

Galois Theory notes

arnaucube

2025

Abstract

Notes taken while studying Galois Theory, mostly from Ian Stewart's book "Galois Theory" [1].

Usually while reading books and papers I take handwritten notes in a notebook, this document contains some of them re-written to *LaTeX*.

The notes are not complete, don't include all the steps neither all the proofs.

Contents

1	Recap on the degree of field extensions	1
2	Tools	4
2.1	De Moivre's Theorem and Euler's formula	4
2.2	Eisenstein's Criterion	4
2.3	Elementary symmetric polynomials	4
2.4	Cyclotomic polynomials	4
2.5	Lemma 1.42 from J.S.Milne's book	5
2.6	Dihedral groups - Groups of symmetries	5
3	Exercises	7
3.1	Galois groups	7
3.1.1	t6-7	7

1 Recap on the degree of field extensions

(Definitions, theorems, lemmas, corollaries and examples enumeration follows from Ian Stewart's book [1]).

Definition 4.10. A *simple extension* is $L : K$ such that $L = K(\alpha)$ for some $\alpha \in L$.

Example 4.11. Beware, $L = \mathbb{Q}(i, -i, \sqrt{5}, -\sqrt{5}) = \mathbb{Q}(i, \sqrt{5}) = \mathbb{Q}(i + \sqrt{5})$.

Definition 5.5. Let $L : K$, suppose $\alpha \in L$ is algebraic over K . Then, the *minimal polynomial* of α over K is the unique monic polynomial m over K , $m(t) \in K[t]$, of smallest degree such that $m(\alpha) = 0$.
eg.: $i \in \mathbb{C}$ is algebraic over \mathbb{R} . The minimal polynomial of i over \mathbb{R} is $m(t) = t^2 + 1$, so that $m(i) = 0$.

Lemma 5.9. Every polynomial $a \in K[t]$ is congruent modulo m to a unique polynomial of degree $< \delta m$.

Proof. Divide a/m with remainder, $a = qm + r$, with $q, r \in K[t]$ and $\delta r < \delta m$. Then, $a - r = qm$, so $a \equiv r \pmod{m}$.

It remains to prove uniqueness.

Suppose $\exists r \equiv s \pmod{m}$, with $\delta r, \delta s < \delta m$. Then, $r - s$ is divisible by m , but has smaller degree than m .

Therefore, $r - s = 0$, so $r = s$, proving uniqueness. \square

Lemma 5.14. Let $K(\alpha) : K$ be a simple algebraic extension, let m be the minimal polynomial of α over K , let $\delta m = n$.

Then $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ is a basis for $K(\alpha)$ over K . In particular, $[K(\alpha) : K] = n$.

Definition 6.2. The degree $[L : K]$ of a field extension $L : K$ is the dimension of L considered as a vector space over K .

Equivalently, the dimension of L as a vector space over K is the number of terms in the expression for a general element of L using coefficients from K .

Example 6.3. 1. \mathbb{C} elements are 2-dimensional over \mathbb{R} ($p + qi \in \mathbb{C}$, with $p, q \in \mathbb{R}$), because a basis is $\{1, i\}$, hence $[\mathbb{C} : \mathbb{R}] = 2$.

2. $[\mathbb{Q}(i, \sqrt{5}) : \mathbb{Q}] = 4$, since the elements $\{1, \sqrt{5}, i, i\sqrt{5}\}$ form a basis for $\mathbb{Q}(i, \sqrt{5})$ over \mathbb{Q} .

Theorem 6.4. (*Short Tower Law*) If $K, L, M \subseteq \mathbb{C}$, and $K \subseteq L \subseteq M$, then $[M : K] = [M : L] \cdot [L : K]$.

Proof. Let $(x_i)_{i \in I}$ be a basis for L over K , let $(y_j)_{j \in J}$ be a basis for M over L . $\forall i \in I, j \in J$, we have $x_i \in L, y_j \in M$.

Want to show that $(x_i y_j)_{i \in I, j \in J}$ is a basis for M over K .

i. prove linear independence:

Suppose that

$$\sum_{ij} k_{ij} x_i y_j = 0 \quad (k_{ij} \in K)$$

rearrange

$$\sum_j \underbrace{\left(\sum_i k_{ij} x_i \right)}_{\in L} y_j = 0 \quad (k_{ij} \in K)$$

Since $\sum_i k_{ij} x_i \in L$, and the $y_j \in M$ are linearly independent over L , then $\sum_i k_{ij} x_i = 0$.

Repeating the argument inside $L \longrightarrow k_{ij} = 0 \quad \forall i \in I, j \in J$.
 So the elements $x_i y_j$ are linearly independent over K .

ii. prove that $x_i y_j$ span M over K :

Any $x \in M$ can be written $x = \sum_j \lambda_j y_j$ for $\lambda_j \in L$, because y_j spans M over L . Similarly, $\forall j \in J, \lambda_j = \sum_i \lambda_{ij} x_i y_j$ for $\lambda_{ij} \in K$.

Putting the pieces together, $x = \sum_{ij} \lambda_{ij} x_i y_j$ as required.

□

Lemma 6.6. (*Tower Law*)

If $K_0 \subseteq K_1 \subseteq \dots \subseteq K_n$ are subfields of \mathbb{C} , then

$$[K_n : K_0] = [K_n : K_{n-1}] \cdot [K_{n-1} : K_{n-2}] \cdot \dots \cdot [K_1 : K_0]$$

Proof. From 6.4.

□

[...]

2 Tools

This section contains tools that I found useful to solve Galois Theory related problems, and that don't appear in Stewart's book.

2.1 De Moivre's Theorem and Euler's formula

Useful for finding all the roots of a polynomial.

Euler's formula:

$$e^{i\psi} = \cos\psi + i \cdot \sin\psi$$

The n -th roots of a complex number $z = x + iy = r(\cos\theta + i \cdot \sin\theta)$ are given by

$$z_k = \sqrt[n]{r} \cdot \left(\cos\left(\frac{\theta + 2k\pi}{n}\right) + i \cdot \sin\left(\frac{\theta + 2k\pi}{n}\right) \right)$$

for $k = 0, \dots, n - 1$.

So, by Euler's formula:

$$z_k = \sqrt[n]{r} \cdot e^{i\left(\frac{\theta + 2k\pi}{n}\right)}$$

2.2 Eisenstein's Criterion

reference: Stewart's book

Let $f(t) = a_0 + a_1t + \dots + a_nt^n$, suppose there is a prime q such that

1. $q \nmid a_n$
2. $q | a_i$ for $i = 0, \dots, n - 1$
3. $q^2 \nmid a_0$

Then, f is irreducible over \mathbb{Q} .

TODO proof & Gauss lemma.

2.3 Elementary symmetric polynomials

TODO from orange notebook, page 36

2.4 Cyclotomic polynomials

TODO theory from brown muji notebook, page 82

Examples:

$$\Phi_n(x) = x^{n-1} + x^{n-2} + \dots + x^2 + x + 1 = \sum_{i=0}^{n-1} x^i$$

$$\Phi_{2p}(x) = x^{p-1} + \dots + x^2 - x + 1 = \sum_{i=0}^{p-1} (-x)^i$$

$$\Phi_m(x) = x^{m/2} + 1, \text{ when } m \text{ is a power of } 2$$

2.5 Lemma 1.42 from J.S.Milne's book

TODO add reference to Milne's book

Useful for when dealing with $x^p - 1$ with p prime.

Observe that

$$x^p - 1 = (x - 1)(x^{p-1} + x^{p-2} + \dots + 1)$$

Notice that

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \dots + 1$$

is the p -th Cyclotomic polynomial.

Lemma 1.42. If p prime, then $x^{p-1} + \dots + 1$ is irreducible; hence $\mathbb{Q}[e^{2\pi i/p}]$ has degree $p - 1$ over \mathbb{Q} .

Proof. Let $f(x) = (x^p - 1)/(x - 1) = x^{p-1} + \dots + 1$ then

$$f(x+1) = \frac{(x+1)^p - 1}{x+1-1} = \frac{(x+1)^p - 1}{x} = x^{p-1} + \dots + a_i x^i + \dots + p$$

$$\text{with } a_i = \binom{p}{i+1}.$$

We know that $p \nmid a_i$ for $i = 1, \dots, p-2$, therefore $f(x+1)$ is irreducible by Eisenstein's Criterion.

This implies that $f(x)$ is irreducible. □

2.6 Dihedral groups - Groups of symmetries

Source: Wikipedia and [2].

Dihedral groups (\mathbb{D}_n) represent the symmetries of a regular n -gon.

Properties:

- are non-abelian (for $n > 2$), ie. $rs \neq sr$
- order $2n$
- generated by a rotation r and a reflexion s
- $r^n = s^2 = id, \quad (rs)^2 = id$

Subgroups of \mathbb{D}_n :

- rotation form a cyclic subgroup of order n , denoted as $\langle r \rangle$
- for each d such that $d|n$, $\exists \mathbb{D}_d$ with order $2d$
- normal subgroups
 - for n odd: \mathbb{D}_n and $\langle r^d \rangle$ for every $d|n$
 - for n even: 2 additional normal subgroups
- Klein four-groups: $\mathbb{Z}_2 \times \mathbb{Z}_2$, of order 4

Total number of subgroups in \mathbb{D}_n : $d(n) + s(n)$, where $d(n)$ is the number of positive divisors of n , and $s(n)$ is the sum of those divisors.

Example . For \mathbb{D}_6 , we have $\{1, 2, 3, 6\}|6$, so $d(n) = d(6) = 4$, and $s(6) = 1+2+3+6 = 12$; henceforth, the total amount of subgroups is $d(n)+s(n) = 4+12 = 16$.

For $n \geq 3$, $\mathbb{D}_n \subseteq \mathbb{S}_n$ (subgroup of the Symmetry group).

3 Exercises

3.1 Galois groups

3.1.1 $t^6 - 7 \in \mathbb{Q}$

This exercise comes from a combination of exercises 12.4 and 13.7 from [1].

First let's find the roots. By De Moivre's Theorem (2.1), $t_k = \sqrt[6]{7} \cdot e^{i \frac{2\pi k}{6}}$.

From which we denote $\alpha = \sqrt[6]{7}$, and $\zeta = e^{i \frac{2\pi}{6}}$, so that the roots of the polynomial are $\{\alpha, \alpha\zeta, \alpha\zeta^2, \alpha\zeta^3, \alpha\zeta^4, \alpha\zeta^5\}$, ie. $\{\alpha\zeta^k\}_0^5$.

Hence the *splitting field* is $\mathbb{Q}(\alpha, \zeta)$.

Degree of the extension

In order to find $[\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}]$, we're going to split it in tow parts. By the Tower Law (6.6),

$$[\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}]$$

To find each degree, we will find the minimal polynomial of the adjoined term over the base field of the extension:

- i. minimal polynomial of α over \mathbb{Q}

By Einsenstein's Criterion (2.2), with $q = 7$ we have that $q \nmid 1, 7 \mid -7, 0, 0, \dots$, and $7^2 \nmid -7$, hence $f(t)$ is irreducible over \mathbb{Q} , thus is the minimal polynomial

$$m_i(t) = f(t) = t^6 - 7$$

which has roots $\{\alpha\zeta^k\}_0^5$.

- ii. minimal polynomial of ζ over $\mathbb{Q}(\alpha)$

Since ζ is the primitive 6th root of unity, we know that the minimal polynomial will be the 6th cyclotomic polynomial (2.4):

$$m_{ii}(t) = \Phi_6(t) = t^2 - t + 1$$

which has roots $\zeta, -\zeta$.

Since $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$, and the roots of $\Phi_6(t) = t^2 - t + 1$ are in \mathbb{C} , $\Phi_6(t)$ remains irreducible over $\mathbb{Q}(\alpha)$.

Therefore, by the tower of law,

$$[\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}] = \deg \Phi_6(t) \cdot \deg f(t) = 2 \cdot 6 = 12$$

and by the Fundamental Theorem of Galois Theory, we know that

$$|\Gamma(\mathbb{Q}(\alpha, \zeta) : \mathbb{Q})| = [\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}] = 12$$

which tells us that there exist 12 \mathbb{Q} -automorphisms of the Galois group.

Let's find the 12 \mathbb{Q} -automorphisms. Start by defining σ which fixes ζ and acts on α , sending it to another of the roots of the minimal polynomial of α over \mathbb{Q} , $f(t)$, choose $\alpha\zeta$.

Now define τ which fixes α and acts on ζ , sending it into another root of the minimal polynomial of ζ over $\mathbb{Q}(\alpha)$, choose $-\zeta$.

$$\begin{aligned}\sigma : \alpha &\mapsto \alpha\zeta & \tau : \alpha &\mapsto \alpha \\ \zeta &\mapsto \zeta & \zeta &\mapsto -\zeta = \zeta^{-1}\end{aligned}$$

In other words, we have 12 \mathbb{Q} -automorphisms, which are the combination of σ and τ :

$$\begin{aligned}\sigma^k \tau^j : \alpha &\mapsto \alpha\zeta^k \\ \zeta &\mapsto \zeta^j\end{aligned}$$

for $0 \leq k \leq 5$ and $j = \pm 1$.

TODO diagram

Observe, that Γ is generated by the combination of σ and τ , and it is isomorphic to the group of symmetries of order 12, the dihedral group (2.6) of order 12, \mathbb{D}_6 , ie. $\Gamma \cong \mathbb{D}_6$.

Let's find the subgroups of Γ , and the fixed fields of $\mathbb{Q}(\alpha, \zeta)$.

We know that $\Gamma \cong \mathbb{D}_6$, and we know from the properties of the dihedral group (2.6) that the number of subgroups of \mathbb{D}_6 will be $d(6) + s(6) = 4 + 12 = 16$ subgroups.

generators	order	group	fixed field	notes (check fixed field)
$\langle \rangle = \langle \sigma^6 \rangle = \langle \tau^2 \rangle$	1	id	$\mathbb{Q}(\alpha, \zeta)$	
$\langle \sigma \rangle = \langle \sigma^5 \rangle$	6	\mathbb{Z}_6	$\mathbb{Q}(\zeta)$	
$\langle \sigma^2 \rangle = \langle \sigma^4 \rangle$	3	\mathbb{Z}_3	$\mathbb{Q}(\alpha^3, \zeta)$	$\sigma^2(\alpha^3) = \alpha^3 \zeta^{3 \cdot 2} = \alpha^3 \zeta^6 = \alpha^3 \cdot 1 = \alpha^3$
$\langle \sigma^3 \rangle$	2	\mathbb{Z}_2	$\mathbb{Q}(\alpha^2, \zeta)$	$\sigma^3(\alpha^2) = (\alpha \zeta^3)^2 = \alpha^2 \zeta^6 = \alpha^2$
$\langle \tau \rangle$	2	\mathbb{Z}_2	$\mathbb{Q}(\alpha)$	
$\langle \sigma \tau \rangle$	2	\mathbb{Z}_2	$\mathbb{Q}(\alpha + \alpha \zeta)$	$\sigma \zeta(\alpha + \alpha \zeta) = \sigma(\alpha + \alpha \zeta^{-1}) = \alpha \zeta + \alpha \zeta^{-1} \zeta = \alpha \zeta + \alpha$
$\langle \sigma^2 \tau \rangle$	2	\mathbb{Z}_2	$\mathbb{Q}(\alpha + \alpha \zeta^2), \mathbb{Q}(\alpha \zeta)$	$\sigma^2 \tau(\alpha + \alpha \zeta^2) = \sigma(\alpha + \alpha \zeta^{-2}) = \alpha \zeta^2 + \alpha \zeta^{-2} \zeta^2 = \alpha \zeta^2 + \alpha$
$\langle \sigma^3 \tau \rangle$	2	\mathbb{Z}_2	$\mathbb{Q}(\alpha + \alpha \zeta^3)$	$\sigma^3 \tau(\alpha + \alpha \zeta^3) = \sigma(\alpha + \alpha \zeta^{-3}) = \alpha \zeta^3 + \alpha \zeta^{-3} \zeta^3 = \alpha \zeta^3 + \alpha$
$\langle \sigma^4 \tau \rangle$	2	\mathbb{Z}_2	$\mathbb{Q}(\alpha + \alpha \zeta^4), \mathbb{Q}(\alpha \zeta^2)$	$\sigma^4 \tau(\alpha + \alpha \zeta^4) = \sigma(\alpha + \alpha \zeta^{-4}) = \alpha \zeta^4 + \alpha \zeta^{-4} \zeta^4 = \alpha \zeta^4 + \alpha$
$\langle \sigma^5 \tau \rangle$	2	\mathbb{Z}_2	$\mathbb{Q}(\alpha + \alpha \zeta^5)$	$\sigma^5 \tau(\alpha + \alpha \zeta^5) = \sigma(\alpha + \alpha \zeta^{-5}) = \alpha \zeta^5 + \alpha \zeta^{-5} \zeta^5 = \alpha \zeta^5 + \alpha$
$\langle \sigma, \tau \rangle = \langle \sigma^5, \tau \rangle$	$6 \cdot 2 = 12$	\mathbb{D}_6	\mathbb{Q}	
$\langle \sigma^2, \tau \rangle = \langle \sigma^4, \tau \rangle$	$3 \cdot 2 = 6$	\mathbb{D}_3	$\mathbb{Q}(\alpha^3)$	$\sigma^2(\alpha^3) = \alpha^3 \zeta^{3 \cdot 2} = \alpha^3$ and $\tau(\alpha^3) = \alpha^3$
$\langle \sigma^3, \tau \rangle$	$2 \cdot 2 = 4$	\mathbb{D}_2	$\mathbb{Q}(\alpha^2)$	$\sigma^3(\alpha^2) = \alpha^2 \zeta^{2 \cdot 2} = \alpha^2$ and $\tau(\alpha^2) = \alpha^2$
$\langle \sigma^2, \sigma \tau \rangle$	$3 \cdot 2 = 6$	\mathbb{D}_3	$\mathbb{Q}(\alpha^3 + \alpha^3 \zeta^3)$	$\sigma^2(\alpha^3 + \alpha^3 \zeta^3) = \alpha^3 \zeta^3 + \alpha^3 \zeta^3 \zeta^3 = \alpha^3 \zeta^3 + \alpha^3 \zeta^6 = \alpha^3 \zeta^3 + \alpha^3$
$\langle \sigma^3, \sigma \tau \rangle$	$2 \cdot 2 = 4$	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\mathbb{Q}(\alpha^2 \zeta^2), \mathbb{Q}(\alpha^2 + \alpha^2 \zeta^2)$	$\sigma^3(\alpha^2 + \alpha^2 \zeta^2) = \alpha^2 \zeta^{2 \cdot 3} + \alpha^2 \zeta^{2 \cdot 3} \zeta^2 = \alpha^2 + \alpha^2 \zeta^2$
$\langle \sigma^3, \sigma^2 \tau \rangle$	$2 \cdot 2 = 4$	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\mathbb{Q}(\alpha^2 \zeta^4), \mathbb{Q}(\alpha^2 + \alpha^2 \zeta^4)$	and $\sigma \tau(\alpha^2 + \alpha^2 \zeta^2) = \alpha^2 \zeta^2 + \alpha^2 \zeta^{-2} \zeta^2 = \alpha^2 \zeta^2 + \alpha^2$ $\sigma^2 \zeta(\alpha^2 \zeta^4) = \alpha^2 \zeta^2 \zeta^{-4} = \alpha^2 \zeta^{-2} = \alpha^2 \zeta^4$ and $\sigma^3(\alpha^2 \zeta^4) = \alpha^2 \zeta^{2 \cdot 3} \zeta^4 = \alpha^2 \zeta^4$

References

- [1] Ian Stewart. Galois Theory, Third Edition, 2004.
- [2] Gaurab Bardhan, Palash Nath, and Himangshu Chakraborty.