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.
  - $\operatorname{im}(\varphi) = \{\varphi(a) : a \in K\}$ 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** $\operatorname{char}(K)$ of field K is

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

  where $\chi : \mathbb{Z} \to K$, $\chi(m) = 1 + \cdots + 1$ (m times).
- **Example**: $\operatorname{char}(\mathbb{Q}) = \operatorname{char}(\mathbb{R}) = \operatorname{char}(\mathbb{C}) = 0$, $\operatorname{char}(\mathbb{F}_p) = p$ for p prime.
- **Lemma**: for any field K, $\operatorname{char}(K)$ is either 0 or a prime.
- **Theorem**:
  - $\operatorname{char}(K) = 0$ iff $\mathbb{Q}$ is the prime subfield of K.
  - $\operatorname{char}(K) = p > 0$ 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

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

(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 $\mathrm{Frac}(R)$ 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 $I_K(\theta) \coloneqq \{f(x) \in K[x] : f(\theta) = 0\}$. 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, $K_m \coloneqq K[x]/\langle m(x) \rangle$. 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 $L_1 = L_2$ then φ is ***K*-automorphism**.
- **Example**:
  - Complex conjugation $\mathbb{C} \to \mathbb{C}$ is $\mathbb{R}$-automorphism.
  - Let K field, $\operatorname{char}(K) \neq 2$, $\sqrt{2} \notin K$, 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 $[M : K]$. 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 $[L : K] = 4$.