim_K V = \dim_L V \times [L : K]$*

*Proof that Prop. 1.5 $\implies$ the tower law.* If $L/K$ is not finite then $M/K$ is not a finite extension. Otherwise, apply **1.5** with $V = M$. □

*Proof of Prop. 1.5.* If $\dim_L V = d$, take a $L$-vector space basis of $V$, say $\{\alpha_1, \ldots, \alpha_d\}$, and $K$-vector space basis of $L$, say $\{\ell_1, \ldots, \ell_n\}$. Then $\{\ell_i\alpha_i : 1 \le i \le n, 1 \le j \le d\}$ is a basis for $V$ over $K$:

- Clearly it is a spanning set, as every element $\mu_j \in L$ can be written as $\sum_i^n \lambda_{ij}\ell_i$, so if $v \in V$ is represented as $\sum_j^d \mu_j\alpha_j$ it can also be represented as $\sum_j^d \sum_i^n \lambda_{ij}\ell_i\alpha_j$.
- It is also linearly independent - if $\sum_j^d \sum_i^n \lambda_{ij}\ell_i\alpha_j = 0$, then by independence of the $\alpha_j$ we must have $\sum_i^n \lambda_{ij}\ell_i = 0 \forall j$, and then by independence of the $\ell_i$ we have $\lambda_{ij} = 0 \forall i, j$

Hence, $\dim_K V = n \times d = \dim_L V \times [L : K]$ □

**Corollary 1.6.** *If $L/K$ is a finite extension $\alpha \in L$, then $\alpha$ is algebraic over $K$ and $\deg_K \alpha | [L : K]$.*

*Proof.* Immediate from the Tower Law: $L/K(\alpha)/K$ are field extensions. □

Examples:

1. If $[L : K] = p$, a prime, then $\forall \alpha \in L \setminus K, K(\alpha) = L$, as $[K(\alpha) : K] | p$, so is 1 or $p$. It is not 1 as $\alpha \notin K$, so $[L : K(\alpha)] = 1 \iff L = K(\alpha)$.
2. Every irreducible polynomial $f \in \mathbb{R}[x]$ has degree 1 or 2, as $\mathbb{C}$ is algebraically closed, so $f$ has a root $\alpha \in \mathbb{C}$. $[\mathbb{C} : \mathbb{R}] = 2$, so $[\mathbb{R}(\alpha) : \mathbb{R}] = 1$ or 2, so $\deg f = 1$ or 2.
3. $L = \mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{5})$. Then $[L : \mathbb{Q}] = 12$.

   *Proof.* $L \supseteq \mathbb{Q}(\sqrt[3]{2})$. But $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, since the minimal polynomial is $x^3 - 2$. Similarly $[\mathbb{Q}(\sqrt[4]{5}) : \mathbb{Q}] = 4$, so $3|[L : \mathbb{Q}]$ and $4|[L : \mathbb{Q}]$, hence $12|[L : \mathbb{Q}]$. Now $[L : \mathbb{Q}(\sqrt[3]{2})] \le 4$, since the minimal polynomial $x^4 - 5$ is still a polynomial in $\mathbb{Q}(\sqrt[3]{2})$, and hence $[L : \mathbb{Q}] \le 3 \cdot 4 = 12$, so $[L : \mathbb{Q}] = 12$]. □

4. Let $\omega = e^{2\pi \mathrm{i}/p}$ where $p$ is an odd prime, and let $\alpha = \omega + \omega^{-1} = e^{2\pi \mathrm{i}/p} + e^{-2\pi \mathrm{i}/p}$. What is $\deg_{\mathbb{Q}} \alpha$? Observe that $\omega$ is a root of $f(x) = 1 + x + \ldots + x^{p-1}$, which is irreducible by application of Eisenstein to $f(x+1)$. So $[\mathbb{Q}(\omega) : \mathbb{Q}] = p - 1$. Now clearly $\alpha = \omega + \omega^{-1} \in \mathbb{Q}(\omega)$, so we have field extensions $\mathbb{Q}(\omega)/\mathbb{Q}(\alpha)/\mathbb{Q}$, and hence $\deg_{\mathbb{Q}} \alpha | p - 1$. If we consider $[\mathbb{Q}(\omega) : \mathbb{Q}(\alpha)]$, we can note that $\alpha\omega = \omega^2 + 1$, so $\omega$ is a root of $x^2 - \alpha x + 1$, hence $[\mathbb{Q}(\omega) : \mathbb{Q}(\alpha)] = 1$ or 2. It is not 1 as $\omega \notin \mathbb{Q}(\alpha)$, and so $\deg_{\mathbb{Q}} \alpha = \frac{p-1}{2}$.

**Corollary 1.7.**

1. *$\alpha_1, \alpha_2, \ldots, \alpha_n$ are algebraic over $K$ if and only if $[K(\alpha_1, \alpha_2, \ldots, \alpha_n) : K] < \infty$*
2. *If $\alpha, \beta$ algebraic over $K$ then $\alpha \pm \beta, \alpha\beta, \alpha/\beta$ (if $\beta \neq 0$) are algebraic over $K$.*

*Proof.*

1. $\Longleftarrow$: if $[K(\alpha_1, \ldots, \alpha_n) : K] < \infty$ then $\dim_K K(\alpha_i) < \infty$ so $\alpha_i$ algebraic over $K$.

   $\Longrightarrow$: $\alpha_n$ algebraic over K $\implies$ $\alpha_n$ algebraic over $K(\alpha_1, \ldots, \alpha_{n-1})$
   $\Longrightarrow [K(\alpha_1, \ldots, \alpha_n) : K(\alpha_1, \ldots, \alpha_{n-1})] < \infty$.

   Hence by induction $[K(\alpha_1, \ldots, \alpha_n) : K] < \infty$, as it is product of finitely many finite integers.

2. This is immediate from *1* as $\alpha \pm \beta, \alpha\beta, \alpha/\beta \in K(\alpha, \beta)$, which is a finite extension of $K$.

□

**Corollary 1.8.** *The elements of $L$ which are algebraic over $K$ form a subfield of $L$.*

Example: Let $a, b \in K$, and set $\alpha = \sqrt{a}, \beta = \sqrt{b}$. Let's try to define a polynomial satisfied by $\alpha + \beta = \gamma$. Compare powers of $\gamma$ and use that $\alpha^2 = a, \beta^2 = b$ to simplify and look for linear relationships.

$$\begin{aligned} \gamma^2 &= \alpha^2 + 2\alpha\beta + \beta^2 = a + b + 2\alpha\beta \\ \gamma^4 &= (a+b)^2 + 4\alpha\beta(a+b) + 4\alpha^2\beta^2 \\ &= a^2 + 6ab + b^2 + 4\alpha\beta(a+b) \\ \therefore \gamma^4 - 2(a+b)\gamma^2 &= -(a-b)^2 \end{aligned}$$

So $\gamma$ is a root of $x^4 - 2(a+b)x^2 + (a-b)^2$

Note that if $\deg_K \alpha = m, \deg_\alpha \beta = n$ then $K(\alpha, \beta)$ is spanned over $K$ by monomials $\alpha^i \beta^j$ for $0 \leq i < m, 0 \leq j < n$. Hence for any $\gamma \in K(\alpha, \beta)$, the terms $1, \gamma, \ldots, \gamma^{mn}$ must be linear combinations over $K$ over the monomials $\alpha^i \beta^j$, and, as there are $mn + 1$ of them they must be linearly dependent over $K$. However, they polynomial satisfied by $X$ obtained in this way is in general not going to be the minimal polynomial.

Exercise: Show that, if $m, n$ and $mn$ are elements of $\mathbb{Q}$ and are not squares, then $[\mathbb{Q}(\sqrt{m} + \sqrt{n}) : \mathbb{Q}] = 4$.

An extension $L/K$ is an ***algebraic extension*** if every $\alpha \in L$ is algebraic over $K$.

Example: $\bar{\mathbb{Q}} \coloneqq \{\alpha \in \mathbb{C} : \alpha \text{ algebraic over } \mathbb{Q}\}$ is an algebraic extension of $\mathbb{Q}$, but is not a finite extension of $\mathbb{Q}$, as $\sqrt[n]{2} \in \bar{\mathbb{Q}}$ so $[\bar{\mathbb{Q}} : \mathbb{Q}] \geq n$ for all integers $n$.

**Proposition 1.9.**

1. *A finite extension is algebraic*
2. *$K(\alpha)/K$ is an algebraic extension $\implies$ $\alpha$ is algebraic over $K$*
3. *If $M/L/K$ are extensions then $M/K$ is algebraic if and only if $M/L$ and $L/K$ are algebraic*