1. Introduction

1.1. Cubic equations over $\mathbb{C}$

- For a polynomial equation, a **solution by radicals** is a formula for solutions using only addition, subtraction, multiplication, division and radicals $\sqrt[m]{\cdot}$ for $m \in \mathbb{N}$.
- For general cubic equation $x^3 + a_2 x^2 + a_1 x + a_0 = 0$:
  - **Tschirnhaus transformation** is substitution $t = x + \frac{a_2}{3}$, giving

    $$t^3 + pt + q = 0, \quad p = \frac{-a_2^2 + 3a_1}{3}, \quad q = \frac{2a_2^3 - 9a_1 a_2 + 27a_0}{27}$$

    This is a **reduced** cubic equation.
  - When $t = u + v$, $t^3 - (3uv)t - (u^3 + v^3) = 0$ which is in the reduced cubic form with $p = -3uv, q = -(u^3 + v^3)$.
  - We have

    $$(y - u^3)(y - v^3) = y^2 - (u^3 + v^3)y + u^3 v^3 = y^2 + qy - \frac{p^3}{27} = 0$$

    so $u^3, v^3 = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$.
  - So a solution to $t^3 + pt + q = 0$ is

    $$t = u + v = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

    The other solutions are $\omega u + \omega^2 v$ and $\omega^2 u + \omega v$ where $\omega = e^{2\pi i/3}$ is the 3rd root of unity. This is because u and v each have three solutions indepedently to $u^3, v^3 = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$, but also $uv = -\frac{p}{3}$.
- **Remark**: the above method doesn't work for fields of characteristic 2 or 3 since the formulas involve division by 2 or 3 (which is dividing by zero in these respective fields).
- For general cubic equation $x^3 + a_3 x^3 + a_2 x^2 + a_1 x + a_0 = 0$:
  - Substitution $t = x + \frac{a_3}{4}$ gives **reduced** quartic equation

    $$t^4 + pt^2 + qt + r = 0$$

  - We then manipulate the polynomial so that it is the sum or difference of two squares and use $a^2 + b^2 = (a + ib)(a - ib)$ or $a^2 - b^2 = (a + b)(a - b)$:

    $$\left(t^2 + w\right)^2 + (p - 2w)t^2 + qt + \left(r - w^2\right) = 0$$

  - $(p - 2w)t^2 + qt + \left(r - w^2\right) = 0$ is a square iff its discriminant is zero:

    $$q^2 - 4(p - 2w)\left(r - w^2\right) = 0 \Longleftrightarrow w^3 - \frac{1}{2}pw^2 - rw + \frac{1}{8}\left(4pr - q^2\right) = 0$$

  - This **cubic resolvent** is solvable by radicals. Taking any of the solutions and substituting for w gives a sum or difference of two squares in t. The quadratic factors can then be solved.

1.2. Galois theory for quadratic equations

2. Fields and polynomials

2.1. Basic properties of fields

- **Definition**: ring R is **field** if every element of $R - \{0\}$ has mutliplicative inverse and $1 \neq 0 \in R$.
- **Lemma**: every field is integral domain.
- **Definition**: field homomorphism is a ring homomorphism $\varphi : K \to L$ between fields:
  - $\varphi(a + b) = \varphi(a) + \varphi(b)$
  - $\varphi(ab) = \varphi(a)\varphi(b)$
  - $\varphi(1) = 1$

These imply $\varphi(0) = 0$, $\varphi(-a) = -\varphi(a)$, $\varphi(a^{-1}) = \varphi(a)^{-1}$.

- **Lemma**: let $\varphi : K \to L$ homomorphism.
  - $\text{im}(\varphi) = \{\varphi(a) : a \in K\}$ is a field.
  - $\ker(\varphi) = \{a \in K : \varphi(a) = 0\} = \{0\}$, i.e. φ is injective.
- **Definition**: **subfield** K of field L is subring of L where K is a field. L is a **field extension** of K.
- The above lemma shows the image of $\varphi : K \to L$ is a subfield of L.
- **Lemma**: intersections of subfields are subfields.
- **Prime subfield** of L: intersection of all subfields of field L.
- **Definition**: **characteristic** $\text{char}(K)$ of field K is

  $$\text{char}(K) \coloneqq \min\{n \in \mathbb{N} : \chi(n) = 0\}$$

  (or 0 if this does not exist) where $\chi : \mathbb{Z} \to K$, $\chi(m) = 1 + \cdots + 1$ (m times).
- **Example**: $\text{char}(\mathbb{Q}) = \text{char}(\mathbb{R}) = \text{char}(\mathbb{C}) = 0$, $\text{char}(\mathbb{F}_p) = p$ for p prime.
- **Lemma**: for any field K, $\text{char}(K)$ is either 0 or a prime.
- **Theorem**:
  - $\text{char}(K) = 0$ iff $\mathbb{Q}$ is the prime subfield of K.
  - $\text{char}(K) = p > 0$ iff $\mathbb{F}_p$ is the prime subfield of K.
- Note $p \mid \binom{p}{i}$ so $(a + b)^p = a^p + b^p$.

2.2. Polynomials over fields

- **Degree** of $f(x) = a_0 + a_1 x + \cdots + a_n x_n$, $a_n \neq 0$ is $\deg(f(x)) = n$.
- $\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$ and $\deg(f(x) + g(x)) = \max\{\deg(f(x)), \deg(g(x))\}$ with equality if $\deg(f(x)) \neq \deg(g(x))$.
- Degree of zero polynomial is $\deg(0) = -\infty$.
- Only invertible elements in $K[x]$ are non-zero constants $f(x) = a_0 \neq 0$.
- Similarities between $\mathbb{Z}$ and $K[x]$ for field K:
  - $K[x]$ is integral domain.
  - There is a division algorithm for $K[x]$: for $f(x), g(x) \in K[x]$, $\exists! q(x), r(x) \in K[x]$ with $\deg(r(x)) < \deg(g(x))$ such that

$$f(x)=q(x)g(x)+r(x)$$

- Every $f(x), g(x) \in K[x]$ have greatest common divisor $\gcd(f(x), g(x))$ unique up to multiplication by non-zero constants. By Euclidean algorithm for polynomials,

$$\exists a(x), b(x) \in K[x] : a(x)f(x)+b(x)g(x)=\gcd(f(x), g(x))$$

- Can construct field from $K[x]$: **field of fractions** of $K[x]$ is

$$K(x)=\operatorname{Frac}(K[x])=\left\{\frac{f(x)}{g(x)} : f(x), g(x) \in K[x], g(x) \neq 0\right\}$$

  (We can construct the field of fractions for any integral domain).
- $K[x]$ is PID and UFD.

- **Definition**: $f(x) \in K[x]$ **irreducible** in $K[x]$ if
  - $\deg(f(x)) \geq 1$ and
  - $f(x)=g(x)h(x) \Longrightarrow g(x)$ or $h(x)$ is constant

2.3. Tests for irreducibility

- If $f(x)$ has linear factor in $K[x]$, it has root in $K[x]$.
- **Rational root test**: if $f(x)=a_0+\cdots+a_n x^n \in \mathbb{Z}[x]$ has rational root $\frac{b}{c} \in \mathbb{Q}$ with $\gcd(b, c)=1$ then $b \mid a_0$ and $c \mid a_n$. This doesn't show f is irreducible for $\deg(f(x)) \geq 4$.
- **Gauss's lemma**: let $f(x) \in \mathbb{Z}[x]$, $f(x)=g(x)h(x)$, $g(x), h(x) \in \mathbb{Q}[x]$. Then $\exists r \in \mathbb{Q} : rg(x), r^{-1}h(x) \in \mathbb{Z}[x]$.
- **Example**: let $f(x)=x^4-3x^3+1 \in \mathbb{Q}[x]$. Using the rational root test, $f(\pm 1) \neq 0$ so no linear factors in $\mathbb{Q}[x]$. Checking quadratic factors, let

$$f(x)=(ax^2+bx+c)(rx^2+sx+t), \quad a, b, c, r, s, t \in \mathbb{Z} \text{ by Gauss's lemma}$$

  So $1=ar \Rightarrow a=r=\pm 1$. $1=ct \Rightarrow c=t=\pm 1$. $-3=b+s$ and $0=c(b+s)$: contradiction. So $f(x)$ irreducible in $\mathbb{Q}[x]$.
- **Example**: let $f(x)=x^4-3x^2+1 \in \mathbb{Q}[x]$. The rational root test shows there are no linear factors. Checking quadratic factors, let

$$f(x)=(ax^2+bx+c)(rx^2+sx+t), \quad a, b, c, r, s, t \in \mathbb{Z} \text{ by Gauss's lemma}$$

  As before, $a=r=\pm 1$, $c=t=\pm 1$. $0=b+s \Rightarrow b=-s$, $-3=at+bs+cr=-b^2 \pm 2$. $b=1$ works. So $f(x)=(x^2-x-1)(x^2+x-1)$.
- **Proposition**: let $f(x)=a_0+\cdots+a_n x^n \in \mathbb{Z}[x]$. If exists prime $p \nmid a_n$ such that $\overline{f}(x)$ is irreducible in $\mathbb{F}_p[x]$, then $f(x)$ irreducible in $\mathbb{Q}[x]$.
- **Example**: let $f(x)=8x^3+14x-9$. Reducing $\bmod 7$, $\overline{f}(x)=x^3-2 \in \mathbb{F}_7[x]$. No roots exist for this, so $f(x)$ irreducible in $\mathbb{Q}[x]$. For polynomials, no p is suitable, e.g. $f(x)=x^4+1$.
- Gauss's lemma works with any UFD R instead of $\mathbb{Z}$ and field of fractions $\operatorname{Frac}(R)$ instead of $\mathbb{Q}$: let F field, $R=F[t]$, $K=F(t)$, then $f(x) \in R[x]$ irreducible in $K[x]$ iff $f(x)$ has no proper factors in $R[x]$.

- **Eisenstein's criterion**: let $f(x) = a_0 + \cdots + a_n x^n \in \mathbb{Z}[x]$, prime $p \in \mathbb{Z}$ such that $p \mid a_0, ..., p \mid a_{n-1}$, $p \nmid a_n$, $p^2 \nmid a_0$. Then $f(x)$ irreducible in $\mathbb{Q}[x]$.
- Eisenstein's criterion generalises to UFD R instead of $\mathbb{Z}$, $\operatorname{Frac}(R)$ instead of $\mathbb{Q}$.
- **Example**: let $f(x) = x^3 - 3x + 1$. Consider $f(x-1) = x^3 - 3x^2 + 3$. Then by Eisenstein's criterion with $p = 3$, $f(x-1)$ irreducible in $\mathbb{Q}[x]$ so $f(x)$ is as well, since factoring $f(x-1)$ is equivalent to factoring $f(x)$.
- **Example**: ***p*-th cyclotomic polynomial** is

  $$f(x) = \frac{x^p - 1}{x - 1} = 1 + \cdots + x^{p-1}$$

  Now

  $$f(x+1) = \frac{(1+x)^p - 1}{1 + x - 1} = x^{p-1} + px^{p-2} + \cdots + \binom{p}{p-2} x + p$$

  so can apply Eisenstein with p.
-

3. Field extensions

3.1. Definitions and examples

- **Definition**: **field extension** L/K is field L containing subfield K. Can specify homomorphism $\iota : K \to L$ (which is injective)
- **Example**:
  - $\mathbb{C}/\mathbb{R}$, $\mathbb{C}/\mathbb{Q}$, $\mathbb{R}/\mathbb{Q}$.
  - $L = \mathbb{Q}\left(\sqrt{2}\right) = \left\{a + b\sqrt{2} : a, b \in \mathbb{Q}\right\}$ is field extension of $\mathbb{Q}$. $\mathbb{Q}(\theta)$ is field extension of $\mathbb{Q}$ where θ is root of $f(x) \in Q[x]$.
  - $L = \mathbb{Q}(\sqrt[3]{2}) = \left\{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Q}\right\}$ is smallest subfield of $\mathbb{R}$ containing $\mathbb{Q}$ and $\sqrt[3]{2}$.
  - $L = K(t)$ is field extension of K.
- **Definition**: let L/K field extension, $S \subseteq L$. Then ***K* with *S* adjoined**, $K(S)$, is minimal subfield of L containing K and S. If $|S| = 1$, L/K is a **simple extension**.
- **Example**: $\mathbb{Q}\left(\sqrt{2}, \sqrt{7}\right) = \{a + b\sqrt{2} + c\sqrt{7} + d\sqrt{14} : a, b, c, d, \in \mathbb{Q}\}$ is $\mathbb{Q}$ with $S = \{\sqrt{2}, \sqrt{7}\}$.
- **Example**: $\mathbb{R}/\mathbb{Q}$ is not simple extension.
- **Definition**: a **tower** if a chain of field extensions, e.g. $K \subset M \subset L$.

3.2. Algebraic elements and minimal polynomials

- **Definition**: let L/K field extension, $\theta \in L$. Then θ is **algebraic over *K*** if

  $$\exists 0 \neq f(x) \in K[x] : f(\theta) = 0$$

  Otherwise, θ is **transcendental over *K***.
- **Example**: for $n \geq 1$, $\theta = e^{2\pi i/n}$ is algebraic over $\mathbb{Q}$ (root of $x^n - 1$).
- **Example**: $t \in K(t)$ is transcendental over K.

- **Lemma**: the algebraic elements in $K(t)/K$ are precisely K.
- **Lemma**: let L/K field extension, $\theta \in L$. Define $I_K(\theta) := \{f(x) \in K[x] : f(\theta) = 0\}$. Then $I_K(\theta)$ is ideal in $K[x]$ and
  - If θ transcendental over K, $I_K(\theta) = \{0\}$
  - If θ algebraic over K, then exists unique monic irreducible polynomial $m(x) \in K[x]$ such that $I_K(\theta) = \langle m(x) \rangle$.
- **Definition**: for $\theta \in L$ algebraic over K, **minimal polynomial** of θ over K is the unique monic polynomial $m(x) \in K[x]$ such that $I_K(\theta) = \langle m(x) \rangle$. The **degree** of θ over K is $\deg(m(x))$.
- **Remark**: if $f(x) \in K[x]$ irreducible over K, monic and $f(\theta) = 0$ then $f(x) = m(x)$.
- **Example**:
  - Any $\theta \in K$ has minimal polynomial $x - \theta$ over K.
  - $i \in \mathbb{C}$ has minimal polynomial $x^2 + 1$ over $\mathbb{R}$.
  - $\sqrt{2}$ has minimal polynomial $x^2 - 2$ over $\mathbb{Q}$. $\sqrt[3]{2}$ has minimal polynomial $x^3 - 2$ over $\mathbb{Q}$.

3.3. Constructing field extensions

- **Lemma**: let K field, $f(x) \in K[x]$ non-zero. Then

$$f(x) \text{ irreducible over } K \iff K[x]/\langle f(x) \rangle \text{ is a field}$$

- **Theorem**: let $m(x) \in K[x]$ irreducible, monic, $K_m := K[x]/\langle m(x) \rangle$. Then
  - K_m/K is field extension.
  - Let $\theta = \pi(x)$ where $\pi : K[x] \to K_m$ is canonical projection, then θ has minimal polynomial $m(x)$ and $K_m = K(\theta)$.
- **Definition**: let L_1/K, L_2/K field extensions, $\varphi : L_1 \to L_2$ field homomorphism. φ is ***K*-homomorphism** if $\forall a \in K, \varphi(a) = a$ (φ fixes elements of K).
  - If φ is isomorphism then it is ***K*-isomorphism**.
  - If $L_1 = L_2$ and φ is bijective then φ is ***K*-automorphism**.
- **Example**:
  - Complex conjugation $\mathbb{C} \to \mathbb{C}$ is $\mathbb{R}$-automorphism.
  - Let K field, $\text{char}(K) \neq 2$, $\sqrt{2} \notin K$, so $x^2 - 2$ is minimal polynomial of $\sqrt{2}$ over K, then $K\left(\sqrt{2}\right) \cong K[x]/\langle x^2 - 2 \rangle$ is field extension of K and $a + b\sqrt{2} \to a - b\sqrt{2}$ is K-automorphism.
- **Proposition**: let L/K field extension, $\tau \in L$ with $m(\tau) = 0$ and $K_L(\tau)$ be minimal subfield of L containing K and τ. Then exists unique K-isomorphism $\varphi : K_m \to K_L(\tau)$ such that $\varphi(\theta) = \tau$.
- **Proposition**: let θ transcendental over K, then exists unique K-isomorphism $\varphi : K(t) \to K(\theta)$ such that $\varphi(t) = \theta$:

$$\varphi\left(\frac{f(g)}{g(t)}\right) = \varphi\left(\frac{f(\theta)}{g(\theta)}\right)$$

3.4. Explicit examples of simple extensions

- Let $r \in K^\times$ non-square in K, then $x^2 - r$ irreducible in $K[x]$. E.g. for $K = \mathbb{Q}(t)$, $x^2 - t \in K[x]$ irreducible. Then $K(\sqrt{t}) = \mathbb{Q}(\sqrt{t}) =\cong K[x]/\langle x^2 - t\rangle$. Then for $s = \sqrt{3}$, we have an extension $\mathbb{Q}(s)/\mathbb{Q}(s^2)$.
- Define $\mathbb{F}_9 = \mathbb{F}_3[x]/\langle x^2 - 2\rangle \cong \mathbb{F}_3(\theta) = \{a + b\theta : a, b \in \mathbb{F}_3\}$ for θ a root of $x^2 - 2$.
- **Proposition**: let $K(\theta)/K$ where θ has minimal polynomial $m(x) \in K[x]$ of degree n. Then

$$K[x]/\langle m(x)\rangle \cong= K(\theta) = \left\{c_0 + c_1\theta + \cdots + c_{n-1}\theta^{n-1} : c_i \in K\right\}$$

  and its elements are written uniquely: $K(\theta)$ is vector space over K of dimension n with basis $\left\{1, \theta, ..., \theta^{n-1}\right\}$.
- **Example**: $\mathbb{Q}\left(\sqrt[3]{2}\right) = \left\{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Q}\right\} \cong \mathbb{Q}[x]/\langle x^3 - 2\rangle$. $\mathbb{Q}\left(\omega\sqrt[3]{2}\right)$ and $\mathbb{Q}\left(w^2\sqrt[3]{2}\right)$ where $\omega = e^{2\pi i/3}$ are isomorphic to $\mathbb{Q}\left(\sqrt[3]{2}\right)$ as $\omega\sqrt[3]{2}$, $\omega\sqrt[3]{4}$ have same minimal polynomial.

3.5. Degrees of field extensions

- **Definition**: **degree** of field extension L/K is

$$[L : K] := \dim_L(F)$$

  Write $[L : K] < \infty$ if degree is finite.
- **Example**:
  - When θ algebraic over K of degree n, $[K(\theta) : K] = n$.
  - Let θ transcendental over K, then $[K(\theta) : K] = \infty$, so $[K(t) : K] = \infty$, $[\mathbb{Q}(\pi) : \mathbb{Q}]$, $[\mathbb{R} : \mathbb{Q}] = \infty$.
- **Proposition**: let $[L : K] < \infty$, then every element in L/K is algebraic over K (in this case, L/K is **algebraic extension**).
- **Tower theorem**: let $K \subseteq M \subseteq L$ **tower** of field extensions. Then
  - $[L : K] < \infty \Longleftrightarrow [L : M] < \infty \land [M : K] < \infty$.
  - $[L : K] = [L : M][M : K]$.
- **Example**:
  - $K = \mathbb{Q} \subset M = \mathbb{Q}(\sqrt{2}) \subset L = \mathbb{Q}(\sqrt{2}, \sqrt{7})$. M/K has basis $\left\{1, \sqrt{2}\right\}$ so $[M : K] = 2$. Let $\sqrt{7} \in \mathbb{Q}\left(\sqrt{2}\right)$, then $\sqrt{7} = c + d\sqrt{2}$, $c, d \in \mathbb{Q}$ so $7 = \left(c^2 + 2d^2\right) + 2cd\sqrt{2}$ so $7 = c^2 + 2d^2$, $0 = 2cd$ so $d^2 = \frac{7}{2}$ or $c^2 = 7$, which are both contradictions. So $[L : K] = 4$ with basis $\{1, \sqrt{2}, \sqrt{7}, \sqrt{14}\}$.
  - Let $K = \mathbb{Q} \subset M = \mathbb{Q}(i) \subset \mathbb{Q}(i, \sqrt{2})$. We know $[\mathbb{Q}(i) : \mathbb{Q}] = 2$, and $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, $[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}] = 2$ (since $i \notin \mathbb{R}$) so $[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}(\sqrt{2})] = 2$.
  - Let $K = \mathbb{Q} \subset M = \mathbb{Q}(\sqrt{2}) \subset L = \mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$. Then $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, $[\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = 3$ so $2 \mid [L : K]$ and $3 \mid [L : K]$ so $6 \mid [L : K]$ so $[L : K] \geq 6$. But $[L : M] \leq 3$ and $[M : K] \leq 2$ so $[L : K] \leq 6$ hence $[L : K] = 6$.
- More generally, we have $[K(\alpha, \beta) : K] \leq [K(\alpha) : K][K(\beta) : K]$.
- **Example**:
  - Let $\theta = \sqrt[3]{4} + 1$. $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt[3]{4})$ so minimal polynomial over $\mathbb{Q}$, m, has $\deg(m) = 3$. $(\theta - 1)^3 = 4$ so minimal polynomial is $x^3 - 3x^2 + 3x - 5$.

- Let $\theta = \sqrt{2} + \sqrt{3}$. $\mathbb{Q}(\sqrt{2}, \theta) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ which has degree 2 over $\mathbb{Q}(\sqrt{2})$ so minimal polynomial of θ over $\mathbb{Q}(\sqrt{2})$ has degree 2, $\left(\theta - \sqrt{2}\right) = \sqrt{3}$ so minimal polynomial is $x^2 - 2\sqrt{2}x - 1$.
- Let $\theta = \sqrt{2} + \sqrt{3}$. $\mathbb{Q} \subset \mathbb{Q}(\theta) \subset \mathbb{Q}(\sqrt{2}, \sqrt{7})$ so $[\mathbb{Q}(\theta) : \mathbb{Q}] \mid [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ so $[\mathbb{Q}(\theta) : \mathbb{Q}] \in \{1, 2, 4\}$. Can't be 1 as $\theta \notin \mathbb{Q}$. If it was 2 then $1, \theta, \theta^2$ are linearly dependent over $\mathbb{Q}$ which leads to a contradiction. So degree of minimal polynomial of θ over $\mathbb{Q}$ is 4. $\theta^2 = 5 + 2\sqrt{6} \Rightarrow \left(\theta^2 - 5\right)^2 = 24$ so minimal polynomial is $x^4 - 10x^2 + 1$.

4. Galois extensions

4.1. Splitting fields

- **Definition**: for field K, $0 \neq f(x) \in K[x]$, L/K is **splitting field** of $f(x)$ over K if
  - $\exists c \in K^\times, \theta_1, ..., \theta_n \in L : f(x) = c(x - \theta_1) \cdots (x - \theta_n)$ ($f(x)$ **splits over** $\boldsymbol{L}$).
  - $L = K(\theta_1, ..., \theta_n)$.
- **Example**:
  - $\mathbb{C}$ is splitting field of $x^2 + 1$ over $\mathbb{R}$, since $x^2 + 1 = (x + i)(x - i)$ and $\mathbb{C} = \mathbb{R}(i, -i) = \mathbb{R}(i)$.
  - $\mathbb{C}$ is not splitting field of $x^2 + 1$ over $\mathbb{Q}$ as $\mathbb{C} \neq \mathbb{Q}(i, -i)$.
  - $\mathbb{Q}$ is splitting field of $x^2 - 36$ over $\mathbb{Q}$.
  - $\mathbb{C}$ is splitting of $x^4 + 1$ over $\mathbb{R}$.
  - $\mathbb{Q}(i, \sqrt{2})$ is splitting field of $x^4 - x^2 - 2$ over $\mathbb{Q}$.
  - $\mathbb{F}_2(\theta)$ where $\theta^3 + \theta + 1 = 0$ is splitting field of $x^3 + x + 1$ over $\mathbb{F}_2$.
  - Consider splitting field of $x^3 - 2$ over $\mathbb{Q}$. Let $\omega = e^{2\pi i/3} = \left(-1 + \sqrt{-3}\right)/2$ then $\mathbb{Q}(\sqrt[3]{2}, \omega)$ is splitting field since it must contain $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$, $\omega^2\sqrt[3]{2}$.
- **Theorem**: let $0 \neq f(x) \in K[x]$, $\deg(f) = n$. Then there exists a splitting field L of $f(x)$ over K with

$$[L : K] \leq n!$$

- **Notation**: for field homomorphism $\varphi : K \to K'$ and $f(x) = a_0 + \cdots + a_n x^n \in K[x]$, write

$$\varphi_*(f(x)) := \varphi(a_0) + \cdots + \varphi(a_n)x^n \in K'[x]$$

- **Lemma**: let $\sigma : K \to K'$ isomorphism and $K(\theta)/K$, θ has minimal polynomial $m(x) \in K[x]$, θ' be root of $\sigma_*(m(x))$. Then there exists unique field isomorphism $\tau : K(\theta) \to K'(\theta')$ such that $\tau(\theta) = \theta'$ and $\forall a \in K, \tau(a) = \sigma(a)$.
- **Theorem**: for field isomorphism $\sigma : K \to K'$ and $0 \neq f(x) \in K[x]$, let L be splitting field of $f(x)$ over K, L' be splitting field of $\sigma_*(f(x))$ over K'. Then there exists a field isomorphism $\tau : L \to L'$ such that $\forall a \in K, \tau(a) = \sigma(a)$.
- **Corollary**: setting $K = K'$ and $\sigma = \mathrm{id}$ implies that splitting fields are unique.

4.2. Normal extensions

- **Definition**: L/K is **normal** if: for all $f(x) \in K[x]$, if f is irreducible and has a root in L then all its roots are in L. In particular, $f(x)$ splits completely as product of linear factors in $L[x]$. So the minimal polynomial of $\theta \in L$ over K has all its roots in L and can be written as product of linear factors in $L[x]$.

- **Example**:
  - If $[L : K] = 1$ then L/K is normal.
  - If $[L : K] = 2$ then L/K is normal: let $\theta \in L$ have minimal polynomial $m(x) \in K[x]$, then $K \subseteq K(\theta) \subseteq L$ so $\deg(m(x)) = [K(\theta) : K] \in \{1, 2\}$:
    - If $\deg(m(x)) = 1$ then $m(x)$ is already linear.
    - If $\deg(m(x)) = 2$ then $m(x) = (x - \theta)m_1(x)$, $m_1(x) \in L[x]$ is linear so $m(x)$ splits completely in $L[x]$.
  - If $[L : K] = 3$ then L/K is not necessarily normal. Let θ be root of $x^3 - 2 \in \mathbb{Q}[x]$. Other two roots are $\omega\theta$, $\omega^2\theta$ where $\omega = e^{2\pi i/3}$. If $\omega\theta \in \mathbb{Q}(\theta)$ then $\omega = \frac{\omega\theta}{\theta} \in L$ so $\mathbb{Q} \subset \mathbb{Q}(\omega) \subset \mathbb{Q}(\theta)$ but $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$ which doesn't divide $[\mathbb{Q}(\theta) : \mathbb{Q}] = 3$.
  - Let $\theta \in \mathbb{C}$ be root of irreducible $f(x) = x^3 - 3x - 1 \in \mathbb{Q}[x]$. Let $\theta = u + v$, then $(u + v)^3 - 3uv(u + v) - (u^3 + v^3) \equiv 0$ implies $uv = 1 = u^3v^3$, $u^3 + v^3 = 1$. So $(y - u^3)(y - v^3) = y^2 - y + 1$ has roots u^3 and v^3. So the three roots of f are

    $$\begin{aligned} u + v &= e^{\pi i/9} + e^{-\pi i/9} = 2\cos(\pi/9) \\ \omega u + \omega^2 v &= e^{7\pi i/9} + e^{-7\pi i/9} = 2\cos(7\pi/9) \\ \omega^2 u + \omega v &= e^{13\pi i/9} + e^{-13\pi i/9} = 2\cos(13\pi/9) \end{aligned}$$

    Furthermore, for each i, j, $\theta_i \in \mathbb{Q}(\theta_j)$, e.g.

    $$\theta_2 = 2\cos\left(\pi - \frac{2\pi}{9}\right) = -2\cos\left(\frac{2\pi}{9}\right) = -2\left(2\cos\left(\frac{\pi}{9}\right)^2 - 1\right) = 2 - \theta_1^2$$

    So $\mathbb{Q}(\theta)$ contains all roots of $f(x)$.
- **Theorem (normality criterion)**: L/K is finite and normal iff L is splitting field for some $0 \neq f(x) \in K[x]$ over K.
- **Example**:
  - $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7})/Q$ is normal as it is the splitting field of $f(x) = (x^2 - 2)(x^2 - 3)(x^2 - 5)(x^2 - 7) \in \mathbb{Q}[x]$.
  - $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal but $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$ is normal as it is the splitting field of $x^3 - 2 \in \mathbb{Q}$.
  - $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not normal but $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$ is normal.
  - Let θ root of $f(x) = x^3 - 3x - 1 \in \mathbb{Q}[x]$. Then $\mathbb{Q}(\theta)/\mathbb{Q}$ is normal as is splitting field of $f(x)$ over $\mathbb{Q}$.
  - $\mathbb{F}_2(\theta)/\mathbb{F}_2$ where $\theta^3 + \theta^2 + 1 = 0$ is normal.
  - $\mathbb{F}_p(\theta)/\mathbb{F}_p(t)$ where $\theta^p = t$ is normal as it is the splitting field of $x^p - t = x^p - \theta^p = (x - \theta)^p$ so $f(x)$ splits into linear factors in $L[x]$.
- **Definition**: field N is **normal closure** of L/K if $K \subseteq L \subseteq N$, N/K is normal, and if $K \subseteq L \subseteq N' \subseteq N$ with N'/K normal then $N = N'$.
- **Theorem**: every finite extension L/K has normal closure N.

- **Definition**: $\text{Aut}(L/K)$ is group of K-automorphisms of L/K with composition the group operation.
- **Example**:
  - $\text{Aut}(\mathbb{C}/\mathbb{R})$ contains at least two elements: complex conjugation: $\sigma(a+bi) = a - bi$ and the identity map $\text{id} = \sigma^2$. If $\tau \in \text{Aut}(\mathbb{C}/\mathbb{R})$ then $\tau(a+bi) = a + b\tau(i)$. But $\tau(i)^2 = \tau(i^2) = \tau(-1) = -1$ hence $\tau(i) = \pm i$. So there are only two choices for τ. So $\text{Aut}(\mathbb{C}/\mathbb{R}) = \{\text{id}, \sigma\}$.
  - Let $f(x) = x^2 + px + q \in \mathbb{Q}[x]$ irreducible with roots θ, θ'. Then $\text{Aut}(\mathbb{Q}(\theta)/\mathbb{Q}) = \{\text{id}, \sigma\} \cong \mathbb{Z}/2$ where $\sigma(a + b\theta) = a + b\theta'$.
  - Let θ root of $x^3 - 2$, let $\sigma \in \text{Aut}(\mathbb{Q}(\theta)/\mathbb{Q})$. Now $\sigma(\theta)^3 = \sigma(\theta^3) = \sigma(2) = 2$ so $\sigma(\theta) \in \{\theta, \omega\theta, \omega^2\theta\}$ but $\omega\theta, \omega^2\theta \notin \mathbb{Q}(\theta)$ so $\sigma(\theta) = \theta \Longrightarrow \sigma = \text{id}$.
  - Let $\theta^p = t$, $\sigma \in \text{Aut}\big(\mathbb{F}_p(\theta)/\mathbb{F}_p(t)\big)$. Then

$$\sigma(\theta)^p = \sigma(\theta^p) = \sigma(t) = t = \theta^p$$

    so $(\sigma(\theta) - \theta))^p = \sigma(\theta)^p - \theta^p = 0 \Longrightarrow \sigma(\theta) = \theta \Longrightarrow \sigma = \text{id}$.
  - Let $\sigma \in \text{Aut}(\mathbb{R}/\mathbb{Q})$. Then $\alpha \leq \beta \in \mathbb{R} \Longrightarrow \beta - \alpha = \gamma^2$, $\gamma \in \mathbb{R}$, so $\sigma(\beta) - \sigma(a) = \sigma(\gamma)^2 \geq 0$ so $\sigma(\alpha) \leq \sigma(\beta)$. Given $\alpha \in \mathbb{R}$, there exist sequences $(r_n), (s_n) \subset \mathbb{Q}$ with $r_n \leq \alpha \leq s_n$ and $r_n \to \alpha$, $s_n \to \alpha$ as $n \to \infty$. Hence $r_n = \sigma(r_n) \leq \sigma(\alpha) \leq \sigma(s_n) = s_n$ so $\sigma(\alpha) = \alpha$ by squeezing. Hence $\text{Aut}(\mathbb{R}/\mathbb{Q}) = \{\text{id}\}$.
- **Theorem**: let $L = K(\theta)$, θ root of irreducible $f(x) \in K[x]$, $\deg(f) = n$. Then $|\text{Aut}(L/K)| \leq n$, with equality iff $f(x)$ has n distinct rotos in L.
- **Theorem**: let L/K be finite extension. Then $|\text{Aut}(L/K)| \leq [L : K]$, with equality iff L/K is normal and minimal polynomial of every $\theta \in L$ over K has no repeated roots (in a splitting field).

4.3. Separable extensions

- **Definition**: let L/K finite extension.
  - $\theta \in L$ is **separable over K** if its minimal polynomial over K has no repeated roots (in its splitting field).
  - L/K is **separable** if every $\theta \in L$ is separable over K.
- **Example**:
  - Let $\theta^3 = 2$, the minimal polynomial of θ over $\mathbb{Q}$ is $x^3 - 2 = (x - \theta)(x - \omega\theta)(x - \omega^2\theta)$, so $\mathbb{Q}(\theta)/\mathbb{Q}$ is not normal.
  - Let $\theta^3 = t$, so minimal polynomial of θ over $\mathbb{F}_3(t)$ is $x^3 - t = (x - \theta)^3$, so $\mathbb{F}_3(\theta)/\mathbb{F}_3(t)$ is not separable but is normal.
- **Definition**: let $f(x) = \sum_{i=0}^n a_i x^i \in K[x]$. **Formal derivative** of $f(x)$ is

$$Df(x) = D(f) \coloneqq \sum_{i=1}^n i a_i x^{i-1} \in K[x]$$

- Formal derivative satisfies:

$$D(f+g) = D(f) + D(g), \quad D(fg) = f \cdot D(g) + D(f) \cdot g, \quad \forall a \in K, D(a) = 0$$

Also $\deg(D(f)) < \deg(f)$. But if $\operatorname{char}(K) = p$, then $D(x^p) = px^{p-1} = 0$ so it is not always true that $\deg(D(f)) = \deg(f) - 1$.

- **Theorem (sufficient conditions for separability)**: finite extension L/K is separable if any of the following hold:
  - $\operatorname{char}(K) = 0$,
  - $\operatorname{char}(K) = p$ and $K = \{b^p : b \in K\}$ for prime p,
  - $\operatorname{char}(K) = p$ and $p \nmid [L : K]$.
- **Definition**: K is a **perfect field** if the first two of the above properties hold.
- **Remark**: all finite extensions of any perfect extension (e.g. $\mathbb{Q}, \mathbb{F}_p$) are separable (recall Fermat's little theorem: $\forall a \in \mathbb{F}_p, a = a^p$). So to find a non-separable extension L/K, we need $\operatorname{char}(K) = p > 0$, K infinite and $p \mid [L : K]$. For example, $L = \mathbb{F}_p(\theta)$, $K = \mathbb{F}_p(t)$ where $\theta^p = t$.
- **Theorem**: let $\alpha_1, ..., \alpha_n$ algebraic over K, then $K(\alpha_1, ..., \alpha_n)/K$ is separable iff every α_i is separable over K.
- **Remark**: for tower $K \subseteq M \subseteq L$, L/K is separable iff L/M and M/K are separable. However, the same statement for normality does not hold.
- **Theorem of the Primitive Element**: let L/K finite and separable. Then L/K is simple, i.e. $\exists \alpha \in L : L = K(\alpha)$.

4.4. The fundamental theorem of Galois theory

- **Definition**: finite extension L/K is **Galois extension** if it is normal and separable. Equivalently, $|\operatorname{Aut}(L/K)| = [L : K]$. When L/K is Galois, the **Galois group** is $\operatorname{Gal}(L/K) := \operatorname{Aut}(L/K)$.
- **Definition**: let $\mathcal{F} := \{\text{intermediate fields of } L/K\}$ and $\mathcal{G} := \{\text{subgroups of } \operatorname{Gal}(L/K)\}$. Define the map $\Gamma : \mathcal{F} \to \mathcal{G}$, $\Gamma(M) = \operatorname{Gal}(L/M)$.
- **Definition**: let L field, G a group of automorphisms of L. **Fixed field** L^G of G is set of elements in L which are invariant under all automorphisms in G:

$$L^G := \{\alpha \in L : \forall \alpha \in G, \sigma(\alpha) = \alpha\}$$

- **Theorem**: if G is fintie group of automorphisms of L then L^G is subfield of L and $\left[L : L^G\right] = |G|$.
- **Corollary**: if L/K is Galois then
  - $L^{\operatorname{Gal}(L/K)} = K$.
  - If $L^G = K$ for some group G of K-automorphisms of L, then $G = \operatorname{Gal}(L/K)$.
- **Remark**: if L/K is Galois and $\alpha \in L$ but $\alpha \notin K$, then there exists an automorphism $\sigma \in \operatorname{Gal}(L/K)$ such that $\sigma(\alpha) \neq \alpha$.
- **Definition**: for H subgroup of $\operatorname{Gal}(L/K)$, set $L^H := \{\alpha \in L : \forall \sigma \in H, \sigma(\alpha) = \alpha\}$, then $K \subseteq L^H \subseteq L$. Define $\Phi : \mathcal{G} \to \mathcal{F}$, $\Phi(H) = L^H$.
- Γ and Φ are inclusion-reversing: $M_1 \subseteq M_2 \Longrightarrow \Gamma(M_2) \subseteq \Gamma(M_1)$, and $H_1 \subseteq H_2 \Longrightarrow \Phi(H_2) \subseteq \Phi(H_1)$.
- **Theorem A**: for finite Galois extension L/K,
  - $\Gamma : \mathcal{F} \to \mathcal{G}$ and $\Phi : \mathcal{F} \to \mathcal{F}$ are mutually inverse bijections (the **Galois correspondence**).
  - For $M \in \mathcal{F}$, L/M is Galois and $|\operatorname{Gal}(L/M)| = [L : M]$.

  - For $H \in \mathcal{G}$, L/L^H is Galois and $\mathrm{Gal}(L/L^H) = H$.
- **Remark**: $\mathrm{Gal}(L/K)$ acts on $\mathcal{F}$: given $\sigma \in \mathrm{Gal}(L/K)$ and $K \subseteq M \subseteq L$, consider $\sigma(M) = \{\sigma(\alpha) : \alpha \in M\}$ which is a subfield of L and contains K, since σ fixes elements of K. Given another automorphism $\tau : L \to L$,

$$\begin{aligned}\tau \in \mathrm{Gal}(L/\sigma(M)) &\iff \forall \alpha \in M, \tau(\sigma(\alpha)) = \sigma(\alpha) \\ &\iff \forall \alpha \in M, \sigma^{-1}(\tau(\sigma(\alpha))) = \alpha \\ &\iff \sigma^{-1}\tau\sigma \in \mathrm{Gal}(L/M) \\ &\iff \tau \in \sigma \ \mathrm{Gal}(L/M)\sigma^{-1}\end{aligned}$$

  Hence $\sigma \ \mathrm{Gal}(L/M)\sigma^{-1}$ and $\mathrm{Gal}(L/M)$ are conjugate subgroups of $\mathrm{Gal}(L/K)$. Now

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

- **Theorem B**: for finite Galois extension L/K, $G = \mathrm{Gal}(L/K)$ and $K \subseteq M \subseteq L$. Then the following are equivalent:
  - M/K is Galois.
  - $\forall \sigma \in G, \quad \sigma(M) = M$.
  - $H = \mathrm{Gal}(L/M)$ is normal subgroup of $G = \mathrm{Gal}(L/K)$.

  When these conditions hold, we have $\mathrm{Gal}(M/K) \cong G/H$.