Algebra II – Lecture Notes

Han-Miru Kim

June 1, 2021

0 Repetition Algebra I

0.1 Ring Theory

Definition 0.1. Let R be a UFD and $f \in R[X] \setminus \{0\}$. The gcd of the coefficients of f is called the **content** $I(f)$ of f.
We say that f is **primitive**, if $I(f) \in R^\times$.

Theorem 0.2 (Eisenstein Criterion)**.** *Let R be a UFD and $f = a_n X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in R[X]$ be primitive such that there exists some prime $p \in R$ with*

$$p \nmid a_n, \quad p|a_0, \ldots p|a_{n-1}, \quad p^2 \nmid a_0$$

then f is prime in $R[X]$.

We will often use the special case where $R = \mathbb{Z}$.

0.2 Group Theory

For every g in a group G, the mapping

$$\gamma_g : G \to G, \quad x \mapsto gxg^{-1}$$

is an automorhpism. The association

$$\Phi : G \to \mathrm{Aut}(G), \quad g \mapsto \gamma_g$$

is a group homomorphism. Its kernel $Z_G = \operatorname{Ker}\Phi$ is called the **center** of the group G.

Definition 0.3. A group G is said to be **nilpotent** of order 1, if G is abelian.
We say that it is nilpotent of order $n+1$ if G/Z_G is nilpotent of order n.

Definition 0.4. A **subnormal series** in a group G is a chain of subgroups such that

$$\{e\} = G_0 \lhd G_1 \lhd G_2 \lhd \ldots \lhd G_n = G$$

such that every subgroup is normal in the next one. We say that G is **resolvable**, if such a subnormal series exists such that G_{k+1}/G_k is an abelian group for all k.

0.3 Field Theory

Definition 0.5. Let L be a field and $K \subseteq L$ a subring that is also a field. We say that K is a **subfield** of L and we call L a **field-extension** of K and write L/K (L over K).
L can also be seen as a vector space over K. Its **degree** is $[L : K] := \dim_K L$. If $[L : K] < \infty$, we say that L is a **finite field extension** of K.

Lemma 0.6. *Let F/L and L/K be finite field extensions. Then*

$$[F : K] = [F : L] \cdot [L : K]$$

To prove this, we consider basis $x_1, \dots, x_m \in F$ of F over L and a basis $y_1, \dots, y_n \in L$ of L over K and show that the products $x_i y_j \in F$ for $1 \leq i \leq m, 1 \leq j \leq n$ is a basis of F over K.

Definition 0.7. Let L/K be a field extension. For $x \in L$ consider the **evaluation mapping**

$$\varphi_x : K[X] \to L, \quad f \mapsto f(x)$$

(a) If φ_x is injective, we say that x is **trancendental** over K.

(b) If φ_x is not injective, we say x is **algebraic** over K.

If this is the case, then $\operatorname{Ker} \varphi_x = (m_x)$ is an ideal and we call $m_x(X)$ the **minimal polnomial** of x and its degree the degree of x.

We call L **algebraic** over K, if every $x \in L$ is algebraic.

Note that x is algebraic over K if and only if x is the root of a non-zero polynomial $f \in K[X]$.

Proposition 0.8. *If L/K is a finite field extension, then L is algebraic over K.*

By seeing L as an n-dimensional vector space over K, we can easily see that the $n+1$ vectors $1, \alpha, \alpha^2, \dots, \alpha^n$ are linearly dependent. This gives us a non-zero polynomial for which α is a root.
The converse is not true.

Proposition 0.9. *Let L/K be a field extension and $x \in L$. Then there exists a (up to isomorhpism) unique subfield $K(x)$ of L that is the smallest subfield of L containing K and x and:*

- *If x is transcendent, then $K[X] = \Im\varphi_x \cong L[X]$*
- *If x is algebraic, then*

Definition 0.10. Let $f \in K[X] \setminus \{0\}$. A field extension L/K of the form $L = K(a_1, \dots, a_n$, where $f(X) = \alpha \prod_{i=1}^{n} (X - a_i)$ for $\alpha \in L^\times$ is a **splitting field** of f over K.

Every polynomial has a splitting field and they are unique up to a (non-canonical) isomorphism.

Definition 0.11. A field K is called **algebraically closed**, if every non-zero polynomial splits into linear factors in K.
If L/K is a field extension such that L is algebraically closed, then the set

$$E = \{x \in L | x \text{ is algebraic over } K\}$$

forms an algebraically closed field that does not depend on the choice of such L. We call E the **algebraic closure** $\overline{K}$ of K.

Definition 0.12. Let E/k be a field extension and $\alpha \in E$. Then $k[\alpha]$ is the image of the evaluation homormophism

$$k[X] \to E, \quad p \mapsto p(\alpha)$$

Since E is a field, $k[\alpha]$ is an integraldomain and $k(\alpha)$ is the space of rational functions of $k[\alpha]$

1 Introduction

The main topic of the lecture will be **Galois theory**. The motivating problem in Galois theory is to find a formula for solutions to the function $x^n a_{n-1}x^{n-1} + \ldots + a_0 = 0$. Formulae for linear and quadratic polynomials were already known to Babylonian mathematicians ($\sim$ 1700 B.C).
Euclid ($\sim$ 300 BC) was able to translate the problem for quadratic equations into a geometric problem.
Arabian mathematician al-Khwarizmi (780-850) wrote a book "al-gabr" where we would present a way to systematically solve linear and quadratic equations. From the name al-gabr came our modern anglizied name "Algebra".
In 16-th century Italy, Scipione del Ferro was able to solve equations of degree 3, with the degree 4 case being solved by Ludovico Ferrari. These solutions were initially kept secret until they were publicised by Cardano. Cardano's transformed equations of the form $x^3 + ax^2 + bx + c = 0$ into simpler equations of the form

$$\xi^3 + p\xi + q = 0 \quad \text{for} \quad \xi = x - \frac{a}{3}$$

The idea is to then write $\xi = y + u$, where we set u later to simplify the equation. Substituting gives us

$$\begin{aligned}\xi^3 + p\xi + q &= y^3 + 3y^2u + 3yu^2 + u^3 + p(y+u) + q \\ &= y^3 + (y+u)(3yu+p) + u^3 + q\end{aligned}$$

By setting u such that $3yu + p = 0$, i.e. $u = -\frac{p}{3y}$, we obtain a simple formula for y

$$y^3 - \frac{p^3}{27y^3} + q = 0 \implies y^6 + qy^3 - \left(\frac{p}{3}\right)^3$$

Which is quadratic in $z = y^3$ and can easily be solved. The solution only uses the arithmetic operations of addition, subtraction, multiplication, division and taking roots.
Many people tried to solve the equation for degree 5, but were unable to do so.
Substantion contribution was made by Lagrange (1736 - 1813) which found htat if ξ_1, ξ_2, ξ_3 were solutions to the equation $\xi^3 + p\xi + q = 0$, then the six solutions to the resolvent $y^6 + qy^3 - (\frac{p}{3})^3 = 0$ can be expressed in terms of the Permutation group S_3

$$y_\sigma = \frac{1}{3}\left(\xi_{\sigma(1)} + \omega\xi_{\sigma(2)} + \omega^2\xi_{\sigma(3)}\right)$$

where $\omega = e^{\frac{2\pi i}{3}}$ is the primary third root of unity.
Paolo Ruffini then wanted to show that the general solution to the equation of degree 5 had no closed formula. He studied rational functions $f(\zeta_1, \ldots \zeta_5)$, where ξ_i are solutions to the equation of degree 5 and realized that the permutations $\sigma \in S_5$ that keep $f(\sigma(\zeta))$ invariant form a subgroup of S_5
He then classified the subgroups of S_5, and Nils Henrik Abel finished the proof the theorem

Theorem 1.1 (Abel-Ruffini)**.** *The general equation of fifth degree*

$$x^5 + ax^4 + bx^3 + cx^2 + dx + e = 0$$

does not have a formula for the roots that only uses finite arithmetic operations.

The statement of the theorem is very intuitive, but it is hard to give a precise mathematical definition of it. This makes it also quite hard to prove. We will prove this as a side-result of Galois-theory, where we have seen that the alternating group A_5 is anabelian and simple (a group whose normal divisors are only the trivial group and the group itself).
What we will do is to every polynomial $f \in k[X]$ we associate a group $\mathrm{Gal}(f) < S_n$ and show that if k is "nice enough", then $f(X) = 0$ is solvable if and only if $\mathrm{Gal}(f)$ is resolvable.

2 Galois Groups of a field extension

Let E be a field. Then the set of field isomorphisms

$$\mathrm{Aut}(E) := \{\varphi : E \to E | \varphi \text{ is a field isomorphisms}\}$$

is a group under composition.
If $k \subseteq E$ is a subfield, we call E a field-extension of k.

Definition 2.1. For a given field extension E/k, the associated **Galois group** is the subgroup

$$\mathrm{Gal}(E/k) := \{\varphi \in \mathrm{Aut}(E) : \varphi(x) = x \forall x \in k\} < \mathrm{Aut}(E)$$

We know from Algebra I that E can be seen as a k-vector space. As we will see in the exercise classes, we can show that every $\varphi \in \mathrm{Gal}(E/k)$ is an isomorphism of E as a k-vector space.
For example, we can show that $\mathrm{Gal}(\mathbb{C}, \mathbb{R}) = \{id_{\mathbb{C}}, \bar{\cdot}\}$, where $\bar{\cdot}$ is the complex conjugation.

Lemma 2.2. *Let $f \in k[X]$ be a polynomial and E/k be a field extension such that f splits in E (i.e. f can be written as a product of linear factors). If we set $R(f) \subseteq E$ to be the set of roots of f, then every $\sigma \in \mathrm{Gal}(E/k)$ induces a permutation on $R(f)$.*

Proof. Let $f(X) = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0$, where $a_i \in k$, $\alpha \in R(f)$ and $\sigma \in \mathrm{Gal}(E/k)$. Then we can write

$$\begin{aligned} 0 = f(\alpha) = \sigma(f(\alpha)) = \sigma(a_n a^n + \ldots + a_0) = \sigma(a_n)\sigma(\alpha)^n + \ldots + \sigma(a_0) \\ = a_n \sigma(\alpha)^n + \ldots + a_0 = f(\sigma(\alpha)) \end{aligned}$$

so $\sigma(\alpha) \in R(f)$ and $\sigma(R(f)) \subseteq R(f)$. Since $\sigma : E \to E$ is injective and $|R(\varphi)| \leq n$, it follows that $\sigma(R(f)) = R(f)$ □

Definition 2.3. Let $f \in k[X]$. The **Galois group** of f is the Galois group $\mathrm{Gal}(E/k)$ associated to the field extension of the splitting field E of f.

We know from Algebra I that the splitting field always exists and is unique up to isomorphism. So the Galois group is also unique up to isomorphism.
For a set X, let S_X denote the set of permutations of X.

Lemma 2.4. *Let E/k be a splitting field of a polynomial $f \in k[X]$ and $R(f) \subseteq E$ its roots. Then the restriction mapping*

$$\mathrm{Gal}(E/k) \to S_{R(f)}, \quad \sigma \mapsto \sigma_{|R(f)}$$

is an injective group homomorphism.

Proof. From Lemma 2.4 we know that $\sigma(R(f)) = R(f)$ for all $\sigma \in \mathrm{Gal}(E/k)$. For injectivity let $R(f) = \{\alpha_1, \ldots, \alpha_n\}$. From Algebra I, we know tha $E = k[\alpha_1, \ldots, \alpha_n]$, where $k[\alpha_1, \ldots, \alpha_n]$ is the image of the restriction mapping

$$k[X_1, \ldots, X_n] \to E, \quad p \mapsto p(\alpha_1, \ldots, \alpha_n)$$

We now show that the kernel of the ring homomorphism is the identity id_E. Assume $\sigma \in \mathrm{Gal}(E/k)$ such that $\sigma|_{R(f)} = \mathrm{id}_{R(f)}$, which means $\sigma(\alpha_i) = \alpha_i$. Let $\xi \in E$ and chose $p \in k[X_1, \ldots, X_n]$ such that $p(\alpha_1, \ldots, \alpha_n) = \xi$. Since $\sigma(x) = x \forall x \in K$ it follows that

$$\sigma(\xi) = \sigma(p(\alpha_1, \ldots, \alpha_n)) = p(\sigma(\alpha_1), \ldots \sigma(\alpha_n)) = p(\alpha_1, \ldots, \alpha_n) = \xi$$

which shows $\sigma = \mathrm{id}_E$.
An alternate proof would be to write

$$E = k(\alpha_1, \ldots, \alpha_n) = \left\{ \frac{p(\alpha_1, \ldots, \alpha_n)}{q(\alpha_1, \ldots, \alpha_n)} | p, q \in k[X_1, \ldots, X_n], q(\alpha_1, \ldots, \alpha_n) \neq 0 \right\}$$

and applying such a σ on any rational function obviously keeps it invariant, so $\sigma = \mathrm{id}_E$. □

Example 2.5. Take $k = \mathbb{F}_p(t)$ and $f = X^p - t \in k[X]$. Then f is irreducible and $|R(f)| = 1$.
Let E be a splitting field of f and $\alpha \in R(f)$. So $\alpha^p = t$. It follows that

$$(X - \alpha)^p = X^p - \alpha^p = X^p - t = f \implies R(f) = \{\alpha\}$$

A central goal of this section is to find out criteria for when $|\mathrm{Gal}(E/K)| = [E : K]$ We will show that this is the case when f is irreducible such that $|R(f)| = \deg(f)$.

Definition 2.6. A polynomial is said to have no **multiple roots**, if in a splitting field, $|R(f)| = \deg f$.

Lemma 2.7. *Let $f \in k[x]$ and $f' \in k[x]$ the formal derivative of f. Then*

$$f \text{ has no multiple roots} \iff \gcd(f, f') \in k[x]^\times$$

We will prove this in exercise sheet 2.
The nice thing about this is that the euclidean algorithm can calculate the gcd and we know that it is rather easy.

Corollary 2.7.1 (Rotman Lemma 3.4)**.** *Let $f \in k[X]$ irreducible satisfying one of the following:*

(a) $\mathrm{char}\, k = 0$

(b) If $\mathrm{char}\, k > 0$*,then* $\mathrm{char}\, k \not| \deg f$

then f does not have multiple roots.

Proof. For $d = \deg f$ and $a_d \neq 0$ we write out f and f'

$$f(x) = a_x X^d + a_{d-1} X^{d-1} + \ldots + a_0 \qquad f'(x) = a_x d X^{d-1} + a_{d-1}(d-1) X^{d-2} + \ldots + a_1$$

Since f is irreducible and either (a) or (b) is true, we know $a_d d \neq 0$, so $\deg f' = d - 1$.
If $p \in k[x]$ divides both f and f', then for sure $\deg p \leq d - 1$. But f is irreducible, so $\deg p = 0$. Therefore, $p \in k$ and $\gcd(f, f') = 1$. Using the previous lemma, it follows that f does not have multiple roots. □

Definition 2.8.

- An irreducible polynomial is **separable**, if it has no multiple roots.
- A polynomial is **separable**, if all its irreducible factors are separable

Example 2.9. $X^4 + 1 \in \mathbb{Q}[X]$ is irreducible, and since $\mathrm{char}\, \mathbb{Q} = 0$, it follows from the previous corollary that it seperable. Note that $(X^4 + 1)^{15}$ is also separable, in the reducible sense.

Let E/k be a field extension, $\alpha \in E$ $\varphi_\alpha : k[X] \to E$ the evaluation homomorphism at α. Then $\mathrm{Ker}\, \varphi_\alpha$ is an ideal in $k[X]$. There are two possibilities

- $\mathrm{Ker}\, \varphi_\alpha = \{0\}$. We then say that α is **transcendent** over k.

- $\operatorname{Ker}\varphi_\alpha \neq \{0\}$ and we say that α is **algebraic** over k. Since $k[x]$ is a PID there exists a unique unitary (leading coefficient = 1) polynomial $\operatorname{irr}(\alpha, k)$ that generates $\operatorname{Ker}\varphi_\alpha$, i.e. $(\operatorname{Ker}\varphi_\alpha = (\operatorname{irr}(\alpha, k))$. We call this polynomial the **minimal polynomial** (and sometimes write $m_{\alpha,k}$.

Since $m_{\alpha,k}$ is irreducible and $k[X]$ is a euclidean domain, it follows that ${}^{k[x]}\!/_{\operatorname{Ker}\varphi_\alpha}$ is a field and φ_α induces a field isomorphism

$$\overline{\varphi}_\alpha : {}^{k[X]}\!/_{\operatorname{Ker}\varphi_\alpha} \to k(\alpha)$$

Let $\varphi : k \to k'$ be a field isomorphism. By the universal property of the polynomial ring, this induces a ring isomorphism

$$\varphi_* : k[X] \to k'[X], \quad \varphi_*(a_n X^n + \dots a_0) := \varphi(a_n)X^n + \dots \varphi(a_0)$$

Since φ_* is a ring isomorphism it follows that $p \in k[x]$ is irreducible if and only f $\varphi_*(p)$ is irreducible.

Lemma 2.10 (Rotman 3.130)**.** *Sei $\varphi : K \to K'$ ein Körperisomorphismus, $f \in K[X]$ irreduzibel und $f_* = \varphi_*(f) \in K'[X]$.*
Dann gibt es für alle $\alpha \in R(f),\ \beta \in R(f_*)$ einen Körperisomorphismus $\widehat{\varphi} : K(\alpha) \to K'(\beta)$ der φ erweitert und α auf β abbildet.

Beweis. Da $K[X]$ ein Hauptidealring und $f \in K[X]$ irreduzibel ist, ist (f) ein maximales Ideal. Insbesondere ist $K[X]/(f)$ ein Körper. Weiterin ist α eine Nullstelle von f und da f irreduzibel ist, generiert f gerade den Kern des Evaluationshomomorphismus: $\operatorname{Ker}\operatorname{ev}_\alpha = (f)$. Dasselbe gilt natürlich auch für f_*. Darum induziert φ_* mit dem Ersten Isomorphiesatz einen Körperisomorphismus

$$\begin{array}{ccc} K[X] & \xrightarrow{\varphi_*} & K'[X] \\ \downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle \pi_2} \\ K[X]/_{\operatorname{Ker}\operatorname{ev}_\alpha} & \xrightarrow{\overline{\varphi_*}} & K'[X]/_{\operatorname{Ker}\operatorname{ev}_\beta} \end{array}$$

Diese Abbildung ist wohldefiniert, da die Abbildung $\pi_2 \circ \varphi_* : K[X] \to {}^{K'[X]}\!/_{\operatorname{Ker}\operatorname{ev}_\beta}$ für π_2 die kanonische Projektion einen Ringhomomorphismus ist und als Kern gerade $\operatorname{Ker}\pi_2 \circ \varphi_* = \operatorname{Ker}\operatorname{ev}_\alpha$ hat.
Zuletzt benutzen wir gerade die Definition der Adjunktion von Nullstellen an einem Körper und erhalten somit Körperisomorphismen Φ, Ψ:

$$\Phi : {}^{K[X]}\!/_{\operatorname{Ker}\operatorname{ev}_\alpha} \to K(\alpha), \quad \text{und} \quad \Psi : {}^{K'[X]}\!/_{\operatorname{Ker}\operatorname{ev}_\beta} \to K'(\beta)$$

und man beachte, dass dies wegen $\varphi_*(f) = f_*$ gerade α auf β abbildet.
Wir können die ganze Argumentation in einem Diagramm zusammenfassen.

$$\begin{array}{ccc} K & \xrightarrow{\varphi} & K' \\ \downarrow & & \downarrow \\ K[X] & \xrightarrow{\varphi_*} & K'[X] \\ \downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle \pi_2} \\ K[X]/_{\operatorname{Ker}\operatorname{ev}_\alpha} & \xrightarrow{\overline{\varphi_*}} & K'[X]/_{\operatorname{Ker}\operatorname{ev}_\beta} \\ \downarrow{\scriptstyle \wr\,\Phi} & & \downarrow{\scriptstyle \wr\,\Psi} \\ K(\alpha) & \xrightarrow{\widehat{\varphi}=\Psi\circ\overline{\varphi_*}\circ\Phi^{-1}} & K'(\beta) \end{array}$$

und sehen, dass $\widehat{\varphi} = \Psi \circ \overline{\varphi_*} \circ \Phi^{-1}$ gerade die gewünschten Eigenschaften hat. □

A stronger version of this lemma is the following proposition:

Proposition 2.11. *Let $k \subseteq B \subseteq E$ be field extensions where E is the splitting field of some $g \in k[x]$. Then, any automorphism $\sigma : B \to B$ can be extended to an automorphism $\Sigma : E \to E$*

Proof. We prove this using induction on $[E : k]$. If $[E : k] = 1$, then f splits in linear factors in $k[X]$ and the same is true for f_*. □

Theorem 2.12 (Rotman 3.7)**.** *Let $\varphi : k \to k'$ be a field isomorphism, $f \in k[X]$, $f_* = \varphi_*(f)$ and E/k be a splitting field of f and E_* a splitting field of f_*.*
If f is seperable, then there are exactly $[E : k]$ isomorphisms $\Phi : E \to E_*$ extending φ. In particular, $|\mathrm{Gal}(E/k)| = [E : k]$ as we can just take $k' = k, E' = E$ and use $\varphi = \mathrm{id}_k$.

Proof. We prove this using induction on $[E : k]$. For $[E : k] = 1$ it's clear as f already splits over k.
If $[E : k] > 1$, then there exists an irreducible factor $p \in k[X]$ of f of highest degree $\deg p = d > 1$. So if we write $f = p \cdot g$ for some $g \in k[X]$ then we can use the fact that φ_* is a ring isomorphism to get

$$\varphi_*(f) = \varphi_*(p)\varphi_*(g) = p_* \cdot g_* = f_*$$

since p is irreducible, so too must be p_* and separable as $\deg(p_*) = \deg(p) = d > 1$. If we name the roots $\alpha_1^*, \ldots, \alpha_d^*$we can use the previous lemma, which gives us for every α_i^* an Isomorphism

$$\hat{\varphi}_i : k(\alpha_i) \to k'(\alpha_i^*) \quad \text{with} \quad \hat{\varphi}_i(\alpha) = \alpha_i^*$$

extending φ. Now write $\alpha = \alpha_i$ for some i to clear up the notation.
We can view the fields $k(\alpha)$ and $k(\alpha^*$ as subfields of E and E_*, respectively.
Using the multiplicity of the field extension dimensions we get

$$[E : k(\alpha)] = \frac{[E : k]}{[k(\alpha) : k} = \frac{[E : k]}{d} < [E : k]$$

using induction on $[E : k(\alpha)]$, we get that there should be exactly $[E : k(\alpha)$ isomorphisms extending $\hat{\varphi} : k(\alpha) \to k'(\alpha_*)$ to $E \to E_*$.
[<???>]
Now we can look at $f \in k[X]$ as polynomials with coefficients in $k(\alpha)$. Same goes for f_*. By the universal property of the polynomial ring, this then induces an isomorphism

$$(\widehat{\varphi})_* : k(\alpha) \to k(\alpha_*)$$

which maps $f \in k(\alpha)[X]$ to $f_* \in k(\alpha_*)[X]$. So they are both separable again.
[</???>]
Doing this for all $1 \leq i \leq d$ we get exactly

$$d \cdot [E : k(\alpha)] = [k(\alpha) : k][E : k(\alpha)] = [E : k]$$

isomorphisms $E \to E_*$ extending φ. □

Corollary 2.12.1 (Rotman 3.9)**.** *Let E/k be a splitting field of a separable polynomial $f \in k[X]$ of degree $\deg(f) = n$. If f is irreducible, then n divides $|\mathrm{Gal}(E/k)|$.*

Proof. Let $\alpha \in R(f) \subseteq E$. Then $k(\alpha) \subseteq E$ and since f is irreducible $[k(\alpha) : k] = n = \deg f$.
From the previous theorem (the special case) we immediately get that

$$|\mathrm{Gal}(E/k)| = [E : k] = [E : k(\alpha)] \cdot [k(\alpha) : k] = [E : k(\alpha)] \cdot n$$

□

Theorem 2.13 (Rotman 3.15)**.** *Let p be prime, $n \geq 1 \in \mathbb{N}$. Then $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$ an a generating element is given by the **Frobenius** homomorphism*

$$Fr : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}, \quad x \mapsto x^p$$

Proof. Note that the group of units has $|\mathbb{F}_{p^n}^\times| = p^n - 1$ elements. So $\mathbb{F}_{p^n}^\times$ is exactly the roots of the polynomial $X^{p^n-1} - 1 \in \mathbb{F}_p[X]$.
This polynomial has no multiple roots, which means it is separable. So using the previous theorem, we get that $|\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)| = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$.
We now show that Fr generates all n Elements of the Galois group. For $k \geq 1 \in \mathbb{N}$ we can see that $\mathrm{Fr}^k(\xi) = \xi^{p^k}$. Let m be the order of $\mathrm{Fr} \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. This means that we would have $\xi^{p^m} = \xi$ for all $\xi \in \mathbb{F}_{p^n}$ which gives us $n \leq m \leq n$. □

Theorem 2.14. *Let p be prime and $f \in \mathbb{Q}[X]$ with $\deg f = p$ and a splitting field E.*
Assume that f is irreducible and f has exactly $p - 2$ real roots. Then $\mathrm{Gal}(E/\mathbb{Q}) \cong S_p$.

We know from the previous corollary that $\deg f = p$ divides $|\mathrm{Gal}(E/\mathbb{Q})|$.
To complete the proof, we need the following lemma.

Lemma 2.15 (Cauchy)**.** *Let G be a finite group and p prime that divides the order of G. Then G contains an element of order p.*

We could obviously use the Sylow-theorem to prove the existence of a subgroup of order p, but there is also a more elementary proof.

Proof Lemma. Let

$$\Gamma_p = \{(g_1, \ldots, g_p) \in G^p | g_1 \ldots g_p = e\} \subseteq G^p$$

and define a group action of the symmetry group S_p on G^p by permutation of the elements.
We claim that the p-cycle $\sigma = (1, 2, \ldots, p) \in S_p$ is an invaraint, since

$$g_2 \ldots g_p g_1 = g_1^{-1}(g_1 \ldots g_p)g_1 = g_1^{-1} e g_1 = e$$

and therefore, the cyclic subgroup generated by σ also keeps Γ_p invariant. If we let $C_p = \{\mathrm{id}, \sigma, \ldots, \sigma^{p-1}\} < S_p$, then we see that Γ_p can be written as the disjoint union of C_p orbits.
Further, the only possible cardinalities of a C_p orbit is either 1 or p. Since p divides $|G|^{p-1}$ it must also divide the cardinality of the set of C_p orbits of cardinality 1. So there is at least one non-trivial element there. But the only possible C_p orbits of cardinality 1 are orbits of elements of the form $(h, h, \ldots, h)$ with the trivial element being $(e, e, \ldots, e)$.
This shows the existence of such an h with order p. □

Proof Theorem. Consider the field extension $\mathbb{C}/\mathbb{Q}$. Since $\mathbb{C}$ is algebraically closed, we can chose a splitting field E of f with $Q \subseteq E \subseteq \mathbb{C}$. Let $R(f) = \{\alpha_1, \dots, \alpha_p\}$ be the roots of f and order them such that $\{\alpha_3, \dots, \alpha_n\} \subseteq \mathbb{R}$. Since $f \in \mathbb{Q}[X]$, its coefficients are real, so $\alpha_2 = \overline{\alpha_1}$. Using Lemma 2.4 we can identify $\mathrm{Gal}(E/\mathbb{Q})$ with a subgroup of $S_{R(f)} = S_p$, so we have the inclusion $\mathrm{Gal}(E/\mathbb{Q}) \subseteq S_p$.
If we write $\epsilon : \mathbb{C} \to \mathbb{C}$ to be the complex conjucation, then we have $\epsilon(E) = E$, so $\epsilon|_E \in \mathrm{Gal}(E/\mathbb{Q})$ corresponds to the transposition $\tau_{12} \in S_p$.
We also know from Coroallary 2.12.1 that since f is irreducible, p divides $|\mathrm{Gal}(E/\mathbb{Q})|$. Cauchy's Lemma then says that there exists an element of order p in $\mathrm{Gal}(E/\mathbb{Q})$. But the elements of order p are exactly the p-cycles in S_p.
From exercise sheet 03 problem 6, the p-cycles and a transposition generate S_p, which concludes the proof. □

A remarkable thing about this proof is that it combines knowledge about fields, finite groups and permutation groups.

Example 2.16. We wish to compute the Galois group of $f = X^5 - 4X + 2 \in \mathbb{Q}[X]$.
f fulfills the Eisenstein criterion for the prime $p = 2$ so it is irreducible (and prime). f also has exactly $3 = 5 - 2$ real roots, because $f' = 5X^4 - 4$ has two real roots $\pm\sqrt[4]{\frac{4}{5}}$.

There exists a correspondence between irreducibility and transitivity of the Galois group.

Corollary 2.16.1 (Rotman 3.14)**.** *Let $f \in k[X]$ and let E be a splitting field of f. If f has no multiple roots, then*

$$f \text{ is irreducible} \iff \mathrm{Gal}(E/K) \text{ acts transitively on } R(f)$$

Note: the implication $\implies$ holds without the assumption that f has no mltiple roots as the following proof will show.

Proof. Let f be irreducible. Recall that transitivtiy means that for every $\alpha, \beta \in R(f)$ there exists a $g \in \mathrm{Gal}(E/k)$ such that $g \cdot \alpha = \beta$.
This is just the special case for Theorem 2.10 for $k' = k$ and $\varphi = \mathrm{id}_K$. See Exercise sheet 02 problem 3 for details.
Now, assume the group action $\mathrm{Gal}(E/k) \to R(f)$ is transitive and let $f = pq$ for $p, q \in K[X]$. Then $R(p), R(q) \subseteq R(f)$. Since f has no multiple roots $R(p) \cap R(q) = \emptyset$. But since the group action is transitive, it means that one of $R(p), R(q)$ is empty or else that would mean a $g \in \mathrm{Gal}(E/k)$ would map an element of $R(p)$ to an element of $R(q)$ but since $\mathrm{Gal}(E/k)R(p) \subseteq R(p)$ it means that their intersection is non-empty. Since either one of p or q has no roots, f is irreducible. □

Definition 2.17. A field extension E/k is calld **normal** if it is a splitting field of a polynomial $f \in k[X]$.

Note: If E/B and B/k are field extensions such that E/k is normal, then E/B is also normal as we can take the same polynomial $f \in k[X] \subseteq B[X]$.

Theorem 2.18. *Let E/B and B/k be finite extensions such that E/k and B/k are normal. Then for all $\sigma \in \mathrm{Gal}(E/k), \sigma(B) = B$ and the group homomorphism*

$$\mathrm{Gal}(E/k) \to \mathrm{Gal}(B/k), \quad \sigma \mapsto \sigma|_B$$

is surjective with kernel $\mathrm{Gal}(E/B)$.

Proof. Let $f \in k[X]$ be the polynomial such that B is the splitting field of f. From Lemma **??**, it follows that

$$\sigma(R(f)) = R(f), \quad \forall \sigma \in \mathrm{Gal}(E/k)$$

so since $B = k(R(f))$, we also get $\sigma(B) = B$. Therefore, the group homomorphism $\mathrm{Gal}(E/k) \to \mathrm{Gal}(B/k)$ is indeed well defined. The kernel is obiously $\mathrm{Gal}(E/B)$. To show surjectivity, let $\sigma \in \mathrm{Gal}(B/k)$. Because E/k is normal, there exists a $g \in k[X]$ such that E is the splitting field of g. But then, the induced ring homomorphism σ_* maps g to g, and as such, Lemma 2.11 says that that σ can be extended to an automorphism $\Sigma : E \to E$ with $\Sigma|_B = \sigma$. □

In the exercise sheet 4 problem 6 we will prove the following theorem

Theorem 2.19. *A finite extension E/k is normal if and only if every irreducible polynomial $f \in k[X]$ that has a root in E also splits over E.*

3 Resolvable groups

In this section, we will prove the insolvability of the quntic using radicals. The main problem is to find a good definition of what a *formula* using some arithmetic operations *is*.
For this, we will start with a **field**, which is closed under the normal operations. Then we define **pure extensions**, which are field extensions obtained by adjoining roots of polynomials. Then, we introduce **radical extensions** and **resolvable extensions** to check whether a polynomial can be solved. This will result in Galois' theorem.

Theorem (Galois)**.** *Let $f \in k[x]$ and E be its splitting field.*
If f is solvable using radicals, then $\mathrm{Gal}(E/k)$ *is a resolvable group.*

Let $K = k(\alpha)$ be a field extension of k for some $\alpha \neq 0$. Then the set

$$\{n \in \mathbb{Z} : \alpha^n \in k\}$$

is a subgroup of $\mathbb{Z}$ and therefore of the form $m\mathbb{Z}$ for some $m \in \mathbb{N}$. But it could be that no powers of α are in k. (For example $\mathbb{Q}(\pi)$). Then $m\mathbb{Z} = 0$.

Definition 3.1. The field extension $k(\alpha)/k$ is said to be a **pure extension** of **type** $m \geq 1$ if

$$\{m\mathbb{Z} = n \in \mathbb{Z} : \alpha^k \in k\} \neq 0$$

We say that a field extension K/k is **radical** if there exists a tower of pure field extensions

$$k = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_t = K, \quad K_{i+1}/K_i \text{ pure}$$

A polynomial $f \in k[X]$ is said to be **solvable by radicals**, if there exists a splitting field of f contained in a radical extension of k.

We see that this defintion of radically solvable polynomials matches with our intuition that the m-th root of a number in k has a power that is in k again.

Example 3.2. Let $f(x) = X^2 + bX + c \in k[X]$ and E be a splitting field of f containing its roots $R(f) = \{\alpha_1, \alpha_2\}$.
Plugging in a root and expanding binomially, we get

$$0 = \alpha^2 + b\alpha + c = \left(\alpha + \tfrac{b}{2}\right)^2 + c - \tfrac{b^2}{4}$$

so if $u := \alpha_1 + \frac{b}{2} \in E/k(u)$, then $u^2 = \frac{b^2}{4} - c \in k$. But since $E = k(\alpha_1, \alpha_2)$ and

$$\alpha_1 = u - \tfrac{b}{2}, \quad \alpha_2 + \alpha_1 = -b \implies \alpha_2 = -b - \alpha_1 = -u - \tfrac{b}{2}$$

so $E = k(u)$.

Let $k(\alpha)/k$ be a pure extension of type m. If we consider the prime factorisation $m = p_1 \dots p_r$, then we can look at the towers

$$k(\alpha) \supset k(\alpha^{p_1}) \supset k(\alpha^{p_1 p_2} \supset \dots \supset k(\alpha^m) = k$$

where every extension is of type p_i. This leads us to study $X^p - c \in k[x]$.

Lemma 3.3. *Let p be prime and $f = X^p - c \in k[X]$. Then*

(a) There are two cases: f is irreducible, or c is the p-th power of an element in k.

(b) Let E/k be the splitting field of f and assume k contains all p-th roots of 1. Let $\alpha \in E, \alpha \in R(f)$, then $E = k(\alpha)$ and

(i) If f is irreducible and $\mathrm{char}(k) \neq p$, then $\mathrm{Gal}(E/k) \cong \mathbb{Z}/p\mathbb{Z}$

(ii) If f is irreducible and $\mathrm{char}(k) = p$, then $\mathrm{Gal}(E/k) = \{e\}$.

(iii) If f is reducible, then $E = k$ (and $\mathrm{Gal}(E/k) \cong (e)$)

Proof. (a) If f is reducible, then $f = gh$ for some $g = X^d + b_{d-1}X^{d-1} + \dots + b_0, 1 \leq d < p$. Let E/k be a splitting field of $f = X^p - c$ and $\alpha \in R(f)$. If $\beta \in R(f)$ is another root, then $\alpha^p = \beta^p = c \implies \frac{\alpha^p}{\beta^p} = 1$. Therefore we can write

$$R(f) = \{\alpha \cdot \xi | \xi^p = 1\}$$

and since $R(g) \subseteq R(f)$ and b_0 is the product of all roots of g, we have $b_0 = \alpha^d \cdot \eta$ for some $\eta^p = 1$.

$$\implies b_0^p = \alpha^{dp} = c^d$$

but since p is prime and $1 \leq d < p$, p and d have no common divisors, so there exist $r, s \in \mathbb{Z}$ such that $rp + sd = 1$. This gives us

$$c = c^{rp+sd} = c^{rp}c^{ds} = c^{rp}b_0^{ps} = (c^r b_0^s)^p$$

(b) By assumption, k contains all the roots of 1. By our trick $\frac{\alpha^p}{\beta^p} = 1$, the roots of f must be of the form

$$R(f) = \{\alpha\zeta : \zeta^p = 1\} \implies E = k(\alpha)$$

(i) Because $\mathrm{char}(k) \neq p$ and f is irreducible we have that the derivative is $f' = pX^{p-1} \neq 0$. Since $\gcd(f, f') = 1$, f is also separable by the $\gcd(f, f')$ lemma. By Theorem 2.12, we have

$$|\mathrm{Gal}(E/k)| = |[E : k]| = |[k(\alpha) : k]| = p$$

and since the only groups of order p are cyclic, $\mathrm{Gal}(E/k) \cong \mathbb{Z}/p\mathbb{Z}$.

Other parts of lemma ??? □

Now that polynomials that can be solved by radicals have a splitting field contained in a radical extension, we can ask when are radical extensions contained in a normal extension? We want to get a tower $k \subseteq E \subseteq K \subseteq F$, where E is normal and F is normal and radical.
Looking at the tower $k \subseteq E \subseteq F$ of normal extensions $E/k, F/k$ and applying theorem 2.18 we get a surjective homomorphism

$$\mathrm{Gal}(F/k) \to \mathrm{Gal}(E/k), \quad \sigma \mapsto \sigma|_E$$

If we can show that $\mathrm{Gal}(F/k)$ is resolvable, then it follows that $\mathrm{Gal}(E/k)$ is also resolvable. Resulting in the theorem stating that every subgroup and anevery quotient of a resolvable group are again resolvable.
For the next two lemmata, we set the context as follows:

- Let $B = k(u_1, \ldots, u_t)$ be a finite extension. This in particular means that $u_1, \ldots, u_t$ are algebraic (or else it wouldn't be a finite extension)
- Let $p_i = \mathrm{irr}(u_i, k) \in k[X]$ be the minimal polynomial of u_i over k and let E be the splitting field of $f = p_1 \ldots p_t \in k[x]$ and write $G = \mathrm{Gal}(E/k)$.

The following lemma tells us how to construct E given the u_i.

Lemma 3.4. *E can be obtained by adjoining $\sigma(u_i)$ for all $\sigma \in \mathrm{Gal}(E/k)$, and all i*

$$E = k\left(\sigma(u_1), \ldots, \sigma(u_t), \sigma \in \mathrm{Gal}(E/k)\right)$$

Proof. Since E is the splitting field of $f = p_1 \ldots p_t$, E contains all the roots of the p_i. Then for any $u, u' \in R(p_i)$ we can use Lemma 2.10 to find an isomorphism $\hat{\varphi} : k(u) \to k(u')$ extending the identity $\mathrm{id}_k : k \to k$.
Since $f \in k[x]$ can also be viewed as a polynomial $f \in k(u)[X]$, and the extension to the polynomial ring fixes f: $\hat{\varphi}_*(f) = f$, we can use the fact that E is a splitting field together with Proposition 2.11 to extend $\hat{\varphi}$ to an isomorphism $\Phi : E \to E$. In particular, we have $\Phi \in \mathrm{Gal}(E/k)$ and $\Phi(u) = u'$.
Therefore, for all i, any root $u' \in R(p_i)$, there exists a $\sigma \in \mathrm{Gal}(E/k)$ such that $\sigma(u_i) = u'$.
So by writing

$$R(f) = \bigcup_{i=1}^{t} R(p_i) \subseteq \{\sigma(u_i) | 1 \leq i \leq t, \sigma \in \mathrm{Gal}(E/k)\}$$

any root of f can be obtained by adjoining $\sigma(u_i)$ for the right $\sigma \in \mathrm{Gal}(E/k)$. □

Lemma 3.5. *In the context of the previous Lemma, assume that the u_i are ordered such that there exist $m_i \in \mathbb{Z}$ such that*

$$u_1^{m_1} \in K, \quad u_2^{m_2} \in k(u_1), \quad \ldots \quad u_t^{m_t} \in k(u_1, \ldots, u_{t-1})$$

Then E/k is a radical extension

Proof. For $\sigma_r \in \mathrm{Gal}(E/k)$, set $B_0 = k, B_1 = k(\sigma_1(u_1), \ldots \sigma_l(u_1))$ and inductively, set $B_j = B_{j-1}(\sigma_1(u_j), \ldots \sigma_l(u_j))$.
This results in a tower of extensions

$$k = B_0 \subseteq B_1 \subseteq B_2 \subseteq \ldots \subseteq B_t = E$$

Now we show that B_1/k is a radical extension.
Using the assumption, we find that for any $1 \leq r \leq l$:

$$\sigma_r(u_1)^{m_1} = \sigma_r(\underbrace{u_1^{m_1}}_{\in k}) = u_1^{m_1} \in k \subseteq k(\sigma_1(u_1), \ldots, \sigma_{r-1}(u_1))$$

So for all $1 \leq r \leq t$, the extension

$$k(\sigma_1(u_1), \ldots, \sigma_{r-1}(u_1)) \subseteq k(\sigma_1(u_1), \ldots, \sigma_r(u_1))$$

is pure. Therefore, we get a tower or pure extensions

$$k \subseteq k(\sigma_1(u_j)) \subseteq k(\sigma_1(u_j), \sigma_2(u_j)) \subseteq \ldots \subseteq k(\sigma_1(u_j), \ldots, \sigma_{r-1}(u_j)) \subseteq k(\sigma_1(u_j), \ldots, \sigma_r(u_j)) \subseteq \ldots = B_1$$

which means that $k \subseteq B_1$ is radical.
The same argument goes for the other B_j/B_{j-1}, so E/k is radical. □

Corollary 3.5.1. *Let K/k be a radical extension. Then there exists a field F with $k \subseteq K \subseteq F$ such that F/k is radical and normal.*

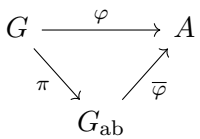
Recall the definition for resolvable groups. A group G is resolvable, if there exists a subnormal sequence

$$\{e\} = G_0 \lhd G_1 \lhd \ldots \lhd G_t = G$$

such that the factor groups G_{i+1}/G_i are abelian.
And we also saw that A_n, S_n were resolvable for $n \geq 4$. There is a criterion for when a group is resolvable, that uses iterated commutator groups:
For a group G, let $[G, G]$ be the subgroup generated by $\{[a, b] | a, b \in G\}$, where $[a, b] = aba^{-1}b^{-1}$. This subgruop $[G, G]$ is a normal divisor of G and also characteristic, which means that it is invariant under automorphisms of G ($\forall \alpha \in \mathrm{Aut}(G), \alpha([G, G]) = [G, G]$).
In Algebra I, we inductively defined

$$G^{(1)} := [G, G], \quad G^{(j+1)} := [G^{(j)}, G^{(j)}]$$

and saw that G is resolvable if and only if there exists an n such that $G^{(n)} = \{e\}$.
We sometimes write $G_{\mathrm{ab}} := G/[G, G]$, which is the largest abelian quotient of G in the sense that for any homomorphism to an abelian group $\varphi : G \to A$, then φ factors through G_{ab}. That is, there exists a unique group homomorhpism $\overline{\varphi} : G_{\mathrm{ab}} \to A$ such that the following diagram commutes



Proposition 3.6. *(a) If $H < G$, then G resolvable $\implies$ H resolvable.*

(b) If $N \lhd G$, then G is resolvable if and only if N and G/N are resolvable.

Proof. Note that if $\varphi : G \to L$ is a homomorphism, then

$$\varphi([a, b]) = [\varphi(a), \varphi(b)], \quad \forall a, b \in G$$

so $\varphi([G, G]) \subseteq [L, L]$. In particular, if φ is surjective, then $\varphi([G, G]) = [L, L]$.

(a) Since $H < G$, we can consider the embedding $\varphi : H \to G$ to get $[H, H] \to [G, G]$. Inductively, we also get $H^{(j)} \subseteq G^{(j)}$, so if G is resolvable for $G^{(n)} = \{e\}$, then $H^{(n)} \subseteq G^{(n)} = \{e\}$.

(b) If G is resolvable, then, by (a), N is resovable. Taking the surjective quotient map $\pi : G \to G/N$, we get $\pi([G, G]) = [G/N, G/N]$, and also inductively, $\pi(G^j) = (G/N)^{(j)}$.

Now, assume that N and G/N are resolvable. Then there exists an $n \geq 1$ such that

$$\{e\} = (G/N)^{(n)} = \pi(G^n) \implies G^{(n)} \subseteq N$$

but since N is resolvable, there exists a $l \geq 1$ such that $N^{(l)} = \{e\}$. Therefore

$$G^{(n+l)} = (G^{(n)})^{(l)} \subseteq N^l = \{e\}$$

□

Now we are finally able to prove the following:

Theorem 3.7. *Let E be a splitting field of $f \in k[X]$. If f is solvable by radicals, then* $\mathrm{Gal}(E/k)$ *is a resolvable group.*

The proof makes use of the following observation

Lemma 3.8. *For a tower of field extensions $k = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_t$ such that*

(a) K_t/k is normal

(b) K_i/K_{i-1} is a pure extension of prime type p_i

(c) k contains all p_i-th roots of 1*.*

Then $\mathrm{Gal}(K_t/k)$ *is resolvable*

The sketch of the proof is as follows: If f is solvable with radicals, then there exists a field L with $k \subseteq E \subseteq L$ and L/k radical.
Using Corollary 3.5.1 there exists a field F with $k \subseteq E \subseteq L \subseteq F$ such that F/k is radical and normal.
The lemma then says that $\mathrm{Gal}(F/k)$ is resovlable, and since

$$\mathrm{Gal}(E/k) \cong {}^{\mathrm{Gal}(F/k)}\!/_{\mathrm{Gal}(F/E)}$$

it follows that $\mathrm{Gal}(E/k)$ is resolvable.

Proof Lemma. Set $G = \mathrm{Gal}(K_t/k), G_1 = \mathrm{Gal}(K_t/K_1), G_2 = \mathrm{Gal}(K_t/K_2)$ etc. and we obtain a sequence of groups

$$\{e\} = G_t \subseteq G_{t-1} \subseteq \ldots \subseteq G_2 \subseteq G_1 \subseteq G$$

If u_i is the adjoint of the i-th pure extension: $K_i = K_{i-1}(u_i)$, which by assumption satisfies $u_i^{p_i} \in K_{i-1}$, we consider the polynomial

$$f_i(X) = X^{p_i} - c_i \in K_{i-1}[X] \quad \text{where} \quad c_i = u_i^{p_i} \in K_{i-1}$$

In 3.3 (a) we saw that either f is irreducible or c_i is the p_i-th power of an element in K_{i-1}.
But by assumption, $u_i \notin K_{i-1}$, so f_i is irreducible and K_{i-1} contains all p_i-th roots of 1. Therefore, K_i is a splitting field of $f_i \in K_{i-1}[X]$.
By the same Lemma, $\mathrm{Gal}(K_i/K_{i-1})$ is either $\mathbb{Z}/p_i\mathbb{Z}$ or $\{e\}$.
Furthermore, because K_i/K_{i-1} is normal and the cyclic group is abelian, the sequence of groups $G_t \subseteq \ldots \subseteq G_1 \subseteq G$ is indeed a subnormal sequence with abelian quotients. □

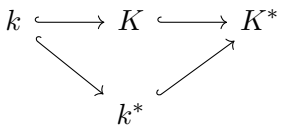
Proof Theorem. Let $f \in k[X]$ be solvable by radicals and E a splitting field of f. By Corollary 3.5.1 we can assume that there exists a field K such that K/k is radical and normal Let

$$k = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_t = K, \quad \text{where} \quad K_i = K_{i-1}(u_i), \text{ and } u_i^{p_i} \in K_{i-1}$$

be the corresponding chain of fields. Set $m = \prod_{i=1}^{t} p_i$ and let

$$\begin{aligned} k^* &= \text{ splitting field of } X^m - 1 \in k[X] \\ K^* &= \text{ splitting field of } X^m - 1 \in K[X] \end{aligned}$$

In exercise sheet 6, we proved that since K/k and K^*/K are normal, also K^*/k is normal.
Looking at the diagram



we claim that $\mathrm{Gal}(K^*/k^*)$ is resolvable. By setting

$$K_0^* = k^*, K_1^* = K_0^*(u_1), \ldots, K_i^* = K_{i-1}^*(u_i)$$

we obtain a tower from k^* to K^*. Since $u_i^{p_i} \in K_{i-1} \subseteq K_{i-1}^*$, these extensions are all pure, but their prime type might have changed from p_i to something else.
Either it's still p_i, or $\{m \in \mathbb{Z} | u_i^m \in K_{i-1}^*\} = \mathbb{Z}$, in which case $K_i^* = K_{i-1}^*$.
So by the Lemma, $\mathrm{Gal}(K^*/k^*)$ is resolvable.
Now we claim that $\mathrm{Gal}(k^*/k)$ is resolvable. Let

$$\Gamma_m(k^*) = \{\xi \in k^* | \xi^m = 1\}$$

be the set of roots of $X^m - 1$ in k^*. Then $\Gamma_m(k^*)$ is a finite subgroup of $(k^*)^\times$ and thus cyclic.
We also know that the restriction homomorphism

$$\mathrm{Gal}(k^*/k) \to \mathrm{Aut}(\Gamma_m(k^*)), \quad \sigma \mapsto \sigma|_{\Gamma_m(k^*)}$$

is injective. But since $\mathrm{Aut}(\Gamma_m(k^*))$ is abelian, so is $\mathrm{Gal}(k^*/k)$.
Now we know that from $k \subseteq k^* \subseteq K^*$ we get

$$\mathrm{Gal}(K^*/k)/\mathrm{Gal}(K^*/k^*) \cong \mathrm{Gal}(k^*/k)$$

and from proposition 3.6 $\mathrm{Gal}(K^*/k)$ is resolvable.
And looking at $k \subseteq E \subseteq K^*$ we get

$$\mathrm{Gal}(E/k) \cong \mathrm{Gal}(K^*/k)/\mathrm{Gal}(K^*)/E$$

we get $\mathrm{Gal}(K^*/k)$ resolvable $\implies$ $\mathrm{Gal}(E/k)$ resolvable.

□

Corollary 3.8.1 (Abels-Ruffini)**.** *For $n \geq 5$, the general polynomial*

$$f(X) = \prod_{i=1}^{n} (X - y_i)$$

is not solvable by radicals.

Proof. Considering $f \in k(y_1, \ldots, y_n)[X]$ we can write

$$\prod_{i=1}^{n}(X - y_i) = X^n - s_1X^{n-1} + \ldots + (-1)^n s_n$$

so we also get $f \in k(s_1, \ldots, s_n)$. If we set $E = k(s_1, \ldots, s_n) \subseteq k(y_1, \ldots, y_n) = F$, then $f \in E[X]$ and F is a splitting field of f.
We wish to compute $\mathrm{Gal}(E/F)$ and notice that we get an injective group homomorphism

$$\mathrm{Gal}(E/F) \to S_{\{y_1,\ldots,y_n\}}, \quad \sigma \mapsto \sigma|_{\{y_1,\ldots,y_n\}}$$

Now let $s \in S_n$ and $R \in F$ and define

$$(\sigma_s R)(y_1, \ldots, y_n) = R(y_{y_{s(1)}}, \ldots, y_{s(n)}$$

and it's easy to show that $\sigma_s \in \mathrm{Aut}\, F$, where $\sigma_s(s_j) = s_j$ and as such, the restriction homomorphism is a bijection

$$\sigma_s \in \mathrm{Gal}(F/E) \cong S_n$$

So for $n \geq 5$, we know that $[S_n, S_n] = A_n$ is simple and non-abelian, thus $\mathrm{Gal}(F/E) = S_n$ is not solvable. By the theorem, it follows that f is not solvable by radicals. □

Corollary 3.8.2. *The polynomial* $f = X^5 - 4X + 2 \in \mathbb{Q}[X]$ *is not solvable by radicals because* $\mathrm{Gal}(f) = S_5$

The abels ruffini corollary does not fully capture the power of the theorem, which says something deeper that just finding roots of polynomials.

4 The Galois Correspondence

One might ask if the inverse of Theorem 3.7 is true, that is: If E/k is a normal extension for a polynomial $f \in k[X]$ and $\mathrm{Gal}(E/k)$ is resolvable, does that mean that f is solvable by radicals?
More generally one might ask if there is a correspondence between subgroups of $\mathrm{Gal}(E/k)$ and sandwiched fields $k \subseteq B \subseteq E$.
It turns out that such a correspondence exists if we impose the property that f be separable. We wish to better understand this correspondence in this chapter.
Looking at the definition of the galois group of an extension E/k, it consists of automorphisms that keep the field k fixed. But what can happen is that the Galois group fixes more points than just k and we want to find out when that is the case.

Definition 4.1. Let E be a field and $H \subseteq \mathrm{Aut}\, E$ a subset. The set

$$E^h := \{a \in E | \sigma(a) = a \forall \sigma \in H\}$$

is a subfield of E called the **fixing field** of H.

Note that the map $H \mapsto E^H$ is contravariant with respect to inclusion

$$H_1 \subseteq H_2 \implies E^{H_2} \subseteq E^{H_1}$$

and if $\langle H \rangle$ is the subgroup generated by H, $E^{<H>} = E^H$.
If H is the galois group of a field extension E/k, then trivially $k \subseteq E^{\mathrm{Gal}(E/k)}$.

Example 4.2. Take for example $k = \mathbb{F}_p(t), f(X) = X^p - t$ and E a splitting field of f. From the $X^p - c$ Lemma, we know that $\mathrm{Gal}(E/k) = \{e\}$, which shows $k \subsetneq E^{\mathrm{Gal}(E/k)} = E$.

If $H < \mathrm{Aut}\, E$ is a finite subgroup, we can find out the order of the extension E/E^H.
In MMP-II, we saw that we can understand a group by studying its character table, where the characters are group homomorphisms of a group G into the circle group $\mathbb{S}^1$. Here we provide a more generalized definition

Definition 4.3. A **character** of a group G in a field E is a group homomorphism $\chi : G \to E^\times$, into the multiplicative group of E.
We denote the set of characters with $\mathrm{Hom}_{\mathsf{Grp}}(G, E^\times)$. And we write

$$F(G, E) = \{\varphi : G \to E\}$$

for the E-vector space of E-valued functions on G.

Also from MMP-II, we know that the characters in $\mathrm{Hom}_{\mathsf{Grp}}(G, \mathbb{S}^1)$ fulfill the orthogonality relation. For arbitrary fields E, we can get a weaker version:

Proposition 4.4 (Dedekind)**.** $\mathrm{Hom}_{\mathsf{Grp}}(G, E^\times) \subseteq F(G, E)$ *is linearly independent.*

Proof. If assume the opposite, then let $n \geq 2$ be the minimal number such that there exists characters $\chi_1, \ldots, \chi_n$ that are linarly dependend in $F(G, E)$, so

$$\exists c_1, \ldots, c_n \in E \setminus \{0\} \text{ with } c_1\chi_1(x) + \ldots + c_n\chi_n(x) = 0 \quad \forall x \in G$$

Since $\chi_1 \neq \chi_2$, there exists a $y \in G$ with $\chi_1(y) \neq \chi_2(y)$. By evaluating the above expressionat $x \cdot y$, we get

$$c_1\chi_1(x)\chi_1(y) + \ldots + c_n\chi_n(x)\chi_n(y) = 0 \quad \forall x \in G$$

and after dividing by $\chi_n(y)$ and subtracting the original equation, we get

$$c_1\left(\frac{\chi_1(y)}{\chi_n(y)} - 1\right)\chi_1(x) + c_2\left(\frac{\chi_2(y)}{\chi_n(y)} - 1\right)\chi_2(x) + \ldots + c_{n-1}\left(\frac{\chi_{n-1}(y)}{\chi_n(y)} - 1\right)\chi_{n-1}(x) = 0$$

but in particular $\frac{\chi_1(y)}{\chi_n(y)} - 1 \neq 0$, which shows that the $\chi_1, \ldots, \chi_{n-1}$ are linearly dependent, in contradiction to the minimality of n. □

We will use this proposition with another lemma to find a lower bound for $[E : E^G]$.

Lemma

Let E be a field and S a set with $\sigma_1, \ldots, \sigma_n \in F(S, E)$ linearly independent.
Then there exist $s_1, \ldots, s_n \in S$ such that the vectors

$$\begin{pmatrix} \sigma_1(s_1) \\ \vdots \\ \sigma_n(s_1) \end{pmatrix}, \ldots, \begin{pmatrix} \sigma_1(s_n) \\ \vdots \\ \sigma_n(s_n) \end{pmatrix}$$

are linearly independent in E^n.

The proof of this is done in the exercise sheet 8.

Lemma 4.5. *Let $H = \{\sigma_1, \dots, \sigma_n\} \subseteq \operatorname{Aut} E$. Then $[E : E^H] \geq n$.*

Proof. The maps $\sigma_1|_{E^\times}, \dots, \sigma_n|_{E^\times}$ are n characters and thus linearly independent in $F(G, E)$ By the sublemma, there exist scalaer $\{y_1, \dots, y_n\} \subseteq E^\times$ such that the vectors

$$(\sigma_1(y_1), \dots \sigma_n(y_1)), \dots, (\sigma_1(y_n), \dots, \sigma_n(y_n))$$

are linearly independent. If we view E as a vector space over the subfield E^H, then we can show that $\{y_1, \dots, y_n\}$ are linearly independnent over E^H, which shows the proof.
Indeed, if we had scalars $c_1, \dots, c_n \in E^H$ that give a linear combination of y_i summing to zero, then these would also give

$$\sum_{i=1}^{n} c_i \sigma_j(y_i) = 0 \quad \forall j = 1, \dots, n$$

but we already know that the vectors above are linearly independent, we would have that the corresponding matrix has full rank. So

$$\begin{pmatrix} \sigma_1(y_1) & \dots & \sigma_1(y_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(y_1) & \dots & \sigma_n(y_n) \end{pmatrix} \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = 0$$

means $c_1 = \dots = c_n = 0$. □

We can now improve the inequality $[E : E^H] \geq |H|$ into an equality with some sensible assumptions.

Proposition 4.6. *Let $G < \operatorname{Aut} E$ be a finite subgroup. Then*

$$[E : E^G] = |G|$$

Proof. We already gave lower bound, so assume that $[E : E^G] > |G|$.
This means that we could find $b_1, \dots, b_m \in E$ linearly independent over E^G for some $m > n$.
If we look at the linear map

$$T : E^m \to E^n, \quad \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} \mapsto \begin{pmatrix} \sigma_1(b_1) & \dots & \sigma_1(b_m) \\ \vdots & & \vdots \\ \sigma_n(b_1) & \dots & \sigma_n(b_m) \end{pmatrix}$$

Because $m > n$ we have that $\operatorname{Ker} T \neq 0$ and with $\sigma\sigma_j = \sigma_{s_i}$ it follows that

$$(x_1, \dots, x_n) \in \operatorname{Ker} T \implies (\sigma(x_1), \dots, \sigma(x_n)) \in \operatorname{Ker} T$$

If we set

$$r := \min\{k | v \in \operatorname{Ker} T \setminus 0 \text{ has a } k\text{-th non-zero coordinate}\}$$

then let $(x_1, \dots, x_m) \int \operatorname{Ker} T$ such that it's r-th coordinate is non-zero.
Without loss of generality, we can assume that $x_1 \neq 0$ and we get that for all $\sigma \in G$, by the definition of r

$$\operatorname{Ker} T \ni \frac{1}{\sigma(x_1)} \begin{pmatrix} \sigma(x_1) \\ \vdots \\ \sigma(x_n) \end{pmatrix} - \frac{1}{x_1} \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = \begin{pmatrix} 0 \\ \sigma(\frac{x_2}{x_1}) - \frac{x_2}{x_1} \\ \vdots \\ \sigma(\frac{x_m}{x_1}) - \frac{x_m}{x_1} \end{pmatrix}$$

So when applying T to this vector, we get that

$$\sum_{j=1}^{m} \sigma_i(b_j)\frac{x_j}{x_1} = 0$$

which, when applied to $\sigma_i = \mathrm{id}$ gives us

$$\sum_{j=1}^{m} b_j\frac{x_j}{x_1} = 0$$

This gves us a non-trivial linear combination of 0, namely

$$b_1 + b_2\frac{x_2}{x_1} + \ldots + b_m + \frac{x_m}{x_1} = 0$$

which is a contradiction.
This proves the upper bound and thus $[E : E^G] = |G|$ □

Corollary 4.6.1. *Let G, H be finite subgroups of* $\mathrm{Aut}\, E$*. Then*

$$E^G \subseteq E^H \iff H < G$$

Proof. By monotoneity of the fixing fields, $\Leftarrow$ is clear
Now assume $E^G \subseteq E^H$ and $H \not\subset G$. Then, there exists a $\sigma \in H$ with $\sigma \notin G$. But since σ fixes every element of E^H it also fixes every element from E^G, and thus $E^G = E^{G\cup\{\sigma\}}$.
With the previous lemma, we get that

$$|G| = [E : E^G] = [E : E^{G\cup\{\sigma\}}] \geq |G| + 1$$

which is a contradiction. □

Recall that the Galois group of a normal extension for a separable polynomial has order $|\mathrm{Gal}(E/k)| = [E : k]$ and that $[E : E^G] = |G|$.

Theorem 4.7. *Let E/k be a finite extension with galois group $G = \mathrm{Gal}(E/k)$. Then the following are equivalent*

(a) E is a splitting field of a separable polynomial in $k[X]$

(b) $E^G = k$

(c) Every irreducible polynomial in $k[x]$ with a root in E is separable and splits over E.

Proof. $\implies$ 2 Since E is a splitting field of a separable polynomial, it follows that $[E : k] = |G|$ and since G is a finite subgroup of $\mathrm{Aut}\, E$, it follows that $[E : E^G] = |G|$. Because $k \subseteq E^G \subseteq E$, we get

$$[E^G : k] = \frac{[E : k]}{[E : E^g]} = 1 \implies E^G = k$$

2 $\implies$ 3 Let $p \in k[x]$ irreducible with a root $\alpha \in E$. Dividing by the leading coefficient, we can also assume that p is unitary (leading coefficient = 1). We define the polynomial

$$q(X) = \prod_{\sigma\in G/\mathrm{Stab}(\alpha)} (X - \sigma(\alpha))$$

and clearly, q is unitary, has degree $|\mathrm{Orb}(\alpha)|$, has no multiple roots, so is separable. Also, because $p \in k[X]$, we see that $p(\sigma(\alpha)) = \sigma(p(\alpha)) = 0$, so $R(q) \subseteq R(p)$.

In execise sheet 8, Problem 1, we have shown that $q \in E^G[X]$. But because by assumption, $E^G = k$, so q divides p. But they are both unitary, so $p = q$ is separable and splits over E.

$3 \implies 1$ Let $k \subseteq E' \subseteq E$ be maximal with the property that E' is a splitting field of a separable polynomial $g \in k[X]$.

Assume that $E \setminus E'$ is nonempty with $\alpha \in E \setminus E'$. Then the minimal polynomial $\mathrm{irr}(\alpha, k) \in k[X]$ is an irreducible polynomial with root α. By assumption, $\mathrm{irr}(\alpha, k)$ is separable and splits over E. Taking the product $f = g \cdot \mathrm{irr}(\alpha, k)$ we see that $f \in k[X]$ is clearly separable and splits in E. If E'' is a splitting field of f, we would get that $E' \subsetneq E'' \subseteq E$, which is a contradiction to the maximality of E'.

□

Definition 4.8. A finite extension E/k is called a **Galois extension** of k, if E is a splitting field of a separable polynomial in $k[X]$. (Or as we have just shown, if $E^G = k$)

Consider extensions $k \subseteq B \subseteq E$. If E/k is Galois for, say a separable polynomial $f \in k[X]$, then we can take the same polynomial $f \in B[X]$ and so E/B is also Galois. However, it does not necessarily follow that B/k is Galois, as it might not even be a normal extension.

Proposition 4.9. *Let $k \subseteq B \subseteq E$ such that E/k is Galois. Then*

$$B/k \text{ is Galois} \iff \sigma(B) = B \quad \forall \sigma \in \mathrm{Gal}(E/k)$$

Proof. If B/k is Galois, then B is a splitting field of a polynomial $f \in k[X]$.
But by Theorem we immediately get $\sigma(B) = B$ for all $\sigma \in \mathrm{Gal}(E/k)$.
Onthe contrary, if $\sigma(B) = B$ for all $\sigma \in \mathrm{Gal}(E/k)$, then consider the image $H < \mathrm{Gal}(B/k)$ of the restriction homomorphism

$$\mathrm{Gal}(E/k) \to \mathrm{Gal}(B/k), \quad \sigma \mapsto \sigma|_B$$

Then we have

$$k \subseteq B^{\mathrm{Gal}(B/k)} \subseteq B^H \subseteq E^{\mathrm{Gal}(E/k)} = k \implies B^{\mathrm{Gal}(B/k)} = k$$

So B/k is Galois. □

Let G be a group and let $\mathrm{Sub}(G)$ be the set of subgroups of G, ordered via inclusion. If E/k is a field extensions, then write

$$\mathrm{Int}(E/k) = \{\text{fields } B | k \subseteq B \subseteq E\}$$

for the set of intermediary field extensions between E and k. This set is also orded via inclusion.

Theorem 4.10 (Galois correspondence)**.** *Let E/k be a finite Galois extension.*

(a) The map

$$\gamma : \mathit{Sub}(\mathrm{Gal}(E/k)) \to \mathrm{Int}(E/k), \quad H \mapsto E^H$$

is a contravariant bijection with inverse map

$$\delta : \mathrm{Int}(E/k) \to \mathit{Sub}(\mathrm{Gal}(E/k)), \quad B \mapsto \mathrm{Gal}(E/B)$$

(b) $B \in \mathrm{Int}(E/k)$ is Galois if and and only if $\mathrm{Gal}(E/B)$ is a normal subgroup of $\mathrm{Gal}(E/k)$. If that is the case, then

$$\mathrm{Gal}(E/k)/\mathrm{Gal}(E/B) \cong \mathrm{Gal}(B/k)$$

Proof. Recall the Corollary where we showed that if E is a field and H, G are finite subgroups of $\operatorname{Aut} E$, then

$$E^G \subseteq E^H \iff H < G$$

(a) To show injectivity, let H_1, H_2 be subgroups of $\mathrm{Gal}(E/k)$. In particular, H_1, H_2 are finite subgroups of $\operatorname{Aut} E$. Then if $E^{H_1} = E^{H_2}$, the corollary immediately gives $H_1 = H_2$.

For surjectivity, we show that $\gamma \circ \delta = \mathrm{id}_{\mathrm{Int}(E/k)}$. Let $k \subseteq B \subseteq E$. Since E/k Galois $\implies$ E/B Galois, we have

$$(\gamma \circ \delta)(B) = \gamma(\mathrm{Gal}(E/B)) = E^{\mathrm{Gal}(E/B)} = B$$

(b) Assume first that B/k is Galois. In particular, it is normal and by Theorem II-26, we know that $\sigma(B) = B \forall \sigma \in \mathrm{Gal}(E/k)$. And since $\mathrm{Gal}(E/B)$ is the kernel of the restriction mapping

$$\mathrm{Gal}(E/k) \to \mathrm{Gal}(B/k), \quad \sigma \mapsto \sigma|_B$$

it is a normal subgroup. And by the first isomorphism theorem, we get $\mathrm{Gal}(E/k)/\mathrm{Gal}(E/B) \cong \mathrm{Gal}(B/k)$.

On the other hand, assume that $\mathrm{Gal}(E/B)$ is a normal subgroup. We want to show that B/k is Galois, i.e. $B^{\mathrm{Gal}(B/k)} = k$.

To do this, we use the characterisation from Proposition IV-14, which tells us that it suffices to show $\sigma(B) = B \forall \sigma \in \mathrm{Gal}(E/k)$.

Since E/k is Galois, we also get that E/B is Galois, so $E^{\mathrm{Gal}(E/B)} = B$. Let $\sigma \in \mathrm{Gal}(E/k), \xi \in B, h \in \mathrm{Gal}(E/B)$. We show that

$$\sigma(\xi) \in B \iff h(\sigma(\xi)) = \sigma(\xi)$$

But that is clear because

$$h\sigma(\xi) = \sigma((\sigma^{-1}h\sigma\xi) = \sigma(\xi)$$

□

Example 4.11. The polynomial $f = X^3 - 2 \in \mathbb{Q}[X]$ is irreducible and let $E \subseteq \mathbb{C}$ be the splitting field of f.
Since the degree of the extension is 6, we know that $\mathrm{Gal}(E/\mathbb{Q}) \cong S_3$. For $\beta = \sqrt[3]{2} \in \mathbb{R}$ and $\omega = e^{\frac{2\pi i}{3}}$, the roots of f are

$$\alpha_1 = \beta, \alpha_2 = \beta\omega, \alpha_3 = \beta\omega^2$$

Since the galois group acts transitively, let $\sigma_{ij} \in S_3$ be the automorphism that transposes α_i and α_j and let $\tau \in S_3$ be the cyclic permutation of the roots.
Then the correspondence with the subgroups and the subfields are

$$\langle\sigma_{12}\rangle \sim \mathbb{Q}(\alpha_3), \quad \langle\sigma_{13}\rangle \sim \mathbb{Q}(\alpha_2), \quad \langle\sigma_{23}\rangle \sim \mathbb{Q}(\alpha_1), \quad \langle\tau\rangle \sim \mathbb{Q}(\omega)$$

The Galois correspondence has many simple consequences

Corollary 4.11.1. *A finite Galois extension has only finitely many subfields.*

Definition 4.12. A field extension E/k is called **simple** if there exists an $u \in E$ such that $E = k(u)$

Proposition 4.13. *A finite extension E/k is simple if and only if there exist finitely many subfields.*

Proof. Assume there are only finitely many subfields.

- If k is infinite, then E as a k-vectorspace cannot be the union of its finitely mans subfields. (See Exercise sheet 8 Problem 4).

  So there exists an element $u \in E$ that is not contained in any subfield, which shows $E = k(u)$
- If k is finite, then $k = \mathbb{F}_q$ and $E = \mathbb{F}_{q^n}$ for $n = [E : k]$, which means that we can an element u that generates $\mathbb{F}_{q^n}^\times$.

On the other hand let $E = k(u)$ and $k \subseteq F \subseteq E$ an interior field. Then let

$$f_F(T) = \operatorname{irr}(x, F)(T) = T^n + a_{n-1}^{T^{n-1}} + \ldots + a_0 \in F[T]$$

then let $F_0 = k(a_{n-1}, \ldots, a_0) \subseteq F$. Since f_F is irreducible in $F[T]$ it is also irreducible in $F_0(T)$ and so

$$[E : F] = [F(x), F] = n, \quad [E : F_0] = [F_0(x), F_0] = n \implies F = F_0$$

Note that $\operatorname{irr}(x, F)$ divides $\operatorname{irr}(x, k)$ in $E[T]$. Then the number of inteior fields $\leq$ the number of polynomials in $E[T]$ that divide $\operatorname{irr}(x, k)$. □

Corollary 4.13.1. *A finite Galois extension E/k is always simple.*

Example 4.14. Set $E = \mathbb{F}_p(X, Y)$ and $k = \mathbb{F}_p(X^p, Y^p)$. Clearly $[E.k] = p^2$ and there does not exist an $x \in E$ such that $E = k(x)$, but there are infinitely many subfields.

Theorem 4.15. *Let E/k be a finite Galois extension with* $\operatorname{char} k = 0$. *If* $\operatorname{Gal}(E/k)$ *is resolvable, then E is contained in a radical extension of k.*

We first show that there exists a normal divisor $N \lhd \operatorname{Gal}(E/k)$ of index p for some prime p and prove the theorem a bit later.

Proof claim. Because G is finite and resolvable then $[G, G] \nsubseteq G$. and $G/[G, G]$ is a finite abelian group $\neq \{e\}$. By the classification theorem of finite abelian groups (See Algebra I), it can be written as a product of $\mathbb{Z}/p^n\mathbb{Z}$ for primes p and $n \geq 1$.
Because any inclusion $\mathbb{Z}/p^n\mathbb{Z} \supseteq \mathbb{Z}/p^{n-1}\mathbb{Z}$ has index p, we see that $G/[G, G]$ contains a subgroup M of index p. Let

$$\rho : G \to G/[G, G], \quad \text{and} \quad N := \rho^{-1}(M)$$

Then $N \lhd G$ has index p aswell.
Clearly, E^N/k is a Galois extension of degree p. □

Lemma 4.16. *Let E/k be a finite Galois extension with $[E : k] = p$ for some prime p. If k contains a p-th root ω of 1 with $\omega \neq 1$, then*

$$\exists \xi \in E \quad \textit{with} \quad \xi^p \in k \quad E = k(\xi)$$

Proof. First note that $\mathrm{Gal}(E/k)$ is cyclical of order p, so let $\sigma \in \mathrm{Gal}(E/k)$ be a generator of the group.
Viewing $\sigma : E \to E$ as a k-linear map that satisfies $\sigma^p = \mathrm{id}_E$, we claim that $X^p - 1$ is the minimal polynomial of σ.
If there is a smaller polynomial $P = \sum_{i=0}^{p-1} a_i X^i \in k[X]$ with degree $\deg P \leq p-1$ and $P(\sigma) = 0$, then this means

$$\sum_{i=0}^{p-1} a_i \sigma^i = 0$$

but since $\mathrm{id}_E, \sigma, \ldots, \sigma^{p-1}$ are characters $\mathrm{Hom}(E^\times, E^\times)$, they are linearly independent in $F(E^\times, E)$ (by **??**), which means $P = 0$.
Therefore, $X^p - 1$ is the characteristic polynomial of σ and $\omega \in k$ is an eigenvalue of σ.
Let $\xi \in E^\times$ be an eigenvector $\sigma(\xi) = \omega \cdot \xi$. Since $\omega \neq 1$, it must follow that $\xi \in k$ and thus $E = k(\xi)$.
Moreover, $\sigma(\xi^p) = \sigma(\xi)^p = \omega^p \xi^p = \xi^p$. And since σ generates the Galoisgroup, we have $\xi^p \in E^{\mathrm{Gal}(E/k)} = k$. □

Now we are ready to prove the theorem 4.15

Proof Theorem. Let E/k be Galois with $\mathrm{Gal}(E/k)$ resolvable.
We use induction on $[E : k]$. If $[E : k] = 1$ it's clear.
Assume $[E : k] \geq 2$, so $|\mathrm{Gal}(E/k)| = [E : k] \geq 2$.
We have shown earlier in the claim that there exists a normal divisor $N \lhd \mathrm{Gal}(E/k)$ of index p for some prime p.
Since $k \subseteq E^N$, the field E^N/k is a Galois extension of degree p. Let k^*/k be the splitting field of $X^p - 1 \in k[X]$ and $\omega \in k^*$ be a generator of all p-th roots of unity. (i.e. $\omega \neq 1$).

- If $\omega \in k$, then by Lemma 4.16, E^N/k is a pure extension and $[E : E^N] < [E : k]$ and $\mathrm{Gal}(E/E^N) = N$.
  Since $N < \mathrm{Gal}(E/k)$ is a subgroup of a resolvable group, it is also resolvable, and by induction hypthesis we get a tower of pure extensions

  $$E^N = K_1 \subseteq K \subset \ldots \subset K_t$$

  Therefore we see that

  $$k \subseteq E^N = K_1 \subseteq K_2 \subseteq \ldots \subseteq K_t$$

  where K_t is a radical extension of k that contains E.

- If $\omega \notin k$, then we define $E^* = E(\omega)$ and we get the diagram

  $$\begin{array}{ccc} k & \hookrightarrow & k^* \\ \downarrow & & \downarrow \\ E & \hookrightarrow & E^* = E(\omega) \end{array}$$

□

5 Cyclotomic fields

Let $n \geq 1 \in \mathbb{N}$, k a field and $k[n]$ a spiltting field of $f := X^n - 1 \in k[X]$. Let $\mu_n \subseteq k[n]$ be the roots of f. Then μ_n is a finite subgroup of $k[n]^\times$ and therefore cyclic. We call a generator of the group an n-th primitive root of unity.
If $\xi \in \mu_n$ is an n-th primitive root of unity, then $k[n] = k(\xi)$.
When we assume that $\operatorname{char} k = 0$ or $\operatorname{char} k \not| n$, then f and its derivative f' have $\gcd(f, f') = 1$, so the polynomial has no multiple roots.
So f is separable and $k[n]/k$ is a Galois extension. We now wish to compute $\mathrm{Gal}(k[n]/k)$. Let ξ an n-th primitve root of unity and consider the map

$$\mathbb{Z}/n\mathbb{Z} \to \mu_n, \quad k \mapsto \xi^k$$

Then we can describe a $\sigma \in \mathrm{Gal}(k[n]/k)$ with some $a_\sigma \in \mathbb{Z}/n\mathbb{N}$ such that $\sigma(\xi) = \xi^{a_\sigma}$ which means $a_\sigma \in (\mathbb{Z}/n\mathbb{Z})^\times$.
This gives us an injective group homomorphism

$$\mathrm{Gal}(k[n]/k) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times, \quad \sigma \mapsto a_\sigma$$

and we can ask wheter this map is surjective.

Theorem 5.1. *For $k = \mathbb{Q}$, the map*

$$\mathrm{Gal}(\mathbb{Q}[n]/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times, \quad \sigma \mapsto a_\sigma$$

is an isomorphism.

There are many different proofs for this, but an elementary one comes from Dedekind, which uses Gauss's Lemma.

Lemma 5.2 (Gauss)**.** *If a polynomial $p \in \mathbb{Z}[X]$ is a product of polynomials $P, R \in \mathbb{Q}[X]$, then there exist $\lambda, \mu \in \mathbb{Q}^\times$ such that*

$$q := \lambda Q \in \mathbb{Z}[X], r := \mu R \in \mathbb{Z}[X] \text{ and } p = q \cdot r$$

if additionally, p, Q, R are unitary, then $R, Q \in \mathbb{Z}[X]$.

Proof theorem. Let $\xi, \xi^a \in \mu_n$ be n-th primitve roots of unity (which means $\gcd(a, n) = 1$).
To show surjectivity of the map, we show that there exists a $\sigma \in \mathrm{Gal}(\mathbb{Q}[n]/\mathbb{Q})$ such that $\sigma(\xi) = \xi^a$.
Let $f = \mathrm{irr}(\xi, \mathbb{Q}), g = \mathrm{irr}(\xi^a, \mathbb{Q})$ be the minimal polynomials. Then we can show that $f = g$.
Indeed, if we assume $f \neq g$ then because both divide $X^n - 1$, they are irreducible factors. So we can write $X^n - 1 = f \cdot g \cdot h$ for some h unitary. By Gauss's Lemma, we get that $f, g, h \in \mathbb{Z}[X]$.
Reducing modulo p, we get $X^n - 1 = \overline{f} \cdot \overline{g} \cdot \overline{h}$ for $\overline{f}, \overline{g}, \overline{h} \in \mathbb{F}_p[X]$. Since $X^n - 1$ has no multiple roots, it follows that $\gcd(\overline{f}, \overline{g}) = 1$.
By decomposing a into primes: $a = p_1 \dots p_r$ we can assume without loss of generality that a is prime, and show that $\mathrm{irr}(\xi, \mathbb{Q}) = \mathrm{irr}(\xi^p, \mathbb{Q})$ for any $\xi \in \mu_n$ and p prime, because we can extend this argument with

$$\mathrm{irr}(\xi, \mathbb{Q}) = \mathrm{irr}(\xi^{p_1}, \mathbb{Q}) = \mathrm{irr}((\xi^{p_1})^{p_2}, \mathbb{Q}) = \dots = \mathrm{irr}(\xi^a, \mathbb{Q})$$

So let $f = \mathrm{irr}(\xi, \mathbb{Q})$ and $g = \mathrm{irr}(\xi^p, \mathbb{Q})$ for some prime p. Because $g(\xi^p) = 0$, we know that ξ is a root of $g(X^p) \in \mathbb{Z}[X]$ and since f is the minimal polynomial of ξ, ewe can factor

$$g(X^p) = f(X)k(X) \quad \text{for some} \quad k \in \mathbb{Q}[X] \text{ unitary}$$

by Gauss' Lemma, $k \in \mathbb{Z}[X]$ and we have

$$(\overline{g}(X))^p = \overline{g}(X^p) = \overline{f}(X)\overline{k}(X)$$

which contradicts $\gcd(\overline{f}, \overline{g}) = 1$.
So now that we know $f = g = \mathrm{irr}(\xi, \mathbb{Q})$, the proof follows because we have that ξ and ξ^a are both roots of f and $\mathbb{Q}[n]$ is a splitting field of f. And from Corollary 2.16.1, we know that the Galois group of a splitting field over a separable, irreducible polynomial acts transitively over the roots, i.e. $\exists \sigma \in \mathrm{Gal}(\mathbb{Q}[n]/\mathbb{Q})$ with $\sigma(\xi) = \xi^p$. □

With the identity

$$\frac{X^{n+1} - 1}{X - 1} = 1 + X + \ldots + X^n$$

we can

Definition 5.3. Let ξ be an n-th primitve root of unity. We define the n-th **cyclotomic polynomial** as

$$\Phi_n(X) := \prod_{\substack{\gcd(a,n)=1 \\ 1 \le a \le n-1}} (X - \xi^a)$$

Corollary 5.3.1. $\Phi_n \in \mathbb{Z}[X]$ *and is irreducible in* $\mathbb{Q}[X]$

Proof. As we have shown earlier, the splitting field is $\mathbb{Q}[n] = \mathbb{Q}(\xi)$ and by the previous theorem the definition is equivalent to

$$\Phi_n(X) = \prod_{\sigma \in \mathrm{Gal}(\mathbb{Q}[n]/\mathbb{Q})} (X - \sigma(\xi))$$

Note that all its coefficients are in the fixing field $\mathbb{Q}[n]^{\mathrm{Gal}(\mathbb{Q}[n]/\mathbb{Q})}$, but since it has no multiple roots and is thus separable, the fixing field is $\mathbb{Q}$, which shows $\Phi_n \in \mathbb{Q}[X]$.
Moreoever, since $\Phi_n(X)$ divides $X^n - 1$, it follows from Gauss' Lemma that $\Phi_n \in \mathbb{Z}[X]$.
It is also irreducible because by definition, $\mathrm{Gal}(\mathbb{Q}[n]/\mathbb{Q})$ acts transitivitely on its roots. (We use 2.16.1 here) □

Remark 5.4. The degree of Φ_n is equal to the number of relative primes $1 \le a \le n$, or Euler's totient function $\varphi(n)$. In particular, if p is prime, $\Phi_p(X) = X^{p-1} + \ldots + X + 1$.
Fun fact: Φ_{105} is the first cyclotomic polynomial, which has a coefficient *not* equal to $1, 0, -1$. (That is because $105 = 3 \cdot 5 \cdot 7$ is the smallest product of three distict odd primes.)

In the exercise Sheets, we prove the following.

Proposition 5.5. *The cyclotomic polynomials have the following properties: Let p be prime and $n \in \mathbb{N}$*

(a) $X^n - 1 = \prod_{d|n} \Phi_d(X)$

(b) $\Phi_p(X) = X^{p-1} + X^{p-2} + \ldots + 1$

(c) If $n \ge 2$: $\Phi_n(X) = X^{\varphi(n)}\Phi_n(X)$

(d) $\Phi_{p^r} = \Phi_p(X^{p^{r-1}})$

(e) If $\gcd(p,n)=1$*, then*

$$\Phi_{pn}(X)=\frac{\Phi_n(X^p)}{\Phi_n(X)}$$

(f) $\Phi_N(X)=\prod_{d|n}(X^{\frac{n}{d}}-1)^{\mu(d)}$*, where* μ *is the Moebius function*

$$\mu:\mathbb{N}^*\to\{-1,0,1\},\quad \mu(n)=\begin{cases}0 & \text{if } n \text{ divisible by a square of a prime}\\ (-1)^r & n=p_1\dots p_r \text{ pairwise different}\\ 1 & n=1\end{cases}$$

Theorem 5.6. *If* $\gcd(p,n)=1$*, then the image of the map*

$$\mathrm{Gal}(\mathbb{F}_p[n]/\mathbb{F}_p)\to(\mathbb{Z}/n\mathbb{Z})^\times,\sigma\mapsto a \text{ with } \sigma(\xi)=\xi^a$$

is the subgroup generated by $p \mod n$*.*

Proof. We know that $\mathrm{Gal}(\mathbb{F}_p[n]/F_p)$ is generated by the Frobenius automorphism $\varphi_p(\xi)=\xi^p$. Applying it to ξ, an n-th primitive root of 1 we see that

$$\varphi_p\xi\mapsto p\in(\mathbb{Z}/n\mathbb{Z})^\times$$

□

Corollary 5.6.1. *If* $\gcd(p,n)=1$*, then* $[\mathbb{F}_p[n]:\mathbb{F}_p]$ *is a power of* p *modulo* n*.*

To better understand what the group $\mathbb{Z}/n\mathbb{Z}^\times$ is like we show that we can decompose it into smaller copies, if n is not a prime.

Theorem 5.7. *If* $\gcd(n,m)=1$*, then*

$$(\mathbb{Z}/mn\mathbb{Z})^\times\cong(\mathbb{Z}/m\mathbb{Z})^\times\times(\mathbb{Z}/n\mathbb{Z})^\times$$

and if p *is prime* >2*, then*

$$(\mathbb{Z}/p^r\mathbb{Z})^\times\cong\mathbb{Z}/p^{r-1}\times\mathbb{Z}/(p-1)\mathbb{Z}$$

in particular, we have

$$(\mathbb{Z},2^r\mathbb{Z})^\times\cong\mathbb{Z}/2\mathbb{Z}\times(\mathbb{Z}/2^{r-2}\mathbb{Z})$$

For example we can calculate $(\mathbb{Z}/7\mathbb{Z})^\times=\{1,2,3,4,5,6\}\cong\mathbb{Z}/6\mathbb{Z}$ The possible exponents are $1,2,3,6$.

- For $p=2$, we have $2^3=8=1 \mod 7$ and thus $[\mathbb{F}_p[7]:\mathbb{F}_2]=3$ with
$$\Phi_7(T)=(T^3+T+1)(T^3+T^2+)\in\mathbb{F}_[T]$$
- For $p=3$, we need exponent 6, and Φ_7 is irreducible mod 3.
- The prime $p=13$, is of order 2, because $13^2=24\cdot7+1$. We then have
$$\Phi_7(T)=(T^2+3T+1)(T^2+5T+1)(T^2+6T+1)$$

- $p = 29$ is of order 1 and

$$\Phi_7(T) = (T-7)(T-16)(T-20)(T-23)(T-24)(T-25)$$

Theorem 5.8. *If* $\gcd(p,n) = 1$*, then the unitary irreducible factors of* Φ_n *if* $\mathbb{F}_p[X]$ *are all different and have the same degree of order* $p \mod n$ *in* $(\mathbb{Z}(n\mathbb{Z})^\times$.

Proof. Because $X^n - 1$ has no multiple roots the same holds for $\Phi_n(X)$, therefore all irreducible factors have to be different.
Since $\mathbb{F}_p[n]$, is a splitting field of $X^n - 1$, we have that $\Phi_n(X)$ splits into linear factors in $\mathbb{F}_p[n][X]$, so the irreducible factors of $\Phi_n(X)$ must be of the FOrm $\mathrm{irr}(\alpha, \mathbb{F}_p)$ for some $\alpha \in \mathbb{F}_p[n]$ with $\Phi_n(\alpha) = 0$.
So it suffices to show that if $\Phi_n(\alpha) = 0$, then α must be a primitive n-th root of unity. From this, it would follow that $\mathbb{F}_p[n] = \mathbb{F}_p(\alpha)$ and the minimal polynomial $\mathrm{irr}(\alpha, \mathbb{F}_p)$ has degree $[\mathbb{F}_p[n] : \mathbb{F}_p]$.
Now assume that α is *not* a primitive n-th root of unity with $\Phi_n(\alpha) = 0$.
Then there exists a $1 \leq m < n$ with $\alpha^m = 1$ and suc that m divides n. And we can write

$$0 = X^m - 1 = \prod_{l|m} \Phi_d(X)$$

so there has to be a $d_0|m$ with $\Phi_{d_0}(\alpha) = 0$. But we can also write

$$X^m - 1 = \Phi_n(X) \prod_{d|n, d<n} \Phi_d(X)$$

so since d_0 divides m and is a true divisor of n we have that α must be a root of multiplicity at least two. □

Dirichlet proved that given some $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, there are finitely primes p with $p = a \mod n$.

Missing Second Half 28.05.21