

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 $x^3 + a_2x^2 + a_1x + a_0 = 0$:
 - Tschirnhaus transformation** is substitution $t = x + \frac{a_2}{3}$, giving

$$t^3 + pt + q = 0, \quad p := \frac{-a_2^2 + 3a_1}{3}, \quad q := \frac{2a_2^3 - 9a_1a_2 + 27a_0}{27}$$

This is a **reduced** (or **depressed**) 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

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

$$\text{so } u^3, v^3 = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}.$$

- 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 independently 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).

1.2. Quartic equations over \mathbb{C}

- For general quartic equation $x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0$:
 - 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 $a^2 - b^2 = (a + b)(a - b)$:

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

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

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

- 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.

2. Fields and polynomials

2.1. Basic properties of fields

- **Definition:** ring R is **field** if every element of $R - \{0\}$ has multiplicative inverse and $1 \neq 0 \in R$.
- **Lemma:** every field is integral domain.
- **Definition:** **field homomorphism** is ring homomorphism $\varphi : K \rightarrow L$ 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 $\varphi : K \rightarrow L$ field homomorphism.
 - $\text{im}(\varphi) = \{\varphi(a) : a \in K\}$ is 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 field. L is **field extension** of K .
- The above lemma shows image of $\varphi : K \rightarrow L$ is subfield of L .
- **Lemma:** intersections of subfields are subfields.
- **Definition:** **prime subfield** of L is intersection of all subfields of L .
- **Definition:** **characteristic** $\text{char}(K)$ of field K is

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

(or 0 if this does not exist) where $\chi : \mathbb{Z} \rightarrow K$, $\chi(m) = 1 + \dots + 1$ (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 prime.
- **Theorem:**
 - If $\text{char}(K) = 0$ then prime subfield of K is $\cong \mathbb{Q}$.
 - If $\text{char}(K) = p > 0$ then prime subfield of K is $\cong \mathbb{F}_p$.
- **Corollary:**
 - If \mathbb{Q} is subfield of K then $\text{char}(K) = 0$.
 - If \mathbb{F}_p is subfield of K for prime p then $\text{char}(K) = p$.
- **Remark:** let $\text{char}(K) = p$, then $p \mid \binom{p}{i}$ so $(a + b)^p = a^p + b^p$ in K . Also in $K[x]$ for $p > 2$ prime, $x^p - 1 = (x - 1)^p$.
- **Fermat's little theorem:** $\forall a \in \mathbb{F}_p, a^p = a$.

2.2. Polynomials over fields

- **Definition:** **degree** of $f(x) = a_0 + a_1x + \dots + a_nx_n$, $a_n \neq 0$ is $\deg(f(x)) = n$.
 - Degree of zero polynomial is $\deg(0) = -\infty$.
 - $\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$.

- $\deg(f(x) + g(x)) \leq \max\{\deg(f(x)), \deg(g(x))\}$ with equality if $\deg(f(x)) \neq \deg(g(x))$.
- 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

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

where $f_1(x)/g_1(x) = f_2(x)/g_2(x) \iff f_1(x)g_2(x) = f_2(x)g_1(x)$. (We can construct the field of fractions for any integral domain).

- $K[x]$ is PID and so UFD.
- **Definition:** for field K , $f(x) \in K[x]$ **irreducible in $K[x]$** (or $f(x)$ is **irreducible over K**) if
 - $\deg(f(x)) \geq 1$ and
 - $f(x) = g(x)h(x) \implies g(x)$ 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 $f(x) = a_0 + \dots + a_n x^n \in \mathbb{Z}[x]$ has rational root $\frac{b}{c} \in \mathbb{Q}$ with $\gcd(b, c) = 1$ then $b \mid a_0$ and $c \mid a_n$. **Note:** this can't be used to 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 $\exists r \in \mathbb{Q} : rg(x), r^{-1}h(x) \in \mathbb{Z}[x]$. i.e. if $f(x)$ can be factored in $\mathbb{Q}[x]$ it can be factored 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 $1 = ar \implies a = r = \pm 1$. $1 = ct \implies c = t = \pm 1$. $-3 = b + s$ 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 $f(x) = a_0 + \dots + a_n x^n \in \mathbb{Z}[x]$. If exists prime $p \nmid a_n$ such that $\bar{f}(x)$ is irreducible in $\mathbb{F}_p[x]$, then $f(x)$ irreducible in $\mathbb{Q}[x]$.
- **Example:** let $f(x) = 8x^3 + 14x - 9$. Reducing mod 7, $\bar{f}(x) = x^3 - 2 \in \mathbb{F}_7[x]$. 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 $\text{Frac}(R)$ instead of \mathbb{Q} : e.g. 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 $f(x) = a_0 + \dots + a_n x^n \in \mathbb{Z}[x]$, prime $p \in \mathbb{Z}$ such that $p \mid a_0, \dots, p \mid a_{n-1}$, $p \nmid a_n$, $p^2 \nmid a_0$. Then $f(x)$ irreducible in $\mathbb{Q}[x]$.
- **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

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

Now

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

so can apply Eisenstein with $p = p$.

- **Generalised Eisenstein's criterion:** let R be integral domain, $K = \text{Frac}(R)$,

$$f(x) = a_0 + \dots + a_n x^n \in R[x]$$

If there is irreducible $p \in R$ with

$$p \mid a_0, \dots, p \mid a_{n-1}, p \nmid a_n, p^2 \nmid a_0$$

then $f(x)$ is irreducible in $K[x]$.

3. Field extensions

3.1. Definitions and examples

- **Definition: field extension** L/K is field L containing subfield K . Can specify homomorphism $\iota : K \rightarrow L$ (which is injective).
- **Example:**
 - \mathbb{C}/\mathbb{R} , \mathbb{C}/\mathbb{Q} , \mathbb{R}/\mathbb{Q} .
 - $L = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is field extension of \mathbb{Q} . $\mathbb{Q}(\theta)$ is field extension of \mathbb{Q} where θ is root of $f(x) \in \mathbb{Q}[x]$.
 - $L = \mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Q}\}$ is smallest subfield of \mathbb{R} containing \mathbb{Q} and $\sqrt[3]{2}$.
 - $K(t)$ 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:** $\mathbb{Q}(\sqrt{2}, \sqrt{7}) = \{a + b\sqrt{2} + c\sqrt{7} + d\sqrt{14} : a, b, c, d, \in \mathbb{Q}\}$ is \mathbb{Q} with $S = \{\sqrt{2}, \sqrt{7}\}$.
- **Example:** \mathbb{R}/\mathbb{Q} is not simple extension.
- **Definition:** **tower** is 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

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

- **Definition:** let $L_1/K, L_2/K$ field extensions, $\varphi : L_1 \rightarrow L_2$ 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**.
- **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 $\pi : K[x] \rightarrow K_m$ is canonical projection, then θ has minimal polynomial $m(x)$ and $K_m \cong K(\theta)$.

- **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 $\varphi : K_m \rightarrow K_L(\tau)$ such that $\varphi(\theta) = \tau$.
- **Example:**
 - Complex conjugation $\mathbb{C} \rightarrow \mathbb{C}$ 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 $K(\sqrt{2}) \cong K[x]/\langle x^2 - 2 \rangle$ is field extension of K and $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ is K -automorphism.
- **Proposition:** let θ transcendental over K , then exists unique K -isomorphism $\varphi : K(t) \rightarrow K(\theta)$ such that $\varphi(t) = \theta$:

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

3.4. Explicit examples of simple extensions

- Let $r \in K^\times$ non-square in K , $\text{char}(K) \neq 2$, then $x^2 - r$ irreducible in $K[x]$. E.g. for $K = \mathbb{Q}(t)$, $x^2 - t \in K[x]$ is irreducible. Then $K(\sqrt{t}) = \mathbb{Q}(\sqrt{t}) \cong K[x]/\langle x^2 - t \rangle$.
- 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

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

and its elements are written uniquely: $K(\theta)$ is vector space over K of dimension n with basis $\{1, \theta, \dots, \theta^{n-1}\}$.

- **Example:** $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Q}\} \cong \mathbb{Q}[x]/\langle x^3 - 2 \rangle$. $\mathbb{Q}(\omega\sqrt[3]{2})$ and $\mathbb{Q}(\omega^2\sqrt[3]{2})$ where $\omega = e^{2\pi i/3}$ are isomorphic to $\mathbb{Q}(\sqrt[3]{2})$ 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

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

- **Example:**
 - When θ algebraic over K of degree n , $[K(\theta) : K] = n$.
 - Let θ transcendental over K , then $[K(\theta) : K] = \infty$, so $[K(t) : K] = \infty$, $[\mathbb{Q}(\pi) : \mathbb{Q}]$, $[\mathbb{R} : \mathbb{Q}] = \infty$.
- **Definition:** L/K is **algebraic extension** if every element in L is algebraic over K .
- **Proposition:** let $[L : K] < \infty$, then L/K is algebraic extension and $L = K(\alpha_1, \dots, \alpha_n)$ for some $\alpha_1, \dots, \alpha_n \in L$.
- **Tower law:** let $K \subseteq M \subseteq L$ tower of field extensions. Then
 - $[L : K] < \infty \iff [L : M] < \infty \wedge [M : K] < \infty$.
 - $[L : K] = [L : M][M : K]$.
- **Example:**

- $K = \mathbb{Q} \subset M = \mathbb{Q}(\sqrt{2}) \subset L = \mathbb{Q}(\sqrt{2}, \sqrt{7})$. M/K has basis $\{1, \sqrt{2}\}$ so $[M : K] = 2$. Let $\sqrt{7} \in \mathbb{Q}(\sqrt{2})$, then $\sqrt{7} = c + d\sqrt{2}$, $c, d \in \mathbb{Q}$ so $7 = (c^2 + 2d^2) + 2cd\sqrt{2}$ 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 $i \notin \mathbb{Q}(\sqrt{2})$) 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, $\theta - \sqrt{2} = \sqrt{3}$ so minimal polynomial is $x^2 - 2\sqrt{2}x - 1$.
 - Let $\theta = \sqrt{2} + \sqrt{3}$. $\mathbb{Q} \subset \mathbb{Q}(\theta) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ 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. $\theta^2 = 5 + 2\sqrt{6} \Rightarrow (\theta^2 - 5)^2 = 24$ 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
 - $\exists c \in K^\times, \theta_1, \dots, \theta_n \in L : f(x) = c(x - \theta_1) \cdots (x - \theta_n)$ ($f(x)$ **splits over** L).
 - $L = K(\theta_1, \dots, \theta_n)$.
- **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 $x^4 - x^2 - 2 = (x^2 + 1)(x^2 - 2) = (x + i)(x - i)(x + \sqrt{2})(x - \sqrt{2})$ 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 $\omega = e^{2\pi i/3} = (-1 + \sqrt{-3})/2$ 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 $\varphi : K \rightarrow K'$ 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 $\sigma : K \rightarrow K'$ 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 K -isomorphism $\tau : K(\theta) \rightarrow K'(\theta')$ such that $\tau(\theta) = \theta'$.
- **Theorem:** for field isomorphism $\sigma : K \rightarrow K'$ 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 $\tau : L \rightarrow L'$ such that $\forall a \in K, \tau(a) = \sigma(a)$.
- **Corollary:** setting $K = K'$ and $\sigma = \text{id}$ 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

$$\theta_1 = u + v = e^{\pi i/9} + e^{-\pi i/9} = 2 \cos(\pi/9)$$

$$\theta_2 = \omega u + \omega^2 v = e^{7\pi i/9} + e^{-7\pi i/9} = 2 \cos(7\pi/9)$$

$$\theta_3 = \omega^2 u + \omega v = e^{13\pi i/9} + e^{-13\pi i/9} = 2 \cos(13\pi/9)$$

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

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

Also $\theta_1 + \theta_2 + \theta_3 = 0$ so $\theta_3 \in \mathbb{Q}(\theta_1)$. So $\mathbb{Q}(\theta_1)$ 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:**

- $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7})/\mathbb{Q}$ 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, as $\mathbb{F}_2(\theta)$ contains all roots of $x^3 + x^2 + 1$.
- $\mathbb{F}_p(\theta)/\mathbb{F}_p(t)$ 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, unique up to a K -isomorphism.
- **Definition:** $\text{Aut}(L/K)$ is group of K -automorphisms of L/K with composition as 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 distinct 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 $\sigma(\theta) = \theta \implies \sigma = \text{id}$.
 - Let $\theta^p = t$, $\sigma \in \text{Aut}(\mathbb{F}_p(\theta)/\mathbb{F}_p(t))$. Then

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

so $(\sigma(\theta) - \theta)^p = \sigma(\theta)^p - \theta^p = 0 \implies \sigma(\theta) = \theta \implies \sigma = \text{id}$.

- Let $\sigma \in \text{Aut}(\mathbb{R}/\mathbb{Q})$. Then $\alpha \leq \beta \in \mathbb{R} \implies \beta - \alpha = \gamma^2$, $\gamma \in \mathbb{R}$, so $\sigma(\beta) - \sigma(\alpha) = \sigma(\gamma)^2 \geq 0$ 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 $r_n \rightarrow \alpha$, $s_n \rightarrow \alpha$ as $n \rightarrow \infty$. 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 roots 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 $K = \mathbb{F}_p(t)$, then $f(x) = x^p - t \in K[x]$ is irreducible by Eisenstein's criterion with $p = t$, and $f(x) = x^p - \theta^p = (x - \theta)^p$ so θ is root of multiplicity $p \geq 2$. So $\mathbb{F}_p(\theta)/\mathbb{F}_p(t)$ is normal but not separable.
- **Definition:** let $f(x) = \sum_{i=0}^n a_i x^i \in K[x]$. **Formal derivative** of $f(x)$ is

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

- 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 $\text{char}(K) = p$, 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:
 - $\text{char}(K) = 0$,
 - $\text{char}(K) = p$ and $K = \{b^p : b \in K\}$ for prime p ,
 - $\text{char}(K) = p$ and $p \nmid [L : K]$.
- **Definition:** K is **perfect field** if either of first two of 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 $\text{char}(K) = p > 0$, 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 $\alpha_1, \dots, \alpha_n$ algebraic over K , then $K(\alpha_1, \dots, \alpha_n)/K$ 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, $|\text{Aut}(L/K)| = [L : K]$. When L/K is Galois, the **Galois group** is $\text{Gal}(L/K) := \text{Aut}(L/K)$.
- **Definition:** let $\mathcal{F} := \{\text{intermediate fields of } L/K\}$ and $\mathcal{G} := \{\text{subgroups of } \text{Gal}(L/K)\}$. Define the map $\Gamma : \mathcal{F} \rightarrow \mathcal{G}$, $\Gamma(M) = \text{Gal}(L/M)$.
- **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 :

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

- **Theorem:** if G is finite group of automorphisms of L then L^G is subfield of L and $[L : L^G] = |G|$.

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

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

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

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

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

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

- **Example:** let L/K be Galois, $[L : K] = p$ prime.
 - By the tower law, any $K \subseteq M \subseteq L$ has $[L : M] \in \{1, p\}$, $[M : K] \in \{p, 1\}$, so $M = L$ or K . In both cases, M/K is normal.
 - $|\text{Gal}(L/K)| = [L : K] = p$ so $\text{Gal}(L/M) \cong \mathbb{Z}/p$, so the only subgroups are $\text{Gal}(L/K)$ and $\{\text{id}\}$. In both cases, H is normal subgroup of $\text{Gal}(L/K)$.

4.5. Computations with Galois groups

- **Example - quadratic extension:** $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is normal (since degree is 2) and separable (since characteristic is zero). Any element of $\varphi \in G = \text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ is

determined by the image of $\sqrt{2}$. But $\varphi(\sqrt{2})^2 = \varphi(2) = 2$ so $\varphi(\sqrt{2}) = \pm\sqrt{2}$. This gives two automorphisms $\text{id}(\sqrt{2}) = \sqrt{2}$ and $\sigma(\sqrt{2}) = -\sqrt{2}$. So $G = \{\text{id}, \sigma\} = \langle \sigma \rangle \cong \mathbb{Z}/2$. Subgroup $\{\text{id}\}$ corresponds to $\mathbb{Q}(\sqrt{2})$, G corresponds to \mathbb{Q} .

- **Example - biquadratic extension:** $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ over \mathbb{Q} is normal (as splitting field of $(x^2 - 2)(x^2 - 3)$ over \mathbb{Q}) and separable (as $\text{char}(\mathbb{Q}) = 0$), so is Galois extension. Let σ be given as before.
 - Suppose $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$, then $\sigma(\sqrt{3})^2 = \sigma(3) = 3$, so $\sigma(\sqrt{3}) = \pm\sqrt{3}$.
 - If $\sigma(\sqrt{3}) = \sqrt{3}$, then $\sqrt{3} \in \mathbb{Q}(\sqrt{2})^{\{\text{id}, \sigma\}} = \mathbb{Q}$: contradiction.
 - If $\sigma(\sqrt{3}) = -\sqrt{3}$, then $\sigma(\sqrt{2})\sigma(\sqrt{3}) = \sigma(\sqrt{6}) = (-\sqrt{2})(-\sqrt{3}) = \sqrt{6}$, so $\sqrt{6} \in \mathbb{Q}(\sqrt{2})^{\{\text{id}, \sigma\}} = \mathbb{Q}$: contradiction.
 - So $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, hence $[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4$.
 - Now $G = \text{Gal}(L/\mathbb{Q})$ has order $[L : \mathbb{Q}] = 4$, so $G \cong \mathbb{Z}/4$ or $\mathbb{Z}/2 \times \mathbb{Z}/2$.
 - For $\varphi \in G$, $\varphi(\sqrt{2})^2 = 2 \implies \varphi(\sqrt{2}) = \pm\sqrt{2}$, $\varphi(\sqrt{3})^2 = 3 \implies \varphi(\sqrt{3}) = \pm\sqrt{3}$. So there are four choices, corresponding to choices of \pm signs.
 - Define σ, τ by $\sigma(\sqrt{2}) = -\sqrt{2}$, $\sigma(\sqrt{3}) = \sqrt{3}$, $\tau(\sqrt{2}) = \sqrt{2}$, $\tau(\sqrt{3}) = -\sqrt{3}$. Now $\sigma^2 = \tau^2 = \text{id}$, $\sigma\tau(\sqrt{2}) = -\sqrt{2}$, $\sigma\tau(\sqrt{3}) = -\sqrt{3}$ and $\sigma\tau = \tau\sigma$.
 - So $G = \langle \sigma, \tau : \sigma^2 = \tau^2 = \text{id}, \sigma\tau = \tau\sigma \rangle = \langle \sigma \rangle \times \langle \tau \rangle \cong \mathbb{Z}/2 \times \mathbb{Z}/2$.
 - G has proper subgroups $H_1 = \langle \sigma \rangle$, $H_2 = \langle \tau \rangle$, $H_3 = \langle \sigma\tau \rangle$.
 - So the intermediate fields are $L^{H_1}, L^{H_2}, L^{H_3}$.
 - $\sigma(\sqrt{3}) = \sqrt{3} \implies \sqrt{3} \in L^{H_1}$ so $\mathbb{Q}(\sqrt{3}) \subseteq L^{H_1}$, but $[L : \mathbb{Q}(\sqrt{3})] = 2 = |H_1| = [L : L^{H_1}]$. Hence $L^{H_1} = \mathbb{Q}(\sqrt{3})$. Similarly $L^{H_2} = \mathbb{Q}(\sqrt{2})$.
 - $\sigma\tau(\sqrt{6}) = \sqrt{6} \implies \sqrt{6} \in L^{H_3}$, so $L^{H_3} = \mathbb{Q}(\sqrt{6})$.
- **Remark:** it is not generally true that $[K(\sqrt{a}, \sqrt{b}) : K] = 4$, e.g. $\mathbb{Q}(\sqrt{2}, \sqrt{8}) = \mathbb{Q}(\sqrt{2})$.
- **Remark:** can generalise above example to arbitrary $K(\sqrt{a}, \sqrt{b})/K$ where $\text{char}(K) \neq 2$, and $a, b \in K$, $a, b, ab \notin (K^\times)^2$ where $(K^\times)^2$ is set of squares of K^\times .
- **Example - degree 8 extension:**
 - Consider $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ over \mathbb{Q} . L is splitting field of $(x^2 - 2)(x^2 - 3)(x^2 - 5)$, so is normal, and $\text{char}(\mathbb{Q}) = 0$, so is separable, so is Galois.
 - Let $M = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. By above, $\text{Gal}(M/\mathbb{Q}) = \langle \sigma \rangle \times \langle \tau \rangle \cong \mathbb{Z}/2 \times \mathbb{Z}/2$.
 - Suppose $\sqrt{5} \in M$. Then $\sigma(\sqrt{5})^2 = \tau(\sqrt{5})^2 = 5$, so $\sigma(\sqrt{5}) = \pm\sqrt{5}$, $\tau(\sqrt{5}) = \pm\sqrt{5}$.
 - If $\sigma(\sqrt{5}) = \sqrt{5}$, then $\sqrt{5} \in M^{(\sigma)} = \mathbb{Q}(\sqrt{3})$.
 - If $\tau(\sqrt{5}) = \sqrt{5}$, $\sqrt{5} \in M^{(\sigma, \tau)} = \mathbb{Q}$: contradiction.
 - If $\tau(\sqrt{5}) = -\sqrt{5}$, then since $\sqrt{15} \in M^{(\sigma)}$, $\tau(\sqrt{15}) = \sqrt{15}$, so $\sqrt{15} \in M^{(\sigma, \tau)} = \mathbb{Q}$: contradiction.
 - If $\sigma(\sqrt{5}) = -\sqrt{5}$, then $\sigma(\sqrt{10}) = \sigma(\sqrt{2})\sigma(\sqrt{5}) = (-\sqrt{2})(-\sqrt{5}) = \sqrt{10}$, so $\sqrt{10} \in M^{(\sigma)} = \mathbb{Q}(\sqrt{3})$.
 - If $\tau(\sqrt{5}) = \sqrt{5}$, $\tau(\sqrt{10}) = \sqrt{10} \in M^{(\sigma, \tau)} = \mathbb{Q}$: contradiction.
 - If $\tau(\sqrt{5}) = -\sqrt{5}$, $\tau(\sqrt{30}) = \tau(\sqrt{5})\tau(\sqrt{3})\tau(\sqrt{2}) = \sqrt{30} \in M^{(\sigma, \tau)} = \mathbb{Q}$: contradiction.

- So $\sqrt{5} \notin M$, so $[L : \mathbb{Q}] = [L : M][M : \mathbb{Q}] = 8$. The 8 elements in $\text{Gal}(L/\mathbb{Q})$ are determined by choices of $\sqrt{a} \mapsto \pm\sqrt{a}$ where $a \in \{2, 3, 5\}$.
- $\text{Gal}(L/\mathbb{Q}) = \langle \sigma_1, \sigma_2, \sigma_3 \rangle \cong \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$ where $\sigma_1(\sqrt{2}) = -\sqrt{2}$, $\sigma_2(\sqrt{3}) = -\sqrt{3}$, $\sigma_1(\sqrt{5}) = -\sqrt{5}$ and the σ_i fix all other square roots.
- More generally, write $\sigma(\sqrt{5}) = (-1)^j \sqrt{5}$, $\tau(\sqrt{5}) = (-1)^k \sqrt{5}$, $j, k \in \{0, 1\}$. Define $m = 2^j 3^k$, then $\sigma(\sqrt{m}) = (-1)^j \sqrt{m} \Rightarrow \sigma(\sqrt{5m}) = \sqrt{5m}$ and $\tau(\sqrt{m}) = (-1)^k \sqrt{m} \Rightarrow \tau(\sqrt{5m}) = \sqrt{5m}$, so $\sqrt{5m} \in M^{(\sigma, \tau)} = \mathbb{Q}$: contradiction.
- **Example - cubic extension and its normal closure:**
 - Let $L = \mathbb{Q}(\theta)$, $\theta^3 - 2 = 0$. L/\mathbb{Q} isn't Galois since not normal. Take the normal closure $N = \mathbb{Q}(\theta, \omega) = \mathbb{Q}(\theta, \sqrt{-3})$.
 - Let $M = \mathbb{Q}(\omega)$ so $[M : \mathbb{Q}] = 2$, $[L : \mathbb{Q}] = 3$ and $[N : \mathbb{Q}] = 6$. Let $G = \text{Gal}(N/\mathbb{Q})$.
 - Since $|G| = [N : \mathbb{Q}] = 6$, $G \cong \mathbb{Z}/6$ or $G \cong D_3 \cong S_3$.
 - G contains $\text{Gal}(N/L)$. Since $N = L(\omega)$,

$$\text{Gal}(N/L) = \{\text{id}, \tau\} = \langle \tau \rangle \cong \mathbb{Z}/2$$

where $\tau(\sqrt{-3}) = -\sqrt{-3}$ (i.e. $\tau(\omega) = \omega^2$) and $\tau(\theta) = \theta$ as $\theta \in L$.

- G contains $H = \text{Gal}(N/M)$. $N = M(\theta)$, $|H| = [N : M] = 3$ so $\text{Gal}(N/M)$ is cyclic so

$$H = \{\text{id}, \sigma, \sigma^2\} = \langle \sigma \rangle \cong \mathbb{Z}/3$$

where $\sigma(\theta) = \omega\theta$, also $\sigma(\omega) = \omega$ as $\omega \in M$ and $\sigma^2(\theta) = \omega^2\theta$, so H permutes the three roots of $x^3 - 2$.

- $\tau \notin H$ so $H = \{\text{id}, \sigma, \sigma^2\}$ and $\tau H = \{\tau, \tau\sigma, \tau\sigma^2\}$ are disjoint cosets. So $G = H \cup \tau H = \langle \tau, \sigma \rangle$ so $|G| = 6$. $\tau^2 = \sigma^3 = \text{id}$ and $\sigma\tau = \tau\sigma^2$. So $G \cong S_3 \cong D_3$.
- G has one subgroup of order 3, $H = \langle \sigma \rangle$. Fixed field is $N^H = M$. H is only proper normal subgroup of G . Correspondingly, M is only normal extension of \mathbb{Q} in N .
- There are 3 order 2 subgroups: $\langle \tau \rangle$, $\langle \tau\sigma \rangle$, $\langle \tau\sigma^2 \rangle$. $N^{\langle \tau \rangle} = \mathbb{Q}(\theta) = L$, $N^{\langle \tau\sigma \rangle} = \mathbb{Q}(\omega\theta) = \sigma(L)$, $N^{\langle \tau\sigma^2 \rangle} = \mathbb{Q}(\omega^2\theta) = \sigma^2(L)$.
- **Example:** show $\sqrt[3]{3} \notin \mathbb{Q}(\sqrt[3]{2})$.
 - Assume $\sqrt[3]{3} \in \mathbb{Q}(\sqrt[3]{2})$. Then $\sqrt[3]{3} \in N = \mathbb{Q}(\omega, \sqrt[3]{2})$, the normal closure.
 - As above, let $\sigma \in \text{Gal}(N/\mathbb{Q})$, $\sigma(\sqrt[3]{2}) = \omega\sqrt[3]{2}$ and $N^{\langle \sigma \rangle} = \mathbb{Q}(\omega)$. Also,

$$\sigma(\sqrt[3]{3})^3 = \sigma(3) = 3 \implies \sigma(\sqrt[3]{3}) \in \{\sqrt[3]{3}, \omega\sqrt[3]{3}, \omega^2\sqrt[3]{3}\}$$

- If $\sigma(\sqrt[3]{3}) = \sqrt[3]{3}$, then $\sqrt[3]{3} \in N^{\langle \sigma \rangle} = \mathbb{Q}(\omega)$, so $\mathbb{Q}(\sqrt[3]{3}) \subseteq \mathbb{Q}(\omega)$: contradiction.
- If $\sigma(\sqrt[3]{3}) = \omega\sqrt[3]{3}$, then $\sigma(\sqrt[3]{3}/\sqrt[3]{2}) = \sqrt[3]{3}/\sqrt[3]{2}$ hence $\sqrt[3]{3/2} \in N^{\langle \sigma \rangle} = \mathbb{Q}(\omega)$, so $\mathbb{Q}(\sqrt[3]{3/2}) = \mathbb{Q}(\sqrt[3]{12}) \subseteq \mathbb{Q}(\omega)$: contradiction.
- If $\sigma(\sqrt[3]{3}) = \omega^2\sqrt[3]{3}$, $\mathbb{Q}(\sqrt[3]{3/4}) = \mathbb{Q}(\sqrt[3]{6}) \subseteq \mathbb{Q}(\omega)$: contradiction.
- **Remark:** in the above example, $N = \mathbb{Q}(\theta_1, \theta_2, \theta_3) = \mathbb{Q}(\sqrt[3]{2}, \omega)$ where θ_i are the roots of $x^3 - 2$. Plotting this roots on Argand diagram gives the symmetry group $S_3 \cong D_3$ of an equilateral triangle. τ reflects the θ_i (complex conjugation), σ rotates the roots (but **doesn't** rotate all of N , as it fixes \mathbb{Q}). For $g \in G$, $g(\theta_j) = \theta_{\pi(j)}$ where π is permutation of $\{1, 2, 3\}$. So there is a group

homomorphism $\varphi : G \rightarrow S_3$, $\varphi(g) = \pi$. $\ker(\varphi) = \{\text{id}\}$, so φ is injective and also surjective, since $|G| = |S_3| = 6$, so φ is isomorphism.

- **Definition:** for $f(x) \in K[x]$, $\deg(f) = n \geq 1$, with n distinct roots, the **Galois group** of $f(x)$, G_f , is Galois group of splitting field of $f(x)$ over K (provided it is separable).
- **Remark:** elements of G_f permute roots of f , so G_f is subgroup of S_n . If $f(x)$ irreducible over K , then G_f is **transitive** subgroup, i.e. given 2 roots α, β of f , there is a $g \in G_f$ with $g(\alpha) = \beta$. This gives a general pattern

polynomial \longrightarrow field extension \longrightarrow permutation group

- **Example:** consider $\mathbb{Q} \subset L = \mathbb{Q}(\theta) \subset N = \mathbb{Q}(\theta, i)$ where $\theta = \sqrt[4]{2}$. N is normal closure of $\mathbb{Q}(\theta)$, $[N : \mathbb{Q}] = 8$ so $|\text{Gal}(N/\mathbb{Q})| = 8$.
 - Define $\sigma(\theta) = i\theta$, $\sigma(i) = i$, $\tau(\theta) = \theta$, $\tau(i) = -i$. Then $\tau^2 = \sigma^4 = \text{id}$. We have

	id	σ	σ^2	σ^3	τ	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$
θ	θ	$i\theta$	$-\theta$	$-i\theta$	θ	$-i\theta$	$-\theta$	$i\theta$
i	i	i	i	i	$-i$	$-i$	$-i$	$-i$

so $G = \text{Gal}(N/\mathbb{Q}) = \langle \sigma, \tau : \sigma^4 = \tau^2 = \text{id}, \sigma\tau = \tau\sigma^3 \rangle \cong D_4$.

- Order 2 subgroups are $\langle \tau \rangle$, $\langle \tau\sigma \rangle$, $\langle \tau\sigma^2 \rangle$, $\langle \tau\sigma^3 \rangle$, $\langle \sigma^2 \rangle$.
- Order 4 subgroups are $\langle \sigma^2, \tau \rangle \cong (\mathbb{Z}/2)^2$, $\langle \sigma \rangle \cong \mathbb{Z}/4$, $\langle \sigma^2, \tau\sigma \rangle \cong (\mathbb{Z}/2)^2$.
- Respectively, intermediate field extensions of degree 4 are $\mathbb{Q}(\sqrt[4]{2})$, $\mathbb{Q}(i\sqrt[4]{2})$, $\mathbb{Q}(\sqrt{2}, i)$, $\mathbb{Q}((1-i)\sqrt[4]{2})$, $\mathbb{Q}((1+i)\sqrt[4]{2})$.
- Respectively, intermediate field extensions of degree 2 are $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$, $\mathbb{Q}(i\sqrt{2})$.

5. Cyclotomic field extensions

5.1. Roots of unity

- **Definition:** if L/K is Galois, $\text{Gal}(L/K) \cong \mathbb{Z}/n$, then L is **cyclic extension** of K of degree n .
- **Definition:** $\zeta \in K^*$ is **n -th primitive root of unity** if $\zeta^n = 1$ and $\forall 0 < m < n$, $\zeta^m \neq 1$, i.e. order of ζ in K^* is n .
- **Example:**
 - ζ is primitive 1-st root of unity iff $\zeta = 1$.
 - -1 is primitive 2-nd root of unity iff $\text{char}(K) \neq 2$.
 - If $\text{char}(K) = p$ prime, then K contains no p -th primitive roots of unity (since $\zeta^p = 1 \iff (\zeta - 1)^p = 0 \iff \zeta = 1$).
 - If $K = \mathbb{C}$, $\exp(2\pi i/n)$ is n -th primitive root of unity.
- **Proposition:** let $\zeta \in K^*$ primitive n -th root of unity, let $d = \gcd(m, n)$. Then ζ^m is primitive (n/d) -th root of unity.
- **Corollary:** let $\zeta \in K^*$ primitive n -th root of unity.
 - $\zeta^m = 1 \iff m \equiv 0 \pmod{n}$.
 - ζ^m is primitive n -th root of unity iff $\gcd(m, n) = 1$.

- **Definition:** let $\mu(K)$ denote subgroup of all roots of unity in K^* .
- **Theorem:** let K field, H finite subgroup of K^* , then H is cyclic.
- **Corollary:** let K field, $n \in \mathbb{N}$ be largest such that K contains primitive n -th root of unity ζ . Then $\mu(K)$ is cyclic subgroup in K^* generated by ζ .

5.2. n -th cyclotomic field extensions

- **Notation:** let $\zeta_n = \exp(2\pi i/n) \in \mathbb{C}$.
- **Definition:** $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is **n -th cyclotomic field extension**.
- **Proposition:** $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois.
- **Definition:** $\Phi_n(x) := \prod_{a \in A} (x - \zeta_n^a)$ where $A = \{a \in \mathbb{N} : 0 < a < n, \gcd(a, n) = 1\}$.
- **Proposition:** $\Phi_n(x) \in \mathbb{Q}[x]$ is irreducible and so is minimal polynomial of a primitive n -th root of unity over \mathbb{Q} . In particular, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$, where $\varphi(n) = |(\mathbb{Z}/n)^\times|$ is Euler function.
- **Proposition:** properties of φ function:
 - For prime p , $\varphi(p) = p - 1$.
 - For prime p , $\varphi(p^k) = p^k - p^{k-1}$.
 - If $\gcd(n, m) = 1$, then $\varphi(nm) = \varphi(n)\varphi(m)$.
 - If $n = \prod_{i=1}^r p_i^{k_i}$ is prime factorisation of n , then

$$\varphi(n) = n \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right)$$

- **Proposition:** $\forall n \in \mathbb{N}, x^n - 1 = \prod_{n_1|n} \Phi_{n_1}(x)$.
- **Example:**
 - $\Phi_1(x) = x - 1$.
 - $\Phi_1(x)\Phi_2(x) = x^2 - 1 \implies \Phi_2(x) = x + 1$.
 - $\Phi_1(x)\Phi_3(x) = x^3 - 1 \implies \Phi_3(x) = x^2 + x + 1$.
- **Proposition:**
 - For p prime, $\Phi_p(x) = x^{p-1} + \dots + x + 1$.
 - For p prime, $\Phi_{p^k}(x) = \Phi_p(x^{p^{k-1}})$.
 - For every $n \in \mathbb{N}$, $\Phi_n(x)$ has integer coefficients.

5.3. Galois properties of cyclotomic extensions

- **Theorem:** $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n)^\times$.
- **Corollary:** $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is abelian so every subgroup is normal, so any subfield of $\mathbb{Q}(\zeta_n)$ is Galois over \mathbb{Q} .
- **Corollary:** for p prime, $G = \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p)^\times \cong \mathbb{Z}/(p-1)$. In particular, for $d \mid (p-1)$, $\mathbb{Q}(\zeta_p)$ contains exactly one subfield of degree d and there are no other subfields.
- **Remark:** for $d = 2$ in above corollary, $\mathbb{Q}(\zeta_p)$ contains unique quadratic subfield $\mathbb{Q}(\sqrt{D_p})$. $D_p = p$ if $p \equiv 1 \pmod{4}$ and $D_p = -p$ if $p \equiv 3 \pmod{4}$.
- **Example:** $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ not always cyclic, e.g. $\text{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$.
- **Proposition:**
 - If n odd, $\mu(\mathbb{Q}(\zeta_n))$ is cyclic of order $2n$ and is generated by $-\zeta_n$.
 - If n even, $\mu(\mathbb{Q}(\zeta_n))$ is of order n and is generated by ζ_n .

- If $\gcd(m, n) = 1$, then $\mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta_{mn})$.
- $\forall m, n \in \mathbb{N}$, $\mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta_{\text{lcm}(m, n)})$

5.4. Special properties of $\mathbb{Q}(\zeta_p)$, where $p > 2$ is prime

- **Example:** $\text{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \cong (\mathbb{Z}/5)^\times$ has generator $\tau : \zeta_5 \mapsto \zeta_5^2$. \mathbb{Q} -basis $\{1, \zeta_5, \zeta_5^2, \zeta_5^3\}$ is not invariant under action of τ or any power of τ (since $\tau(\zeta_5^2) = \zeta_5^4$) but $\{\zeta_5, \zeta_5^2, \zeta_5^3, \zeta_5^4\}$ is invariant. The same holds for general $p > 2$ prime. For $\alpha_i \in \mathbb{Q}$, $\alpha_1 \zeta_p + \dots + \alpha_{p-1} \zeta_p^{p-1} \in \mathbb{Q}$ iff $\alpha_1 = \dots = \alpha_{p-1}$.
- **Example:** if $x \in \mathbb{Q}(\zeta_p)$, $[\mathbb{Q}(x) : \mathbb{Q}] = |\{\sigma(x) : \sigma \in \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})\}|$. In particular, if τ is generator of $G = \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ and $x = \alpha_1 \zeta_p + \dots + \alpha_{p-1} \zeta_p^{p-1}$ then set of all conjugates of x is equal to (note not all elements are distinct)

$$\{\tau^a(x) : a \in [p-1]\} = \left\{ \sum_{i=1}^{p-1} \alpha_i \zeta_p^{ai} : a \in [p-1] \right\}$$

- **Example:** let $x = \zeta_5 + \zeta_5^4$, $\tau : \zeta_5 \mapsto \zeta_5^2$ is a generator of $\text{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$. $\tau(x) = \zeta_5^2 + \zeta_5^3 \neq x$ but $\tau^2(x) = x$, so $[\mathbb{Q}(x) : \mathbb{Q}] = 2$, i.e. $\mathbb{Q}(\zeta_5 + \zeta_5^4)$ is unique quadratic subfield in $\mathbb{Q}(\zeta_5)$.
- **Definition:** let $x \in \mathbb{Q}(\zeta_p)$, let minimal polynomial of x over \mathbb{Q} be $m(t) = (t - x^{(1)}) \dots (t - x^{(d)})$. **Conjugates** of x over \mathbb{Q} are $x^{(1)} = x, \dots, x^{(d)}$.
- **Example:** minimal polynomial of $\zeta_5 + \zeta_5^4 = 2 \cos(2\pi/5)$ over \mathbb{Q} is $m(x) = (x - \zeta_5 - \zeta_5^4)(x - \zeta_5^2 - \zeta_5^3) = x^2 + x - 1$, with roots $(-1 \pm \sqrt{5})/2$. So $\cos(2\pi/5) = (-1 + \sqrt{5})/4$, and unique quadratic subfield of $\mathbb{Q}(\zeta_5)$ over \mathbb{Q} is $\mathbb{Q}(\sqrt{5})$.
- **Example:** let $\tau \in G$ be generator of $G = \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, i.e. $\tau(\zeta_p) = \zeta_p^a$, $a \bmod p$ generates $(\mathbb{Z}/p)^\times$. Let

$$\Theta_p = \zeta_p - \tau(\zeta_p) + \tau^2(\zeta_p) - \dots + \tau^{p-3}(\zeta_p) - \tau^{p-2}(\zeta_p)$$

Θ_p behaves like $\sqrt{D_p}$: $\tau(\Theta_p) = -\Theta_p$, $\tau^2(\Theta_p) = \Theta_p$. So $\Theta_p \in \mathbb{Q}(\zeta_p)^{\langle \tau^2 \rangle}$. Also, $\tau(\Theta_p^2) = \Theta_p^2$ so $\Theta_p^2 \in \mathbb{Q}(\zeta_p)^{\langle \tau \rangle} = \mathbb{Q}$. In fact, $\Theta_p^2 = D_p$. Therefore

$$\Theta_p^2 = A + B(\zeta_p + \dots + \zeta_p^{p-1}) = A - B$$

So when computing Θ_p^2 , only need to consider coefficients for 1 and ζ_p .

6. Cyclic field extensions

6.1. Cyclic extensions of degree 2

- **Definition:** L/K is **cyclic of degree 2** if it is Galois and $\text{Gal}(L/K) \cong \mathbb{Z}/2$.
- **Example:** let L/K cyclic of degree 2, so $\text{Gal}(L/K) = \{e, \tau\}$, $\tau^2 = e$. Let $\theta \in L - K$, then $\tau(\theta) \neq \theta$ (as otherwise $\theta \in L^{\langle \tau \rangle} = K$). Let $\theta_1 = \tau(\theta) - \theta$, so $\tau(\theta_1) = \tau^2(\theta) - \tau(\theta) = -\theta_1$. If $\text{char}(K) \neq 2$, then $\theta_1 \neq -\theta_1$ and so $\theta_1 \notin K$, $L = K(\theta_1)$. θ_1 is “better” than θ , since $\tau(\theta_1) = -\theta_1$. Now if $a = \theta_1^2$, then $\tau(a) = a$, so $L = K(\sqrt{a})$.
- **Theorem:** if $\text{char}(K) \neq 2$ and L/K is cyclic quadratic extension, then

$$\exists a \in K^\times - K^{\times^2} : L = K(\sqrt{a})$$

- **Definition:** a_1, \dots, a_n are **independent modulo K^{\times^2}** (independent modulo squares) if

$$a_1^{\varepsilon_1} \dots a_n^{\varepsilon_n} \in K^{\times^2} \iff \text{all } \varepsilon_i \text{ are even}$$

- **Proposition:** if $\text{char}(K) \neq 2$:
 - $K(\sqrt{a_1}) = K(\sqrt{a_2}) \iff a_1 \equiv a_2 \pmod{K^{\times^2}}$, i.e. $a_1 = a_2 \cdot b^2$, $b \in K^\times$.
 - If $a_1, \dots, a_n \in K^\times$ are independent modulo K^{\times^2} then $K(\sqrt{a_1}, \dots, \sqrt{a_n})$ has degree 2^n over K with Galois group $\cong (\mathbb{Z}/2)^n$.
 - If L/K Galois with Galois group $(\mathbb{Z}/2)^n$, then

$$\exists a_1, \dots, a_n \in K^\times : L = K(\sqrt{a_1}, \dots, \sqrt{a_n})$$

- **Remark:** let $\text{char}(K) = 2$, then $\forall a \in K^\times$, $L = K(\sqrt{a})$ is normal but not separable (since minimal polynomial of e.g. \sqrt{a} is $x^2 - a = (x + \sqrt{a})(x - \sqrt{a}) = (x - \sqrt{a})^2$ so has repeated roots).

6.2. Cyclic extensions of degree n (the Kummer theory)

- **Definition:** L/K is **cyclic of degree n** if it is Galois and $\text{Gal}(L/K)$ is cyclic of order n .
- **Theorem:** if K contains primitive n -th root of unity and for all divisors $d > 1$ of n , $a \in K^\times$ is not d -th power in K , then $L = K(\sqrt[n]{a})$ is cyclic extension of K of degree n . In particular, $x^n - a \in K[x]$ is irreducible.
- **Proposition:** if $\zeta_p \in K$, $a \in K^\times - K^{\times p}$, then $K(\sqrt[p]{a})/K$ is cyclic of degree p . In particular, $x^p - a \in K[x]$ is irreducible.
- **Theorem:** let K contain n -th primitive root of unity, L/K is cyclic extension of degree n . Then

$$\exists a \in K^\times : L = K(\sqrt[n]{a})$$

- **Artin's lemma:** there exists $b_0 \in L$ such that $\theta_{b_0} \neq 0$, where

$$\theta_{b_0} = b_0 + \zeta_n^{-1} b_1 + \dots + \zeta_n^{-(n-1)} b_{n-1}$$

is **Lagrange resolvent** for b_0 , and $b_i := \tau^i(b_0)$.

7. Finite fields

7.1. Existence and uniqueness

- **Lemma:** let K finite field, then K is field extension of \mathbb{F}_p for some prime p and $|K| = p^n$ where $n = [K : \mathbb{F}_p]$.
- **Theorem:** let p prime. Then $\forall n \in \mathbb{N}$, there is field K with $|K| = p^n$.
- **Theorem:** let K finite field with $|K| = q = p^n$. Then
 - $\forall \alpha \in K, \alpha^q = \alpha$.
 - $x^q - x = \prod_{\alpha \in K} (x - \alpha)$
 - K is splitting field of $x^q - x$ over \mathbb{F}_p .
- **Corollary:** if K_1, K_2 finite fields, $|K_1| = |K_2|$, then $K_1 \cong K_2$.

- **Definition:** let $q = p^n$, then \mathbb{F}_q is the unique (up to isomorphism) field containing q elements.
- **Definition:** for $q = p^n$, the **Frobenius automorphism** is

$$\sigma : \mathbb{F}_q \rightarrow \mathbb{F}_q, \quad \sigma(\alpha) = \alpha^p$$

which is an \mathbb{F}_p -automorphism by Fermat's little theorem.

- **Theorem:** let $q = p^n$, p prime.
 - $\mathbb{F}_q/\mathbb{F}_p$ is Galois of degree n .
 - Frobenius automorphism generates $\text{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ and there is group isomorphism

$$\text{Gal}(\mathbb{F}_q/\mathbb{F}_p) \leftrightarrow \mathbb{Z}/n, \quad \sigma \leftrightarrow 1 \bmod n$$

7.2. Counting irreducible polynomials over finite fields

- **Notation:** let $\text{Irr}_{\mathbb{F}_p}(m)$ denote set of all irreducible polynomials in $\mathbb{F}_p[x]$ of degree N . Let $N_p(m) = |\text{Irr}_{\mathbb{F}_p}(m)|$.
- **Theorem:** let $q = p^m$, then $mN_p(m) = |\{\alpha \in \mathbb{F}_q : \mathbb{F}_p(\alpha) = \mathbb{F}_q\}|$.