Galois theory

1. | Introduction

Solvability of quadratic, cubic and quartic polynomials

Definition 1. A *quadratic polynomial* over a field K is a function of the form:

$$p(x) = ax^2 + bx + c$$

where $a, b, c \in K$. A *cubic polynomial* over a field K is a function of the form:

$$p(x) = ax^3 + bx^2 + cx + d$$

where $a, b, c, d \in K$. A *quartic polynomial* over a field K is a function of the form:

$$p(x) = ax^4 + bx^3 + cx^2 + dx + e$$

where $a, b, c, d, e \in K$.

Lemma 2. Let K be a field, $n \geq 2$ and

$$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

where $a_i \in K$ for $i = 0, \ldots, n-1$. Then, the change of variable $x = u - \frac{a_{n-1}}{n}$ transforms the previous equation into

$$p(u) = u^n + b_{n-2}u^{n-2} + \cdots + b_1 u + b_0$$

for some $b_i \in K$ for $i = 0, \ldots, n-1$. This new equation is called *depressed equation*.

Proposition 3. The solutions of the quadratic polynomial $x^2 + bx + c$ are:

$$\frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

Proposition 4. The solutions of the cubic depressed polynomial $x^3 + px + q$ are:

$$\alpha + \beta := \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

where the cubic roots are chosen such that $\alpha\beta = -p/3$.

Proposition 5. The solutions of the quartic depressed polynomial $x^4 + ax^2 + bx + c$ are:

$$-S \pm \frac{1}{2}\sqrt{-4S^2 - 2a + \frac{b}{S}} \quad \text{and} \quad S \pm \frac{1}{2}\sqrt{-4S^2 - 2a - \frac{b}{S}}$$

where

$$S = \frac{\sqrt{-\frac{2}{3}a + \frac{1}{3}\left(Q + \frac{\Delta_0}{Q}\right)}}{2} \qquad Q = \sqrt[3]{\frac{\Delta_1 + \sqrt{{\Delta_1}^2 - 4{\Delta_0}^3}}{2}}$$

$$\Delta_0 = a^2 + 12c \qquad \Delta_1 = 2a^3 + 27b^2 - 72ac$$

Rings, integral domains and fields

Proposition 6.

1. A subring of an integral domain is an integral domain.
2. A field is an integral domain.
3. A subring of a field is an integral domain.

Lemma 7. Let K be a field and $R \neq \{0\}$ be a ring. Then, all ring morphisms $f : K \to R$ are injective.

Definition 8. Let K, L be fields. A *field morphism* between K and L is a ring morphism $K \to L$.

Lemma 9. Let R be a ring. Then, there exists a unique ring morphism $f : \mathbb{Z} \to R$ satisfying:

- $f(1 + \overset{(n)}{\cdots} + 1) = 1_R + \overset{(n)}{\cdots} + 1_R$ if $n \geq 1$.
- $f(n) = -f(-n)$ if $n \leq -1$.

Definition 10. Let R be a ring and $f : \mathbb{Z} \to R$ be the ring morphism from $\mathbb{Z}$ to R. The *characteristic* of R, $\operatorname{char}(R)$, is defined to be the value of n such that $\ker f = \mathbb{Z}/n\mathbb{Z}$.

Proposition 11. Let K be a field. Then, either $\operatorname{char} K$ is prime or $\operatorname{char} K = 0$.

Definition 12. Let R be a ring. We define the *polynomial ring* $R[x]$ as:

$$R[x] := \{r_0 + r_1 \cdot x + \cdots + r_n \cdot x^n : r_i \in R \ \forall i \text{ and } n \geq 0\}$$

Moreover, we can iterate this definition to define the polynomial ring in m unknowns:

$$R[x_1, \ldots, x_m] = (R[x_1, \ldots, x_{m-1}])\,[x_m]$$

Proposition 13 (Universal property of polynomials in several variables). Let R, S be two rings, $f : R \to S$ be a ring morphism and $s_1, \ldots, s_n \in S$ be not necessarily distinct elements of S. Then, the function $\varphi_{s_1,\ldots,s_n} : R[x_1, \ldots, x_n] \to S$ defined by

$$\varphi_{s_1,\ldots,s_n}\left(\sum_{i_1,\ldots,i_n \geq 0} r_{i_1,\ldots,i_n} {x_1}^{i_1} \cdots {x_n}^{i_n}\right) = \\ = \sum_{i_1,\ldots,i_n \geq 0} f(r_{i_1,\ldots,i_n}) {s_1}^{i_1} \cdots {s_n}^{i_n}$$

is the unique ring morphism such that $\varphi_{s_1,\ldots,s_n}(r) = f(r)$ $\forall r \in R$ and $\varphi_{s_1,\ldots,s_n}(x_i) = s_i$ for $i = 1, \ldots, n$. This function is called *evaluation* of $s_1, \ldots, s_n$ through f.

Field of fractions

Theorem 14 (Universal property of the field of fractions). All integral domains are a subring of a field. More explicitly, if R is an integral domain and K is a field, there exists another field $Q(R)$[1] and an injective ring morphism $\iota : R \hookrightarrow Q(R)$ so that for all injective ring morphism $f : R \hookrightarrow K$, there exists a unique field morphism $\psi_f : Q(R) \to K$ defined by

$$\begin{aligned} \psi_f : Q(R) &\longrightarrow K \\ \frac{a}{b} &\longmapsto f(a)f(b)^{-1} \end{aligned}$$

such that $f = \psi_f \circ \iota$.

Corollary 15. Let R be an integral domain. The field $Q(R)$ with the injection ι is unique up to isomorphism, that is, if there is a field $Q'(R)$ and an injective ring morphism $\iota' : R \hookrightarrow Q'(R)$ satisfying the property of above, then there is a unique isomorphism $\psi_{\iota'} : Q(R) \cong Q'(R)$ such that $\iota' = \psi_{\iota'} \circ \iota$, where $\iota : R \hookrightarrow Q(R)$. This field $Q(R)$ is called *field of fractions* of R.

Definition 16. Let K be a field. The field of fractions of $K[x]$ is defined as $K(x) := Q(K[x])$ and it is called *field of rational functions*. More generally, the field of fractions of $K[x_1, \dots, x_n]$ is defined as:

$$K(x_1, \dots, x_n) := Q(K[x_1, \dots, x_n])$$

The elements of $K(x_1, \dots, x_n)$ are of the form:

$$\left\{ \frac{p(x_1, \dots, x_n)}{q(x_1, \dots, x_n)} : p, q \in K[x_1, \dots, x_n] \right\}$$

Lemma 17. Let R be an integral domain. Then, $R[x]$ is also an integral domain and:

$$Q(R[x]) \cong Q(R)(x)$$

Corollary 18. Let K be a field. For all $n \geq 2$ we have:

$$K(x_1, \dots, x_n) \cong K(x_1, \dots, x_{n-1})(x_n)$$

Subring and subfield generated by a set

Definition 19. Let $(R, +, \cdot)$ be a ring and $X \subseteq R$ be a subset of R. Let

$$P := \{S \subseteq R : X \subseteq S \wedge (S, +, \cdot) \leq (R, +, \cdot)\}$$

Then, the *subring generated* by X is the smallest subring of $(R, +, \cdot)$ containing X. That is:

$$\langle X \rangle_{\text{ring}} = \bigcap_{S \in P} S$$

Definition 20. Let R be a ring, $S \subseteq R$ be a subring of R and $A \subseteq R$ be a subset of R. We denote by $S[A]$ the smallest subring of R containing S and A.

Lemma 21. Let A be a finite set, R and S be rings and $\varphi : R[x_a : a \in A] \to S$ be the evaluation morphism such that $\varphi(r) = r \ \forall r \in R$ and $\varphi(x_a) = a \ \forall a \in A$. Then, $S[A] = \operatorname{im} \varphi$.

Definition 22. Let $(K, +, \cdot)$ be a field and $X \subseteq K$ be a subset of K. Let

$$P := \{L \subseteq K : X \subseteq L, (L, +, \cdot) \text{ is a subfield of } (R, +, \cdot)\}$$

Then, the *subfield generated* by X is the smallest subfield of $(K, +, \cdot)$ containing X. That is:

$$\langle X \rangle_{\text{field}} = \bigcap_{L \in P} L$$

Definition 23. Let L be a field, $K \subseteq L$ be a subfield of L and $A \subseteq L$ be a subset of L. We denote by $K(A)$ the smallest subfield of L containing K and A.

Symmetric polynomials

Definition 24 (Symmetric polynomials). Let R be a ring, $n \in \mathbb{N}$ and $p \in R[x_1, \dots, x_n]$. We say that p is a *symmetric polynomial* if $\forall \sigma \in \mathrm{S}_n$, we have that $p(x_1, \dots, x_n) = p(x_{\sigma(1)}, \dots, x_{\sigma(n)})$. We denote by $R[x_1, \dots, x_n]^{\mathrm{S}_n}$ the set of all symmetric polynomials over $R[x_1, \dots, x_n]$.

Definition 25. Let R be a ring and $n \in \mathbb{N}$. We define the *elementary symmetric polynomials* $s_1, \dots, s_n$ as:

$$s_k = \sum_{1 \leq i_1 < \cdots < i_k \leq n} x_{i_1} \cdots x_{i_k} \quad \text{for } k = 1, \dots, n$$[2]

Definition 26. Let $n \in \mathbb{N}$. We define the *lexicographic order* $<_{\text{lex}}$ in $\mathbb{N}^n$ as:

$$\begin{aligned} (a_1, \dots, a_n) <_{\text{lex}} (b_1, \dots, b_n) &\iff \\ &\iff \exists j \in \mathbb{N} : a_1 = b_1, \dots, a_j = b_j, a_{j+1} < b_{j+1} \end{aligned}$$

Proposition 27. The pair $(\mathbb{N}^n, <_{\text{lex}})$ is a totally ordered set. Moreover, if $x, y, z, t \in \mathbb{N}^n$ are such that $x <_{\text{lex}} y$ and $z <_{\text{lex}} t$, then $x + z <_{\text{lex}} y + t$.

Definition 28. Let R be a ring, $n \in \mathbb{N}$ and $p \in R[x_1, \dots, x_n]$. Suppose p is of the form:

$$p(x_1, \dots, x_n) = \sum_{\substack{i_1, \dots, i_n = 1 \\ i_1 + \cdots + i_n = n}}^{n} a_{i_1, \dots, i_n} {x_1}^{i_1} \cdots {x_n}^{i_n}$$

If $p(x_1, \dots, x_n) \neq 0$, we define the *lexicographic degree* of p as:

$$\deg_{<_{\text{lex}}}(p) := \max_{<_{\text{lex}}} \{(i_1, \dots, i_n) : a_{i_1, \dots, i_n} \neq 0\}$$[3]

If $p(x_1, \dots, x_n) = 0$, we define $\deg_{<_{\text{lex}}}(p) := -\infty$.

Proposition 29. Let R be a ring, $n \in \mathbb{N}$ and $p, q \in R[x_1, \dots, x_n]$. Then:

1. $\deg_{<_{\text{lex}}}(p + q) \leq \max\{\deg_{<_{\text{lex}}}(p), \deg_{<_{\text{lex}}}(q)\}$.
2. $\deg_{<_{\text{lex}}}(pq) = \deg_{<_{\text{lex}}}(p) + \deg_{<_{\text{lex}}}(q)$.

[1] Recall **??** for a formal definition of the field $Q(R)$.

[2] For example, for $n = 3$ we have: $s_1 = x_1 + x_2 + x_3$, $s_2 = x_1x_2 + x_1x_3 + x_2x_3$ and $s_3 = x_1x_2x_3$.

[3] Here, the notation $\max_{<_{\text{lex}}}$ means that the maximum is taken with respect to the order $<_{\text{lex}}$.

Lemma 30 (Waring's method). Let R be an integral domain and $p \in R[x_1, \dots, x_n]^{S_n}$. Suppose that $\deg_{<_{\text{lex}}}(p) = (a_1, \dots, a_n)$ and let $\lambda \in R \setminus \{0\}$ be the coefficient of ${x_1}^{a_1} \cdots {x_n}^{a_n}$ in $p(x_1, \dots, x_n)$. Then, $a_1 \geq \cdots \geq a_n$ and if

$$q := p - \lambda {s_n}^{a_n} {s_{n-1}}^{a_{n-1}-a_n} {s_{n-2}}^{a_{n-2}-a_{n-1}} \cdots {s_1}^{r_1-r_2}$$

then we have $\deg_{<_{\text{lex}}}(q) <_{\text{lex}} \deg_{<_{\text{lex}}}(p)$.

Theorem 31 (Fundamental theorem of symmetric polynomials). Let R be a ring and $n \in \mathbb{N}$. Then:

$$R[x_1, \dots, x_n]^{S_n} = R[s_1, \dots, s_n]$$

That is, every polynomial in $R[x_1, \dots, x_n]^{S_n}$ can be expressed uniquely in terms of elementary symmetric polynomials.

Cyclotomic polynomials

Definition 32. We define the *n-th cyclotomic polynomial* as the unique irreducible polynomial $\Phi_n(x) \in \mathbb{Z}[x]$ such that $\Phi_n(x) \mid x^n - 1$ and $\Phi_n(x) \nmid x^m - 1$ for all $m < n$. For example, the first 8 cyclotomic polynomials are:

$$\begin{aligned}
\Phi_1(x) &= x - 1 \\
\Phi_2(x) &= x + 1 \\
\Phi_3(x) &= x^2 + x + 1 \\
\Phi_4(x) &= x^2 + 1 \\
\Phi_5(x) &= x^4 + x^3 + x^2 + x + 1 \\
\Phi_6(x) &= x^2 - x + 1 \\
\Phi_7(x) &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\
\Phi_8(x) &= x^4 + 1
\end{aligned}$$

Proposition 33. Let $n \in \mathbb{N}$. Then:

$$\Phi_n(x) = \prod_{\substack{1 \leq k \leq n \\ \gcd(k,n)=1}} \left(x - \mathrm{e}^{2\pi \mathrm{i} \frac{k}{n}}\right)$$

Theorem 34. Let $n \in \mathbb{N}$. Then:

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x)$$

2. | Field extensions

Proposition 35. Let K, L be fields. Then, any field morphism $K \to L$ is injective.

Definition 36. Let K, L be two fields. A *field extension* L/K is a field morphism $K \hookrightarrow L$.

Proposition 37. Let L/K be a field extension. Then, L is a vector space over K. Reciprocally, if L is a vector space over K satisfying:

$$(\lambda \cdot 1) \cdot (\mu \cdot 1) = (\lambda \cdot \mu) \cdot 1 \qquad \forall \lambda, \mu \in K$$

then the morphism $f : K \to L$ defined as $f(\lambda) = \lambda \cdot 1$ is a field morphism and L/K is a field extension.

Definition 38. Let L/K be a field extension. We define the *degree* of the extension L/K as:

$$[L : K] := \dim_K(L)$$

We say that the extension L/K is *finite* if $[L : K]$ is finite. Otherwise, we say that L/K is *infinite*.

Lemma 39 (Kronecker's lemma). Let K be a field, $p(x) \in K[x]$ a monic and irreducible polynomial of degree $d \geq 1$ and $L = K[x]/(p(x))$. Then, L/K is a field extension of degree d, and the set $\{1, \overline{x}, \dots, \overline{x}^{d-1}\}$ is a basis of the vector space L over K. Furthermore, $\overline{x} \in L$ is a root of $p(x)$ in L.

Corollary 40. Let K be a field, $p(x) \in K[x]$ a monic and irreducible polynomial of degree $d \geq 1$. Then, there exists a field extension L/K such that $p(x)$ has a root in L.

Algebraic and transcendental numbers

Definition 41. Let L/K be a field extension and $\alpha \in L$. Consider the ring morphism:

$$\begin{aligned}
\varphi_\alpha : K[x] &\longrightarrow L \\
p(x) &\longmapsto p(\alpha)
\end{aligned}$$

1. We say that α is *algebraic* over K if $\ker \varphi_\alpha = (p(x))$, where $p(x) \in K[x]$ is an irreducible polynomial of degree $d \geq 1$. This polynomial is called *irreducible polynomial* of α over K and it is denoted by $\text{Irr}(\alpha, K)(x)$.

2. We say that α is *transcendental* over K if $\ker \varphi_\alpha = (0)$, or equivalently, if it is not algebraic.

Proposition 42. π and e are transcendental over $\mathbb{Q}$.

Proposition 43. Let L/K be a field extension and $\alpha \in L$ be a root of a monic and irreducible polynomial $p(x) \in K[x]$. Then, α is algebraic and $\text{Irr}(\alpha, K)(x) = p(x)$.

Theorem 44. Let $\overline{\mathbb{Q}} \subset \mathbb{C}$ be the set of algebraic numbers over $\mathbb{Q}$. Then, $\overline{\mathbb{Q}}$ is countable.

Simple extensions

Definition 45. A field extension L/K is called *simple* if $L = K(\alpha)$ for some $\alpha \in L$. In that case, the element α is called *primitive element* of L over K.

Theorem 46 (Steinitz's theorem). Let L/K be a finite field extension. Then, L/K is simple if and only if there is a finite number of intermediate fields between K and L.

Proposition 47. Let L/K be a field extension and $\alpha \in L$. Then:

- If α is algebraic over K, then:

$$K(\alpha) = K[\alpha] \cong {K[x]}\Big/{(\text{Irr}(\alpha, K)(x))}$$

- If α is transcendental over K, then:

$$K(\alpha) \cong K(x)$$

Corollary 48. Let L/K be a field extension and $\alpha \in L$. Then, $K(\alpha)/K$ is finite if and only if α is algebraic over K. Furthermore in that case:

$$[K(\alpha) : K] = \deg(\mathrm{Irr}(\alpha, K)(x))$$

Theorem 49 (Tower formula). Let F/L and L/K be field extensions. Then:

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

Proposition 50. Let L/K be a field extension and $\alpha \in L$ be algebraic. Then:

1. The following statements are equivalent:
   i) $\alpha \in K$
   ii) $\mathrm{Irr}(\alpha, K)(x) = x - \alpha$
   iii) $\deg(\mathrm{Irr}(\alpha, K)(x)) = 1$
2. If K'/K is another field extension, then:
   $$\mathrm{Irr}(\alpha, K')(x) \mid \mathrm{Irr}(\alpha, K)(x)$$
   and, moreover, $\mathrm{Irr}(\alpha, K')(x) = \mathrm{Irr}(\alpha, K)(x) \iff \deg(\mathrm{Irr}(\alpha, K')(x)) = \deg(\mathrm{Irr}(\alpha, K)(x))$.
3. $\deg(\mathrm{Irr}(\alpha, K)(x)) \mid [L : K]$

Definition 51. Let $n \in \mathbb{N}$ and $K_0, \dots, K_n$ be fields. A *tower of fields* is a sequence of field extensions K_j/K_{j-1} for $j = 1, \dots, n$. We will denote this tower of fields as:

$$K_n/K_{n-1}/\cdots/K_0$$

Corollary 52. Let $n \in \mathbb{N}$ and $K_n/K_{n-1}/\cdots/K_0$ be a tower of fields. Then:

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

Definition 53. A field extension L/K is called *finitely generated* if there exists $\alpha_1, \dots, \alpha_n \in L$ such that $L = K(\alpha_1, \dots, \alpha_n)$.

Definition 54. Let L/K, F/K be field extensions. We define the *compositum* of L and F, denoted as LF, as smallest field containing L and F.

Proposition 55. Let L/K, F/K be field extensions. Then,

$$[FL : K] \leq [F : K][L : K]$$

and the equality holds if the numbers $[F : K]$ are $[L : K]$ coprime.

Algebraic extensions

Definition 56. Let L/K be a field extension. We say that L/K is *algebraic* if $\forall \alpha \in L$, α is algebraic over K.

Definition 57. Let L/K be a field extension. We say that L/K is *purely transcendental* if $\forall \alpha \in L \setminus K$, α is transcendental over K.

Lemma 58. Let L/K be a finite field extension. Then, L/K is algebraic.

Proposition 59. Let L/K be a field extension. The following are equivalent:

1. L/K is finite.
2. L/K is algebraic and there exist $\alpha_1, \dots, \alpha_n \in L$ such that $L = K(\alpha_1, \dots, \alpha_n)$.
3. There exist $\alpha_1, \dots, \alpha_n \in L$ with α_i algebraic over $K(\alpha_1, \dots, \alpha_{i-1})$ for $i = 1, \dots, n$ such that $L = K(\alpha_1, \dots, \alpha_n)$.

Proposition 60. Let $L/F/K$ be a tower of fields such that F/K is algebraic, and $\alpha \in L$. Suppose that α is algebraic over F. Then, α is algebraic over K.

Proposition 61. Let $L/F/K$ be a tower of fields. Then:

1. If L/K is algebraic, any subring R such that $K \subseteq R \subseteq L$ is a subfield.
2. L/F and F/K are algebraic $\iff$ L/K is algebraic.
3. If $\alpha, \beta \in L$ are algebraic over K, then so are $\alpha + \beta$, $\alpha\beta$ and $\alpha\beta^{-1}$ (if $\beta \neq 0$).
4. The set
   $$E := \{\alpha \in L : \alpha \text{ is algebraic over } K\}$$
   is a subfield of L, the field extension E/K is algebraic and if $L \neq E$, then L/E is purely transcendental.

Morphisms of extensions

Definition 62. Let K, L, F be fields and $f : K \hookrightarrow L$ and $g : K \hookrightarrow F$ be field extensions. A *morphism of field extensions* between f and g (sometimes called *K-field morphism*) is a field morphism $h : L \to F$ such that $g = h \circ f$. We will denote the set of all such morphisms by:

$$\mathrm{Mor}_K(f, g) := \{h : L \longrightarrow F : h \circ f = g\}$$

If f and g are the natural inclusions, we will denote:

$$\mathrm{Mor}_K(L, F) := \mathrm{Mor}_K(f, g) = \{h : L \longrightarrow F : h|_K = \mathrm{id}_K\}$$

If f is the natural inclusion but g isn't, we will denote:

$$\mathrm{Mor}_K(L, g) := \mathrm{Mor}_K(f, g) = \{h : L \longrightarrow F : h|_K = g\}$$

Finally, if g is the natural inclusion but f isn't, we will denote:

$$\mathrm{Mor}_K(f, F) := \mathrm{Mor}_K(f, g) = \{h : L \longrightarrow F : h \circ f = \mathrm{id}_K\}$$

Definition 63. Let K, L, F be fields and $f : K \hookrightarrow L$ and $g : K \hookrightarrow F$ be field extensions. We define the following sets:

$$\mathrm{Iso}_K(f, g) := \{h \in \mathrm{Mor}_K(f, g) : h \text{ is bijective}\}$$
$$\mathrm{Aut}_K(f) := \mathrm{Iso}_K(f, f)$$

If f and g are the natural inclusions, we will denote[4]:

$$\mathrm{Iso}_K(L, F) := \{h \in \mathrm{Mor}_K(L, F) : h \text{ is bijective}\}$$
$$\mathrm{Aut}_K(L) := \mathrm{Iso}_K(L, L)$$

[4] And we define $\mathrm{Iso}_K(L, g)$ and $\mathrm{Iso}_K(f, F)$ analogously as we did before.

Lemma 64. Let L/K be a field extension. Then, $(\mathrm{Aut}_K(L), \circ)$ is a group and it is called *Galois group* of L/K. Hence, $\mathrm{Aut}_K(L)$ is also denoted as $\mathrm{Gal}(L/K)$[5].

Proposition 65. Let L/K be a finite field extension. Then, $\mathrm{Gal}(L/K) = \mathrm{Mor}_K(L, L)$.

Lemma 66. Let K, L, F be fields and $f : K \to L$, $g : K \to F$ be field morphisms. Let $h \in \mathrm{Mor}_K(f, g)$, $\alpha \in L$, and $p(x) \in K[x]$. Then:

$$h(f(p)(\alpha)) = g(p)(h(\alpha))$$[6]

If f and g are the natural inclusions, then:

$$h(p(\alpha)) = p(h(\alpha))$$

Lemma 67. Let L/K, $g : K \hookrightarrow F$ be field extensions and $\alpha \in L$ be algebraic over K. Then, we have the bijection

$$\mathrm{Mor}_K(K(\alpha), g) \overset{\psi}{\cong} \{\beta \in F : g(\mathrm{Irr}(\alpha, K))(\beta) = 0\}$$

given by $\psi(h) = h(\alpha)$. If g is the natural inclusion, then:

$$\mathrm{Mor}_K(K(\alpha), F) \overset{\psi}{\cong} \{\beta \in F : \mathrm{Irr}(\alpha, K)(\beta) = 0\}$$

given by $\psi(h) = h(\alpha)$.

Corollary 68. Let $K(\alpha)/K$ be a finite field extension. Then:

$$\mathrm{Gal}(K(\alpha)/K) \cong \{\beta \in K(\alpha) : \mathrm{Irr}(\alpha, K)(\beta) = 0\}$$

Therefore, $\mathrm{Gal}(K(\alpha)/K)$ is finite and:

$$|\mathrm{Gal}(K(\alpha)/K)| \leq [K(\alpha) : K]$$

Proposition 69. Let K, L, F be fields and $f : K \hookrightarrow L$ and $g : K \hookrightarrow F$ be field extensions. Then:

1. If $f' : K \to L'$, $\varphi : L' \to L$ are field extensions, then:

$$\mathrm{Mor}_K(f, g) = \bigsqcup_{h \in \mathrm{Mor}_K(f', g)} \mathrm{Mor}_{L'}(\varphi, h)$$

In particular, if f, g, f' and φ are the natural inclusions, then:

$$\mathrm{Mor}_K(L, F) = \bigsqcup_{h \in \mathrm{Mor}_K(L', F)} \mathrm{Mor}_{L'}(L, h)$$

2. If $\mathrm{Iso}_K(f, g) \neq \varnothing$, then $\mathrm{Iso}_K(f, g) \cong \mathrm{Gal}(f)$ by sending $h \mapsto h \circ h_0^{-1}$, where $h_0 \in \mathrm{Iso}_K(f, g)$ is a fixed isomorphism. Analogously, if $\mathrm{Iso}_K(L, F) \neq \varnothing$, then $\mathrm{Iso}_K(L, F) \cong \mathrm{Gal}(L/K)$.

3. | Finite fields

Definition 70 (Finite field). A *finite field* F is a finite set which is a field.

Proposition 71. Let F be a finite field. Then, $F = p^n$ where p is a prime number and $n \in \mathbb{N}$.

Theorem 72. Let p be a prime number and $n \in \mathbb{N}$. Then, there exists a unique field with p^n elements up to isomorphism which we will denote by $\mathbb{F}_{p^n}$[7].

Proposition 73. Let p be a prime number and $d, n \in \mathbb{N}$. Then:

$$\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n} \iff d \mid n$$

And in that case, $[\mathbb{F}_{p^n} : \mathbb{F}_{p^d}] = \frac{n}{d}$.

Theorem 74. Let p be a prime number and $d \in \mathbb{N}$. We define the set $P_{p,d}$ as:

$$P_{p,d} := \{f(x) \in \mathbb{F}_p[x] : \deg(f(x)) = d \wedge f(x) \text{ is monic and irreducible}\}$$

Then, for all $n \in \mathbb{N}$ we have:

$$x^{p^n} - x = \prod_{d|n} \prod_{f(x) \in P_{p,d}} f(x)$$

Corollary 75. Let p be a prime number and $d, n \in \mathbb{N}$. Then:

$$p^n = \sum_{d|n} d|P_{p,d}|$$

Corollary 76. For all prime numbers p and for all $n \in \mathbb{N}$, there exists a monic and irreducible polynomial of degree n in $\mathbb{F}_p[x]$.

Corollary 77. Let p be a prime number and $n \in \mathbb{N}$. Then, $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$ for some $\alpha \in \mathbb{F}_{p^n}$. Thus, the extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ is simple.

Definition 78. Let p be a prime number and R be a ring such that $\mathrm{char}\, R = p$. We define the *Frobenius endomorphism* as:

$$\begin{aligned} \mathrm{Frob}_R : R &\longrightarrow R \\ r &\longmapsto r^p \end{aligned}$$

Theorem 79. Let p be a prime number and $n \in \mathbb{N}$. Then, $\mathrm{Frob}_{\mathbb{F}_{p^n}} \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ and, furthermore:

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \mathrm{Frob}_{\mathbb{F}_{p^n}} \rangle \cong \mathbb{Z}/n\mathbb{Z}$$

Corollary 80. Let p be a prime number, $n \in \mathbb{N}$, $q = p^n$ and denote $\mathrm{Frob}_q := \left(\mathrm{Frob}_{\mathbb{F}_{p^n}}\right)^n$. Then, for all $r \in \mathbb{N}$:

$$\mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q) = \langle \mathrm{Frob}_q \rangle \cong \mathbb{Z}/r\mathbb{Z}$$

Definition 81 (Perfect fields). A field K is called *perfect* if either $\mathrm{char}\, K = 0$ or $\mathrm{char}\, K = p > 0$ and $\mathrm{Frob}_K \in \mathrm{Aut}(K)$.

[5] For the general case when $f : K \hookrightarrow L$ is a field extension, we define $\mathrm{Gal}(f) := \mathrm{Aut}_K(f)$.

[6] Here $f(p)$ denotes the evaluation through f of the polynomial $p(x)$. That is, assuming that $p(x)$ is of the form $p(x) = \sum_{i=1}^n a_i x^i$, then $f(p) : \sum_{i=1}^n a_i x^i \longmapsto \sum_{i=1}^n f(a_i) x^i$.

[7] Another commonly used notation to denote the field with p^n elements is $\mathrm{GF}(p^n)$.

4. | Algebraic field extensions

Splitting field

Definition 82. Let K, L be fields and $p(x) \in K[x]$ be a polynomial such that $\deg p(x) = n \geq 1$. We say that $p(x)$ *splits into linear factors* on L if $p(x) = a_n \prod_{i=1}^{n}(x - a_i)$, where $a_i \in L$ for $i = 1, \ldots, n$.

Theorem 83 (Kronecker's theorem). Let K be a field and $S \subset K[x]$ be a finite set. Then, there exists a finite field extension L/K such that all polynomials in S split into linear factors on L.

Theorem 84. Let K be a field and $L = K(\alpha_1, \ldots, \alpha_n)$. Let $f : K \hookrightarrow F$ be a field morphism such that $f(\mathrm{Irr}(\alpha_i, K))(x)$ splits into linear factors on F for all $i = 1, \ldots, n$. Then,

$$1 \leq |\operatorname{Mor}_K(L, f)| \leq [L : K]$$

and, furthermore, $|\operatorname{Mor}_K(L, f)| = [L : K]$ if and only if $f(\mathrm{Irr}(\alpha_i, K))(x)$ has no repeated roots on F for all $i = 1, \ldots, n$.

Definition 85 (Splitting field). Let L/K be a finite field extension and $p(x) \in K[x] \setminus K$ be such that it splits into linear factors in L. Let $\alpha_1, \ldots, \alpha_n$ be their roots. The *splitting field* of $p(x)$ over K is the smallest subfield $K(\alpha_1, \ldots, \alpha_n)$ of L where $p(x)$ splits into linear factors.

Proposition 86. Let K be a field and $p(x) \in K[x] \setminus K$. Then, L is a splitting field of $p(x)$ if and only if $p(x)$ splits into linear factors on L and for all tower of fields $L/F/K$ with $F \neq L$, $p(x)$ doesn't split into linear factors on F.

Theorem 87 (Existence of the splitting field). Let K be a field and $p(x) \in K[x] \setminus K$. Then, there exists a splitting field of $p(x)$ over K.

Theorem 88. Let K be a field, $p(x) \in K[x] \setminus K$ and L/K and F/K be two splitting fields of $p(x)$ over K. Then, $[L : K] = [F : K]$ and

$$1 \leq |\operatorname{Iso}_K(L, F)| \leq [L : K]$$

Furthermore, $|\operatorname{Iso}_K(L, F)| = [L : K]$ if and only if all irreducible factors of $p(x)$ have no repeated roots on F.

Corollary 89. Let K_1, K_2 be fields, $f : K_1 \to K_2$ be a field isomorphism, $p(x) \in K[x] \setminus K$ and L_1/K_1, L_2/K_2 be two field extensions. Suppose L_1 is the splitting of $p(x)$ over K_1 and L_2 be the splitting of $f(p)(x)$ over K_2. Then, there exists a field isomorphism $\varphi : L_1 \to L_2$ such that $\varphi|_{K_1} = f$.

Corollary 90 (Unicity of the splitting field). Let K be a field and $p(x) \in K[x] \setminus K$. Then, any two splitting fields of $p(x)$ over K are isomorphic.

Corollary 91. Let K be a field, $p(x) \in K[x] \setminus K$ and L be the splitting field of $p(x)$ over K. Then:

$$|\mathrm{Gal}(L/K)| \leq [L : K]$$

and $|\mathrm{Gal}(L/K)| = [L : K]$ if and only if $p(x)$ has no repeated roots on L.

Corollary 92. Let L/K be a field extension and $p(x) \in K[x]$. Then, the splitting field of $p(x)$ over L contains the splitting field of $p(x)$ over K.

Proposition 93. Let p be a prime number and $n \in \mathbb{N}$. Then, $\mathbb{F}_{p^n}$ is the splitting field of $x^{p^n} - x \in \mathbb{F}_p[x]$.

Normal extensions

Definition 94. An algebraic field extension L/K is *normal* if for all irreducible polynomial $p(x) \in K[x]$ we have that if $p(x)$ has a root in L, then $p(x)$ splits into linear factors in L.

Proposition 95. Let L/K be finite field extension of degree 2. Then, L/K is normal.

Theorem 96. Let L/K be finite field extension. L/K is normal if and only if L is the splitting field of some polynomial $p(x) \in K[x] \setminus K$.

Corollary 97. Let L/K be finite field extension. Then, there exists a field extension F/L such that:

1. F/K is finite and normal.
2. For all field extensions H/L with H/K normal there is at least one L-field morphism $f : F \to H$.

The extension F/L is called *normal closure* of L/K.

Corollary 98. Let $L/F/K$ be a tower of fields such that L/K is finite and normal. Then, L/F is also finite and normal.

Corollary 99. Let $L/F/K$ be a tower of fields such that L/K is finite and normal. Let $f \in \operatorname{Mor}_K(F, L)$. Then, there exists at least one automorphism $\varphi \in \mathrm{Gal}(L/K)$ such that $\varphi|_F = f$.

Corollary 100. Let L/K be a finite field extension. Then:

$$|\mathrm{Gal}(L/K)| \leq [L : K]$$

Hence, $\mathrm{Gal}(L/K)$ is a finite group.

Corollary 101. Let $L/F/K$ be a tower of fields such that L/K is finite and normal. Then, F/K is normal if and only if $\varphi(F) = F$ $\forall \varphi \in \mathrm{Gal}(L/K)$.

Separable polynomials

Definition 102 (Formal derivative). Let R be a ring and $p(x) = \sum_{n=0}^{d} a_n x^n \in R[x]$. We define *formal derivative* of $p(x)$ as:

$$p'(x) := \sum_{n=1}^{d} n a_n x^{n-1}$$

Proposition 103. Let R be a ring, $a \in R$ and $p(x), q(x) \in R[x]$. Then:

1. $(p(x) + q(x))' = p'(x) + q'(x)$
2. $(ap(x))' = ap'(x)$
3. $(p(x)q(x))' = p'(x)q(x) + p(x)q'(x)$

4.
$$\deg(p'(x)) \leq \deg(p(x)) - 1$$
And the inequality holds if either $\text{char}(R) = 0$ or $\gcd(\text{char}(R), \deg(p(x))) = 1$.

Proposition 104. Let K be a field, $p(x) \in K[x] \setminus K$, L be a splitting field of $p(x)$ over K and $d(x) := \gcd(p(x), p'(x))$. Then:
$$\{\alpha \in L : d(\alpha) = 0\} = \{\alpha \in L : (x-\alpha)^2 \mid p(x)\}$$

Definition 105. Let K be a field and $p(x) \in K[x]$. We say that $p(x)$ is *separable* if it doesn't have multiple roots in its splitting field.

Corollary 106. Let K be a field and $p(x) \in K[x] \setminus K$. Then:
$$p(x) \text{ is separable} \iff \gcd(p(x), p'(x)) = 1$$

Corollary 107. Let K be a field such that $\text{char}\, K = 0$ and $p(x) \in K[x]$ be an irreducible polynomial. Then, $p(x)$ is separable.

Lemma 108. Let K be a field such that $\text{char}\, K = p > 0$ and $p(x) \in K[x]$. Then:
$$p'(x) = 0 \iff \exists q(x) \in K[x] : p(x) = q(x^p)$$

Corollary 109. Let K be a field such that $\text{char}\, K = p > 0$, $p(x) \in K[x]$ and $q(x) := p(x^p)$. Then, all roots of $q(x)$ are multiple.

Corollary 110. Let K be a field such that $\text{char}\, K = p > 0$, $p(x) \in K[x]$ and $q(x) := p(x^p) + bx$, where $b \in K^*$. Then, all roots of $q(x)$ are simple.

Theorem 111. Let K be a perfect field. Then, any irreducible polynomial over K is separable.

Separable extensions

Definition 112 (Separable extension). Let L/K be an algebraic field extension and $\alpha \in L$. We say that α is *separable* over K if $\text{Irr}(\alpha, K)(x)$ is separable. We say that L/K is *separable* if and only if $\forall \alpha \in L$, α is separable over K.

Corollary 113. Let K be a perfect field. Then, any algebraic extension L/K is separable.

Theorem 114 (Separability theorem). Let $K(\alpha_1, \ldots, \alpha_n)/K$ be a finite field extension and $f : K \to L$ a field morphism such that $f(\text{Irr}(\alpha_i, K))(x)$ splits into linear factors $\forall i = 1, \ldots, n$. Then, the following statements are equivalent:

1. $K(\alpha_1, \ldots, \alpha_n)/K$ is separable.
2. $\alpha_1, \ldots, \alpha_n$ are separable over K.
3. $|\text{Mor}_K(K(\alpha_1, \ldots, \alpha_n), f)| = [K(\alpha_1, \ldots, \alpha_n) : K]$.

Corollary 115. Let K be a field and L be the splitting field of a separable polynomial $p(x) \in K[x]$. Then, L/K is separable.

Proposition 116. Let $L/F/K$ be a tower of fields. Then:

1. L/F and F/K are separable $\iff$ L/K is separable.
2. The set
$$E := \{\alpha \in L : \alpha \text{ is separable over } K\}$$
is a subfield of L, the field extension E/K is separable and if $L \neq E$, then $\forall \beta \in L \setminus E$, β is not separable over E. In that case, and if the extension L/E is algebraic, we say that L/E is *purely inseparable*.

Theorem 117 (Primitive element theorem). Let L/K be a finite and separable field extension. Then, L/K is simple.

Galois extensions

Definition 118. We say that a field extension L/K is a *Galois extension* (or is *Galois*) if it is normal and separable.

Theorem 119. Let L/K be a finite field extension. Then:
$$L/K \text{ is Galois} \iff |\text{Gal}(L/K)| = [L : K]$$

Lemma 120. Let $L/F/K$ be a tower of fields such that L/K is Galois. Then, L/F is Galois.

Proposition 121. Let L/K be a Galois extension. Then, $\alpha \in L$ is primitive if and only if $\forall \sigma \in \text{Gal}(L/K) \setminus \{\text{id}\}$, $\sigma(\alpha) \neq \alpha$.

5. | Fundamental theorem of Galois theory

Definition 122. Let L/K be a finite field extension and G be a group. We define the following sets:
$$\mathcal{K}(L/K) := \{F \subseteq L : L/F/K \text{ is a tower of fields}\}$$
$$\mathcal{S}(G) := \{H \subseteq G : H \text{ is a subgroup of } G\}$$

Lemma 123. Let $H \in \mathcal{S}(\text{Gal}(L/K))$ and
$$L^H := \{a \in L : \sigma(a) = a \ \forall \sigma \in H\}$$
Then, L^H is a field (called *fixed field* of H) and $L^H \in \mathcal{K}(L/K)$.

Lemma 124. Let L/K be a finite field extension and $F \in \mathcal{K}(L/K)$. Then, $\text{Gal}(L/F)$ is a subgroup of $\text{Gal}(L/K)$.

Definition 125. Let L/K be a finite field extension. We define the following functions:
$$\begin{array}{rccc} \mathcal{F} : \mathcal{S}(\text{Gal}(L/K)) & \longrightarrow & \mathcal{K}(L/K) \\ H & \longmapsto & L^H \end{array}$$
$$\begin{array}{rccc} \mathcal{G} : \mathcal{K}(L/K) & \longrightarrow & \mathcal{S}(\text{Gal}(L/K)) \\ F & \longmapsto & \text{Gal}(L/F) \end{array}$$

Proposition 126. Let L/K be a finite field extension. Then:

1. $\mathcal{F}(\{\text{id}\}) = L$.
2. $\mathcal{G}(L) = \{\text{id}\}$ and $\mathcal{G}(K) = \text{Gal}(L/K)$.

3. If $H_1, H_2 \in \mathcal{S}(\mathrm{Gal}(L/K))$ are such that $H_1 \subseteq H_2$, then $\mathcal{F}(H_1) \supseteq \mathcal{F}(H_2)$.
4. If $F_1, F_2 \in \mathcal{K}(L/K)$ are such that $F_1 \subseteq F_2$, then $\mathcal{G}(F_1) \supseteq \mathcal{G}(F_2)$.
5. $H \subseteq \mathcal{G}(\mathcal{F}(H))\ \forall H \in \mathcal{S}(\mathrm{Gal}(L/K))$.
6. $F \subseteq \mathcal{F}(\mathcal{G}(F))\ \forall F \in \mathcal{K}(L/K)$.
7. $\mathcal{F} \circ \mathcal{G} \circ \mathcal{F} = \mathcal{F}$.
8. $\mathcal{G} \circ \mathcal{F} \circ \mathcal{G} = \mathcal{G}$.

Lemma 127 (Artin's lemma). Let L/K be a finite field extension and H be a subgroup of $\mathrm{Gal}(L/K)$. Then, $H = \mathrm{Gal}(L/L^H)$ and $|H| = [L : L^H]$.

Corollary 128. Let L/K be a finite field extension. Then, $\mathcal{G} \circ \mathcal{F} = \mathrm{id}$. Thus, $\mathcal{F}$ is injective and $\mathcal{G}$ is surjective.

Theorem 129 (Fundamental theorem of Galois theory). Let L/K be a finite and Galois field extension. Then, $\mathcal{F} \circ \mathcal{G} = \mathrm{id}$. Thus, $\mathcal{F}$ and $\mathcal{G}$ are bijective and they are inverses of each other. Furthermore, if $F \in \mathcal{K}(L/K)$, then:

$$F/K \text{ is normal} \iff \mathrm{Gal}(L/F) \trianglelefteq \mathrm{Gal}(L/K)$$

And in that case:

$$\mathrm{Gal}(L/K)\Big/\mathrm{Gal}(L/F) \cong \mathrm{Gal}(F/K)$$

Corollary 130. Let L/K be a finite and Galois field extension and H be a subgroup of $\mathrm{Gal}(L/K)$. Then:

$$[L^H : K] = \frac{|\mathrm{Gal}(L/K)|}{|H|}$$

Definition 131. Let G be a group. The *lattice of subgroups* of G is the following graph:

- The vertices of the graph are the subgroups of G.
- Two vertices (corresponding to two subgroups H_i, H_j of G) are connected by an edge if $H_i \leq H_j$, with $i \neq j$, and such that there is no $k \neq i, j$ such that $H_i \leq H_k \leq H_j$.

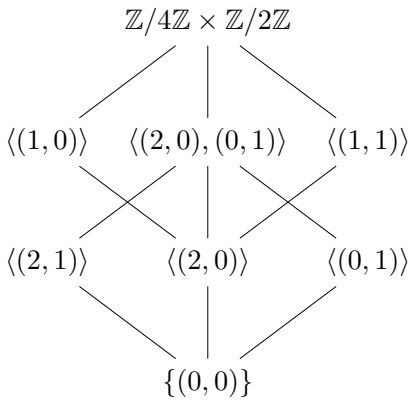

Figure 1: Lattice of subgroups of the group $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Definition 132. Let K be a field, $p(x) \in K[x]$ and L be the splitting field of $p(x)$ over K. We denote $\mathrm{Gal}(p(x)/K) := \mathrm{Gal}(L/K)$.

Definition 133. A subgroup H of S_n is called *transitive* if $\forall i, j \in \{1, \ldots, n\}$, $\exists \sigma \in H$ such that $\sigma(i) = j$.

Lemma 134. The transitive subgroups of S_4, up to isomorphism, are S_4, A_4, D_4, V_4 and C_4, where:

$$\mathrm{V}_4 = \langle (1,2)(3,4), (1,3)(2,4) \rangle \quad \text{and} \quad \mathrm{C}_4 = \langle (1,2,3,4) \rangle$$

Corollary 135. The transitive subgroups of A_4, up to isomorphism, are A_4 and V_4.

Lemma 136. Let K be a field, $p(x) \in K[x]$ be an irreducible and separable polynomial of degree n and L be its splitting field. Let $\alpha_1, \ldots, \alpha_n \in L$ be the roots of $p(x)$. Then, there exists a unique monomorphism $\iota : \mathrm{Gal}(p(x)/K) \hookrightarrow \mathrm{S}_n$ such that $\sigma(\alpha_i) = \alpha_{\iota(\sigma)(i)}$.

Lemma 137. Let K be a field, $p(x) \in K[x]$ be an irreducible and separable polynomial of degree n and $\iota : \mathrm{Gal}(p(x)/K) \hookrightarrow \mathrm{S}_n$ be the monomorphism obtained by fixing an order of the roots of $p(x)$ (in its splitting field). Then, $\mathrm{im}(\iota)$ is a transitive subgroup of S_n.

Definition 138. Let K be a field, $p(x) \in K[x]$ and $\alpha_1, \ldots, \alpha_n$ be the roots of $p(x)$ in its splitting field. We define $\delta(p)$ as:

$$\delta(p) := \prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i)$$

We define the *discriminant* of $p(x)$, $\mathrm{Disc}(p)$, as:

$$\mathrm{Disc}(p) := \prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i)^2 = \delta(p)^2$$

Proposition 139. Let K be a field, $p(x) \in K[x]$ and $\alpha_1, \ldots, \alpha_n$ be the roots of $p(x)$ in its splitting field. Then, $\mathrm{Disc}(p) \in K[\alpha_1, \ldots, \alpha_n]^{\mathrm{S}_n}$.

Lemma 140. Let K be a field, $p(x) \in K[x]$ be an irreducible and separable polynomial of degree n, L be its splitting field and $\alpha_1, \ldots, \alpha_n \in L$ be the roots of $p(x)$. Then, if we think $\mathrm{Gal}(L/K)$ as a subgroup of S_n via the inclusion ι of above, we have that $\forall \sigma \in \mathrm{S}_n$, $\sigma(\delta(p)) = \mathrm{sgn}(\sigma)\delta(p)$.

Corollary 141. Let K be a field, $p(x) \in K[x]$ be an irreducible and separable polynomial of degree n, L be its splitting field and $\alpha_1, \ldots, \alpha_n \in L$ be the roots of $p(x)$. Then, $\mathrm{Disc}(p) \in K$.

Corollary 142. Let K be a field, $p(x) \in K[x]$ be an irreducible and separable polynomial of degree n, L be its splitting field and $\alpha_1, \ldots, \alpha_n \in L$ be the roots of $p(x)$. Then:

$$\delta(p) \in K \iff \mathrm{Gal}(L/K) \subseteq \mathrm{A}_n$$

Proposition 143. Let $f(x) = x^2 + bx + c$ and $g(x) = x^3 + px + q$. Then:

- $\mathrm{Disc}(f) = b^2 - 4c$
- $\mathrm{Disc}(g) = -4p^3 - 27q^2$

6. | Fundamental theorem of algebra

Definition 144. We say that a field K is *algebraically closed* if each polynomial in $K[x]$ splits into linear factors in K.

Proposition 145. Let K be a field. The following statements are equivalent:

1. K is algebraically closed.
2. If $p(x) \in K[x]$ is irreducible, then $\deg(p(x)) = 1$.
3. K/K is the only algebraic extension of K.
4. If L/K is a finite field extension, then $[L : K] = 1$.

Lemma 146. Let G be a 2-group. Then, G has a normal subgroup of index 2.

Theorem 147. Let $L/\mathbb{R}$ be a finite Galois field extension. Then, either $L = \mathbb{R}$ or $L = \mathbb{C}$.

Theorem 148 (Fundamental theorem of algebra). $\mathbb{C}$ is algebraically closed.

Theorem 149. Let K be a field. Then, there exists an algebraic field extension $\overline{K}/K$ such that $\overline{K}$ is algebraically closed. This field $\overline{K}$ is called the *algebraic closure* of K.

7. | Galois theory of solvable equations

Solvable groups

Definition 150. Let G be a finite group. We say G is *solvable* if there is a chain of subgroups H_i of G satisfying:

$$\{e\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = G$$

and such that H_i/H_{i-1} are abelian for all $i = 1, \ldots, n$.

Definition 151. Let G be a group. We say that G is *simple* if its only normal subgroups are the trivial group and the group itself.

Proposition 152. Let G be a solvable group and H be a subgroup of G. Then, H is solvable.

Proposition 153. Let G be a finite group and H be a subgroup of G such that $H \trianglelefteq G$. Then, G is solvable if and only if H and G/H are solvable.

Proposition 154. Let G be a solvable group. Then, there exists a chain of subgroups

$$\{e\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = G$$

such that H_i/H_{i-1} are cyclic for all $i = 1, \ldots, n$.

Theorem 155. A_n is simple for all $n \geq 5$.

Theorem 156. S_n and A_n aren't solvable for all $n \geq 5$.

Radical, cyclotomic and cyclic extensions

Definition 157. We say that a finite field extension L/K is *radical* if there exist $n \in \mathbb{N}$ and $\alpha \in L$ such that $L = K(\alpha)$ and $\alpha^n \in K$. Moreover, if $\alpha^n = 1$ we say the the extension L/K is *cyclotomic*.

Definition 158. We say that a tower of fields $K_n/K_{n-1}/\cdots/K_0$ is a *radical tower* if K_i/K_{i-1} is a radical extension $\forall i = 1, \ldots, n$.

Definition 159. We say that a field extension L/K is *solvable by radicals* if there exists a radical tower of fields $K_n/K_{n-1}/\cdots/K_1/K$ such that $L \subseteq K_n$.

Definition 160. Let K be a field and $p(x) \in K[x]$. We say that $p(x)$ is *solvable by radicals* if the splitting field of $p(x)$ over K is solvable by radicals.

Definition 161. Let $n \in \mathbb{N}$ and K be a field. A *n-th root of unity* is a number $z \in K$ such that $z^n = 1$. A *n-th primitive root of unity* is a n-th root of unity $z \in K$ such that $z^m \neq 1$ for all $m = 1, \ldots, n-1$.

Proposition 162. Let K be a field such that $\operatorname{char} K = 0$, $n \geq 2$ and L be the splitting field of $x^n - 1$ over K. Denote by ξ_n a n-th primitive root of unity. Then, $L = K(\xi_n)$ and $\mathrm{Gal}(L/K) \cong H$ for some $H \in \mathcal{S}\left((\mathbb{Z}/n\mathbb{Z})^*\right)$. Furthermore if $K = \mathbb{Q}$, we have that $\mathrm{Gal}(L/K) \cong (\mathbb{Z}/n\mathbb{Z})^*$.

Proposition 163. Let K be a field such that $\operatorname{char} K = 0$ and $x^n - 1$ splits into linear factors in K. Let $K(\alpha)/K$ be a radical extension. Then, $K(\alpha)/K$ is Galois and $\mathrm{Gal}(K(\alpha)/K) \cong \mathbb{Z}/d\mathbb{Z}$, for some d such that $d \mid n$. Furthermore, $\alpha^d \in K$ and $\mathrm{Irr}(\alpha, K) = x^d - \alpha^d$.

Definition 164. We say that a Galois extension L/K is *abelian* if $\mathrm{Gal}(L/K)$ is abelian. In particular, we say that L/K is *cyclic* if $\mathrm{Gal}(L/K)$ is cyclic.

Lemma 165 (Dedekind's lemma). Let L and F be fields and $f_1, \ldots, f_n : L \to F$ be distinct field morphisms. Then, if $\lambda_1, \ldots, \lambda_n \in F$ are such that $\lambda_1 f_1 + \cdots + \lambda_n f_n = 0$, then $\lambda_1 = \cdots = \lambda_n = 0$. In that case, we say that $f_1, \ldots, f_n$ are *F-linearly independent*.

Theorem 166. Let K be a field such that $\operatorname{char} K = 0$ and $x^n - 1$ splits into linear factors in K. Then, L/K is cyclic of degree n if and only if L/K is radical of degree n.

Lemma 167. Let F/K be a field extension, $p(x) \in K[x]$ be a separable polynomial, L/K be a splitting field of $p(x)$ over K and E/F be a splitting field of $p(x)$ over F. Then, $\mathrm{Gal}(E/F) \cong H$ for some $H \in \mathcal{S}(\mathrm{Gal}(L/K))$

Theorem 168. Let K be a field such that $\operatorname{char} K = 0$, and $p(x) \in K[x]$. Then:

$$p(x) \text{ is solvable by radicals} \iff \mathrm{Gal}(p(x)/K) \text{ is solvable}$$

Lemma 169. Let K be a field, $n \in \mathbb{N}$, $a_1, \ldots, a_n$ be unknowns and $s_1, \ldots, s_n$ be the elementary symmetric polynomials in the variables $a_1, \ldots, a_n$. Then:

$$\mathrm{Gal}(K(a_1, \ldots, a_n)/K(s_1, \ldots, s_n)) \cong \mathrm{S}_n$$

Corollary 170. Let K be a field, $a_1, \ldots, a_n$ be unknowns, $\delta := \prod_{1 \leq i < j \leq n}(a_j - a_i)$ and $s_1, \ldots, s_n$ be the elementary symmetric polynomials in the variables $a_1, \ldots, a_n$.. Then:

$$K(a_1, \ldots, a_n)^{\mathrm{A}_n} = K(s_1, \ldots, s_n)(\delta)$$

Theorem 171 (Abel-Ruffini theorem). There is no solution in radicals to polynomial equations of degree five or higher with arbitrary coefficients.

Proposition 172. Let K be a field such that $\operatorname{char} K = 0$, and $p(x) \in K[x]$ be an irreducible polynomial of degree 5. Then:

$$p(x) \text{ is solvable by radicals} \iff \mathrm{Gal}(p(x)/K) \ncong \mathrm{S}_5, \mathrm{A}_5$$

Theorem 173 (Nart-Vila theorem). For all $n \geq 2$, $\mathrm{Gal}(x^n - x - 1/\mathbb{Q}) \cong \mathrm{S}_n$.

Corollary 174. Let G be a finite group. Then, there exists finite field extensions $K/\mathbb{Q}$ and L/K such that $\mathrm{Gal}(L/K) \cong G$.

Biquadratic polynomials

Theorem 175. Let K be a field such that $\operatorname{char} K = 2$, $p(x) = x^4 + ax^2 + b \in K[x]$ be an irreducible polynomial over K and $d := a^2 - 4b \in K$. Then:

- If $\sqrt{b} \in K \implies \mathrm{Gal}(p(x)/K) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
- If $\sqrt{b} \in \sqrt{d}K \implies \mathrm{Gal}(p(x)/K) \cong \mathbb{Z}/4\mathbb{Z}$
- If $\sqrt{b} \notin K \cup \sqrt{d}K \implies \mathrm{Gal}(p(x)/K) \cong \mathrm{D}_4$