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 $\chi : \mathbb{Z} \to K$, $\chi(m) = 1 + \dots + 1$ (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 $f(x) = a_0 + a_1 x + \dots + a_n x_n$, $a_n \neq 0$ 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 $c \mid a_n$.