Introduction to Galois theory

by

Jens Hee
https://jenshee.dk

December 2021

Change log

10. December 2021

1. Document started.

Contents

1 Introduction 2
1.1 Algebraic numbers 2

2 Polynomials and Extension fields 4
2.1 Polynomials 4
2.2 Fields 4
2.3 Extension fields 4

3 Galois Theory 6
3.1 Splitting fields 6
3.1.1 Examples 6
3.2 Mappings 7
3.3 Galois extension 7
3.3.1 Examples 7
3.4 The Galois main theorem 9

4 Solving by radicals 10

5 Appendix A 11
5.1 Number of automorphisms 11
5.2 Separable polynomials 11
5.3 Abstract fields 12
5.4 Uniqueness of irreducible polynomials 12
5.5 Minimal polynomial 12

Chapter 1

Introduction

The Galois theory is named after the french mathematician Évariste Galois (1811- 1832). He died in a duel at the age of 20 and finalized his work the night before. He was in particular interested in the study of polynomials with rational coefficients and their factorization. The theory provides a connection between field theory and group theory and can be used to explain when the roots of a polynomial with rational coefficients can be expressed by radicals, i.e. when the solution can be expressed by a formula involving only rational numbers, n'th roots, and the four basic arithmetic operations. In fact polynomials of degree more than four cannot be solved by radicals. Moreover the theory can be used to explain why the classical problems trisecting the angle, squaring the circle and doubling the cube are impossible to solve. The theory about finite fields are also named after him. This theory is not covered by this paper.

A central part of Galois theory is the relation between the so called extension fields and groups. Fields are defined as sets where addition, subtraction, multiplication and division are defined. The set of rational numbers, real numbers and complex numbers are all examples of fields. The roots of polynomials with rational coefficients form a field called algebraic numbers.

Groups are defined as sets with a binary operation that is associative. A group has an identity element and every element has an inverse. In Galois theory an element of a group is a mapping of a field extensions to itself.

This paper does not cover all the details of Galois theory, but will hopefully give an introduction making it easier to dig deeper into the subject.

Throughout this paper it is assumed that polynomials have rational coefficients, but the theory also cover the case where the polynomials have coefficients in other fields.

1.1 Algebraic numbers

A number α is called algebraic if it is the root of a polynomial $p(x)$ with rational coefficients. As mentioned above algebraic is not restricted to the case where the polynomials have rational coefficients, but often it is implied.

Examples are:

$$\begin{aligned} \alpha = \sqrt{2} &\quad p(x) = x^2 - 2 \\ \alpha = \sqrt[3]{1+\sqrt{7}} &\quad p(x) = (x^3-1)^2 - 7 \\ \alpha = \cos(\tfrac{2\pi}{7}) &\quad p(x) = 8x^3 + 4x^2 - 4x - 1 \end{aligned}$$

To see that $\cos(\frac{2\pi}{7})$ is in fact a root of $8x^3 + 4x^2 - 4x - 1$ we have:

$$\begin{array}{lcccccl} \cos\frac{2\pi}{7} & = & \frac{\xi+\xi^{'}}{2} & & & = & \alpha, \qquad \xi = e^{\frac{2\pi i}{7}} \\ \cos^2\frac{2\pi}{7} & = & (\frac{\xi+\xi^{'}}{2})^2 & = & \frac{\xi^2+\xi^{'2}+2}{4} & = & \alpha^2 \\ \cos^3\frac{2\pi}{7} & = & (\frac{\xi+\xi^{'}}{2})^3 & = & \frac{\xi^3+\xi^{'3}+3(\xi+\xi^{'})}{8} & = & \alpha^3 \end{array}$$

or

$$\begin{array}{lcl} \xi + \xi^{'} & = & 2\alpha \\ \xi^2 + \xi^{'2} & = & 4\alpha^2 - 2 \\ \xi^3 + \xi^{'3} & = & 8\alpha^3 - 6\alpha \end{array}$$

since

$$\begin{array}{ccccccccccccccc} 1 & + & \xi & + & \xi^2 & + & \xi^3 & + & \xi^4 & + & \xi^5 & + & \xi^6 & = & 0 \\ \xi^{-3} & + & \xi^{-2} & + & \xi^{-1} & + & 1 & + & \xi^1 & + & \xi^2 & + & \xi^3 & = & 0 \end{array}$$

$$8\alpha^3 - 6\alpha + 4\alpha^2 - 2 + 2\alpha + 1 = 0$$

$$8\alpha^3 + 4\alpha^2 - 4\alpha - 1 = 0$$

Substituting $\alpha = x + \beta$ the square part can be eliminated and we get:

$$x^3 - \frac{7}{12}x - \frac{7}{216} = 0$$

and we have the solution:

$$\cos(\frac{2\pi}{7}) = -\frac{1}{6} + \frac{1}{6}\sqrt[3]{\frac{7}{2}}\left(\sqrt[3]{1 + i3\sqrt{3}} + \sqrt[3]{1 - i3\sqrt{3}}\right)$$

Note that although $\cos(\frac{2\pi}{7})$ is real it cannot be written using radicals without complex notation. This is called casus irreducibilis.

Chapter 2

Polynomials and Extension fields

2.1 Polynomials

A polynomial of degree n has n roots in the field C, but they need not be distinct. The set of all polynomials with coefficients in the field K are given by $K[x]$. When dealing with polynomials in $K[x]$, the roots are not restricted to be in K although the coefficients are. A polynomial of degree n may be irreducible over say K, but is still regarded as having n roots over some extension field. An irreducible polynomial over K cannot be factored into polynomials with coefficients i K. The polynomial $x^4+4x^3-x^2-8x-2$ is not irreducible since it can be factored as $(x^2+4x+1)(x^2-2)$ whereas the polynomial x^2+4x+1 is irreducible since it has no rational roots, it has on the other hand the real roots $-2+\sqrt{3}$ and $-2-\sqrt{3}$. If two irreducible polynomials have a root in common they have all roots in common.

2.2 Fields

A field is a set where addition, subtraction, multiplication and division are defined. They are denoted by capital letters e.g. K, L and M. The following letters have a special meaning: Q rational numbers, R real numbers, C complex numbers, all being fields.

2.3 Extension fields

A field L is an extension field of the field K, if $K \subset L$. If a field is extended by an element say $\sqrt{2} \in R$ then the extension L/K becomes:

$$\{x|x = a + b\sqrt{2}, a, b \in K\}$$

The field extension is said to have degree 2. If on the other hand the field is extended by $\sqrt[3]{2}$ it becomes:

$$\{x|x = a + b\sqrt[3]{2} + c\sqrt[3]{2}^2, a, b, c \in K\}$$

and the degree of the extension is said to be 3.

Definition 2.1 The field extension L/K is said to be finite with degree n, if L can be seen as a vector space over K with degree n. In order to emphasize that the field L is an extension field over K it is written L/K. The degree of the extension field L/K is written $[L:K]$.

In the first example above the degree of the extension field is 2 since a and b can be viewed as the coordinates of a two dimensional vector space having $\{1, \sqrt{2}\}$ as the basis. In the second example example above the extension field viewed as a vector has the basis $\{1, \sqrt[3]{2}, \sqrt[3]{2}^2, \}$. It is thus clear that the degree of the extension field depends on the element added.

Definition 2.2 If a polynomial $p(x) \in K[x]$, has a root α, then α is said to be algebraic over K. See also the section "Algebraic numbers" for examples.

Theorem 2.1 α is algebraic over K if and only if it is an element of a finite extension field L/K of degree n.

Proof 2.1a Let α be a root of the irreducible polynomial $p(x)$ of degree n. The ring of polynomials $K[x]$ modulo p(x) form a field of degree n, see Appendix A, α is an element of this field by letting $x \to \alpha$.

Proof 2.1b If an extension field L/K has degree n and it has the element α then L/K can be seen as a vector space over K with dimension n. A non trivial linear combination of n elements of L is thus not zero:

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \quad + a_1\alpha = -a_0 \quad a_0 \neq 0$$

showing that an element $\alpha \in L$ is a root of a polynomial of degree n with coefficients in K.

Theorem 2.2 If α and β are algebraic over K then so are $\alpha + \beta$, $\alpha - \beta$, $\alpha * \beta$ and α/β.

Theorem 2.3 A polynomial with algebraic coefficients has algebraic roots.

Chapter 3

Galois Theory

3.1 Splitting fields

In order to study the roots of a polynomial a field is extended by all the roots of the polynomial. Such an extension field is called a splitting field if it is the minimal field containing the roots. It is separable meaning it has no multiple roots (this is always the case for polynomials with rational coefficients). A splitting field is also normal meaning it contains all the roots of the polynomial. The degree of the splitting field M/K is $n \leq [M : K] \leq n!$ where n is the degree of the polynomial, n always divides $[M : K]$.

3.1.1 Examples

Example 1 The polynomial $x^2 - 2$ has the roots $\pm\sqrt{2}$. Adjoining $\sqrt{2}$ to Q gives a splitting field of degree 2:

$$\{x|x = a + b\sqrt{2}, a, b \in Q\}$$

Note that the field automatically contains the other root $-\sqrt{2}$. It shows that the symmetry of the roots affect the splitting field.

Example 2 The polynomial $x^3 - 2$ has the roots $\sqrt[3]{2}$, $\sqrt[3]{2}e^{\frac{i2\pi}{3}}$ and $\sqrt[3]{2}e^{\frac{i2\pi}{3}2}$. One of the roots is real and construction of a splitting field based on this root alone fails since this gives the field extension:

$$\{x|x = a + b\sqrt[3]{2} + c\sqrt[3]{2}^2, a, b, c \in Q\}$$

This is a extension field, but not a splitting field since it does not contain the complex roots.
It is often convenient to base the extension field on parameters derived from the roots. With $\omega = e^{\frac{i2\pi}{3}}$, the two complex roots can be written: $z1 = \omega\sqrt[3]{2}$ and $z2 = \omega\sqrt[3]{2}^2$. Using $\omega^2 = -\omega - 1$ we have $z1 + z2 = -\sqrt[3]{2}$ and we do not need $z2$ for constructing the field extension that is $Q(\sqrt[3]{2}, \omega)$ gives the splitting field:

$$\{x|x = a + b\sqrt[3]{2} + c\sqrt[3]{2}^2 + d\omega + e\omega\sqrt[3]{2} + f\omega\sqrt[3]{2}^2, a, b, c, d, e, f \in Q\}$$

Note that although the polynomial has degree 3, the splitting field has degree 6.

Example 3 The polynomial $(x^2-2)(x^2-3)$ has the roots $\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}$. The extension field containing $\sqrt{2}$ and $\sqrt{3}$ also contains $-\sqrt{2}$ and $\sqrt{2}$, but it must also contain $\sqrt{6}$ since all products of elements must also be contained in order to form a field. the splitting field is:

$$\{x|x = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}, a, b, c, d \in Q\}$$

Example 4 The polynomial $x^4 - 2$ has the roots $\sqrt[4]{2}$, $i\sqrt[4]{2}$, $-\sqrt[4]{2}$ and $-i\sqrt[4]{2}$ and the splitting field:

$$\{x|x = a + b\sqrt[4]{2} + c\sqrt{2} + d\sqrt[4]{2}^3 + ei + fi\sqrt[4]{2} + gi\sqrt{2} + hi\sqrt[4]{2}^3, a, b, c, d, e, f, g, h \in Q\}$$

Example 5 The polynomial $x^3 + 4x^2 - 4x - 1$ has the roots $cos(\frac{2\pi}{7}), cos(\frac{2\pi 2}{7}), cos(\frac{2\pi 3}{7})$ and the splitting field is:

$$\{x|x = a + b\alpha + c\alpha^2, a, b, \in Q\}$$

where $\alpha = cos(\frac{2\pi}{7})$

3.2 Mappings

An isomorphic mapping ϕ of V_1 to V_2 is a mapping with the following rules:

1. If a and b are distinct element of V_1 then $\phi(a)$ and $\phi(b)$ are distinct elements of V_2
2. If a is an element of V_2 then there is a unique element b of V_1 where $\phi(b) = a$
3. The mapping must preserve the structure of V_1. This implies that for a field $\phi(a+b) = \phi(a) + \phi(b)$ and that $\phi(ab) = \phi(a)\phi(b)$.

An automorphism is an isomorphic mapping where $V_1 = V_2$.

3.3 Galois extension

A Galois extension M/K, is a field extension based of a splitting field. There are exactly $[M : K]$ automorphisms mapping the splitting field to itself including the identity mapping, see chapter "The Galois main theorem". The set of automorphisms is called a Galois group.
Each automorphism maps every element of K itself. Therefore K is called the fixed field of the extension. It is clear that the roots are mapped to other roots since:

$$p(\alpha) = a_n\alpha^n + a_{n-1}\alpha^{n-1} + ... + a_0 = 0$$

$$p(\sigma(\alpha)) = a_n\sigma(\alpha)^n + a_{n-1}\sigma(\alpha)^{n-1} + ... + a_0 = 0$$

showing that the mapping of the root α is root. A root is never mapped to itself by all automorphisms since a splitting field does not contain multiple roots.

3.3.1 Examples

In all examples σ_1 is the identity mapping.

Example 1 $x^2 - 2$:

$\sigma_2(\sqrt{2} \to -\sqrt(2)$

Example 2 $x^3 - 2$

$\sigma_2(\sqrt[3]{2}) \to \omega\sqrt[3]{2}$
$\sigma_2(\omega\sqrt[3]{2}) \to \omega^2\sqrt[3]{2}$
$\sigma_2(\omega^2\sqrt[3]{2}) \to \sqrt[3]{2}$
$\sigma_3(\sqrt[3]{2}) \to \sqrt[3]{2}$
$\sigma_3(\omega\sqrt[3]{2}) \to \omega^2\sqrt[3]{2}$
$\sigma_4 = \sigma_1 \circ \sigma_1$
$\sigma_5 = \sigma_1 \circ \sigma 1 \circ \sigma 1$
$\sigma_6 = \sigma_1 \circ \sigma_2$

Example 3 $(x^2 - 2)(x^2 - 3)$

$\sigma_2(\sqrt{2}) \to -\sqrt{2}$
$\sigma_3(\sqrt{3}) \to \sqrt{3}$
$\sigma_4(\sqrt{6}) \to -\sqrt{6}$
$\sigma_3(\sqrt{2}) \to \sqrt{2}$
$\sigma_3(\sqrt{3}) \to -\sqrt{3}$
$\sigma_3(\sqrt{6}) \to -\sqrt{6}$
$\sigma_4 = \sigma_2 \circ \sigma_3$
Note that $\sigma 4(\sqrt{6}) = \sigma 2(\sqrt{6}\sigma 3\sqrt{6}) = \sigma 2(\sqrt{2})\sigma 2(\sqrt{3})\sigma 3(\sqrt{2})\sigma 3(\sqrt{3}) \to (-\sqrt{2})\sqrt{3}\sqrt{2})(-\sqrt{3})) = \sqrt{6}$

Example 4 $x^4 - 2$

$\sigma_2(\sqrt[4]{2}) \to i\sqrt[4]{2}$
$\sigma_2(i\sqrt[4]{2}) \to -\sqrt[4]{2}$
$\sigma_2(-\sqrt[4]{2}) \to -i\sqrt[4]{2}$
$\sigma_2(-i\sqrt[4]{2}) \to \sqrt[4]{2}$
$\sigma_3(\sqrt[4]{2}) \to \sqrt[4]{2}$
$\sigma_3(-\sqrt[4]{2}) \to -\sqrt[4]{2}$
$\sigma_3(i\sqrt[4]{2}) \to -i\sqrt[4]{2}$
$\sigma_4 = \sigma_1 \circ \sigma 1$
$\sigma_5 = \sigma_1 \circ \sigma 1 \circ \sigma 1$
$\sigma_6 = \sigma_4 \circ \sigma 1$
$\sigma_7 = \sigma_4 \circ \sigma 3$
$\sigma_8 = \sigma_4 \circ \sigma 4$

Example 5 $x^3 + 4x^2 - 4x - 1$

Let $\alpha = cos(\frac{2\pi}{7})$ then the roots of the polynomial are given by: $r1 = 2\alpha^2 - 1, r2 = \alpha, r3 = 4\alpha^3 - 3\alpha$,
$\sigma_2(r1) \rightarrow r2$
$\sigma_2(r2) \rightarrow r3$
$\sigma_2(r3) \rightarrow r1$
$\sigma_3(r2) \rightarrow r3$
$\sigma_3(r3) \rightarrow r2$

3.4 The Galois main theorem

Given is a finite Galois extension M/K and the corresponding Galois group $G = Gal(M/K)$, with a sub group H and

$$M^H = \{x \in M | \sigma(x) = x, \forall \sigma \in H\}$$

$$Gal(M/L) = (\{\sigma \in G | \sigma(x) = x, \forall x \in L\}$$

then there is an intermediate field $K \subset L \subset M$ where:

$$H \rightarrow M^H = L \quad \text{and} \quad L \rightarrow Gal(M/L) = H$$

are inverses and the maps induce a bijection between the normal subgroups of G and the normal, intermediate extensions of M/K.

$$L \longrightarrow Gal(M/L) \longrightarrow M^{Gal(M/L)} = L$$

$$H \longrightarrow M^H \longrightarrow Gal(M/M^H) = H$$

Since M/K is a Galois extension and thereby a splitting field of $p(x)$, M/L is also a Galois extension, since $p(x)$ has coefficients in K and thereby also in L. $Gal(M/L)$ is thus a Galois group and can only fix L ($p(x)$ has no multiple roots). Therefore:

$$[M : L] = |Gal(M/L)| = H$$

Since G is a Galois group then since H is a subgroup of G it is also a Galois group. Hence M^H is a Galois extension and can only be fixed by H. Therefore:

$$|H| = |M^H|$$

This means that there exists a bijection between the sub fields of a Galois extension and the subgroups of a Galois group.

Chapter 4

Solving by radicals

Chapter 5

Appendix A

5.1 Number of automorphisms

The number of automorphisms $Gal(M/K)| = |G|$ is equal to the degree of the splitting field. A primitive element of the splitting field has a minimal polynomial. The degree of the minimal polynomial is equal to the degree of the splitting filed. Each automorphism maps the primitive element to a root in the minimal polynomial. Consequently the number of automorphisms is equal to the degree of the splitting field. As a consequence:

$$|H| = [M : M^H] = [M : L]$$

We have now established the foundation of the Galois theory. It is seen that it makes it possible to transform a problem from the field extension to a problem of a group and we can use the theory about groups to solve problems about polynomials and their roots.
One problem is to prove that polynomials of degree higher than 4 cannot be solved by radicals in general. The problem is formulated based on extension fields and solved by group theory. The result is that it is not possible in general see chapter "Solving by radicals".

5.2 Separable polynomials

Theorem 1 A polynomial is separable if it has no multiple roots. All irreducible polynomials with rational coefficients are separable. If $p = p_1 p_2 ...$ then all factors are separable.

Proof 1 If a polynomial $p(x) \in Q[x]$ has multiple root in an extension then:

$$p(x) = (x - \alpha)^p h(x)$$

$$p'(x) = n(x - \alpha)^{p-1} h(x) + (x - \alpha)^p h'(x) +$$

This shows that $p(x)$ and $p'(x)$ have a common root. If the minimal polynomial of α is $m(x)$ then:

$$p(x) = g(x)m(x)$$

$$p'(x) = r(x)m(x)$$

Since:

$$1 < deg(p'(x)) < deg(p(x))$$

then

$$1 < deg(r(x)) < deg(g(x))$$

and

$$2 \leq deg(g(x))$$

$p(x)$ is thus not irreducible.

5.3 Abstract fields

Example 2.1 The polynomial $3x^2+x+1$ is irreducible within the rational numbers consequently:

$$\frac{x-2}{x+1} = 3x - 1 \quad \text{mod } 3x^2 + x + 1$$

since

$$(3x-1)(x+1) = Q(x)(3x^2+x+1) + x - 2, \qquad\qquad Q(x) = 1$$

5.4 Uniqueness of irreducible polynomials

Theorem 2 Two irreducible polynomials $p(x)$ and $g(x)$ with rational coefficients have no common root in any field extension of Q unless $p(x) = kg(x)$.
If $p(x)$ and $g(x)$ are relatively prime then we can write:

$$p(x)u(x) + g(x)v(x) = 1$$

for some $u(x)$ and $v(x)$ in $Q[x]$. If there were an α in a field extension of Q which is a common root of $p(x)$ $g(x)$, then substituting α for x in the above polynomial identity makes the left side 0 while the right side is 1. This is a contradiction, so $p(x)$ $g(x)$ have no common root in any field extension of Q.

5.5 Minimal polynomial

Example The extension $Q(\sqrt{2}+\sqrt{3})$ has degree of at most 4. The minimal polynomial of $\sqrt{2}+\sqrt{3}$ can be found as:

$$x = \sqrt{2}+\sqrt{3}$$
$$x^2 = 5 + 2\sqrt{6}$$
$$x^2 - 5 = 2\sqrt{6}$$
$$(x^2-5)^2 = 24$$
$$x^4 - 10x^2 + 1 = 0$$

The polynomial of degree 4 $x^4 - 10x^2 + 1$ is thus the minimal polynomial of $\sqrt{2}+\sqrt{3}$.