20250702 MATH4302 NOTE 4[1]

Author: Be $\sqrt{-1}$maginative, and nothing will be $\frac{\mathrm{d}}{\mathrm{d}x}$ifficult!
Email: u3612704@connect.hku.hk;
Phone: +852 5693 2134; +86 19921823546;

Contents

1 Introduction

This note collects some basic concepts in Galois theory. Its purposes are:

(1) Relate Galois theory to covering space theory.
Typically, $\mathbb{Q}[\sqrt[3]{3}, \zeta]$ is called a splitting field of $x^3 - 3$ over $\mathbb{Q}$, where $\zeta^3 = 1$. To clarify the connection, I redefined some terms, e.g., $\sigma : \mathbb{Q} \to \mathbb{Q}[\sqrt[3]{3}, \zeta]$ splits $x^3 - 3$ into $\sqrt[3]{3}$, $\sqrt[3]{3}\zeta$, $\sqrt[3]{3}\zeta^2$ universally (see **definition 2.27.** and **definition 2.34.**).

(2) Introduce the resultant for explicit computation.
The resultant generates a polynomial that vanishes at the sum of two algebraic elements (see **proposition 3.6.** and **Wikepedia**[2]). A result in this document (see **proposition 4.15.** and **this journal article**[3]) relates resultant with cyclotomic polynomials, and Dr. Ching extends this further in personal discussion.

(3) Present explicit and standardized Galois correspondences.
Figures in **subsection 3.2.**, **subsection 4.2.**, **subsection 4.3.** and **subsection 4.4.** describe several Galois correspondences with computational details.

I include valuable materials from Prof. Borcherds' online lectures.[4]

2 Splitting Map

2.1 Field

Definition 2.1. (**Field**)
Let K be a set. If:

(1) There is an addition $(k, l) \mapsto k + l$ on K, satisfying:

$$\begin{aligned}
\forall k, l, m \in K, (k + l) + m &= k + (l + m) \\
\forall k, l \in K, \quad k + l &= l + k \\
\exists 0 \in K, \forall k \in K, \quad 0 + k &= k \\
\forall k \in K, \exists -k \in K, \quad (-k) + k &= 0
\end{aligned}$$

(2) There is a multiplication $(k, l) \mapsto kl$ on K, satisfying:

$$\begin{aligned}
\forall k, l, m \in K, \quad (kl)m &= k(lm) \\
\forall k, l \in K, \quad kl &= lk \\
\exists 1 \in K \backslash \{0\}, \forall k \in K, \quad 1k &= k \\
\forall k \in K \backslash \{0\}, \exists k^{-1} \in K, \quad k^{-1}k &= 1 \\
\forall k, l, m \in K, k(l + m) &= kl + km
\end{aligned}$$

Then K is a field.

Proposition 2.2. Let K be a field, and $I \trianglelefteq K$.

$$I = \{0\} \text{ or } I = K$$

Proof. For all $I \trianglelefteq K$, assume that I contains some $k \in K \backslash \{0\}$.
It follows from $1 = k^{-1}k \in I$ that $I = K$. □

Proposition 2.3. Let R be an integral domain,
and G be a finite subgroup of $R^\times$.

$$\exists r \in G, \langle r \rangle = G$$

Proof. According to **the classification theorem of finite Abelian groups**,
for some unique $m \geq 0$, for some unique $d_0 \mid d_1 \mid \cdots \mid d_{m-2} \mid d_{m-1}$ greater than 1:

$$G \cong \frac{\mathbb{Z}}{d_0\mathbb{Z}} \oplus \frac{\mathbb{Z}}{d_1\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{d_{m-2}\mathbb{Z}} \oplus \frac{\mathbb{Z}}{d_{m-1}\mathbb{Z}}$$

Assume to the contrary that $m > 1$, and we obtain a polynomial $x^{d_{m-1}} - 1$ of degree d_{m-1} over an integral domain R with at least $d_0 d_1 \cdots d_{m-2} d_{m-1} > d_{m-1}$ roots. □

Proposition 2.4. Let R be an integral domain.

$$\mathbf{Char}(R) \text{ is prime or } 0$$

Proof. Assume to the contrary that $\mathbf{Char}(R)$ is the product of $m, n > 1$.
It follows from $mn = 0, m, n \neq 0$ in R that R is not an integral domain. □

Definition 2.5. (**Field Homomorphism**)
Let $K, \bar{K}$ be fields, and $\sigma : K \to \bar{K}$ be a map. If:

$$\begin{aligned} \forall k, l \in K, \sigma(k + l) &= \sigma(k) + \sigma(l) \\ \forall k, l \in K, \quad \sigma(kl) &= \sigma(k)\sigma(l) \\ \sigma(1) &= \bar{1} \end{aligned}$$

Then $\sigma \in \mathbf{Hom}(K, \bar{K})$ is a field homomorphism.

Proposition 2.6. Let K be a field, $\bar{K}$ be a ring with unity,
and $\sigma : K \to \bar{K}$ be a ring homomorphism.

$$\mathbf{Ker}(\sigma) = \{0\}$$

Proof. As $\mathbf{Ker}(\sigma) \trianglelefteq K$ and $1 \notin \mathbf{Ker}(\sigma)$, $\mathbf{Ker}(\sigma) = \{0\}$. □

Proposition 2.7. Let K be a field, $\bar{K}$ be a ring with unity, and $\sigma : K \to \bar{K}$ be a ring homomorphim.

$$\sigma \text{ brings a } K\text{-vector space structure to } \bar{K}$$

Proof. We may divide our proof into two parts.

(1) There is an addition $(\bar{k}, \bar{l}) \mapsto \bar{k} + \bar{l}$ on $\bar{K}$, satisfying:

$$\begin{aligned}
\forall \bar{k}, \bar{l}, \bar{m} \in \bar{K}, (\bar{k} + \bar{l}) + \bar{m} &= \bar{k} + (\bar{l} + \bar{m}) \\
\forall \bar{k}, \bar{l} \in \bar{K}, \qquad \bar{k} + \bar{l} &= \bar{l} + \bar{k} \\
\exists \bar{0} \in \bar{K}, \forall \bar{k} \in \bar{K}, \qquad \bar{0} + \bar{k} &= \bar{k} \\
\forall \bar{k} \in \bar{K}, \exists -\bar{k} \in \bar{K}, \quad (-\bar{k}) + \bar{k} &= \bar{0}
\end{aligned}$$

(2) There is a K-scalar multiplication $(k, \bar{l}) \mapsto \sigma(k)\bar{l}$ on $\bar{K}$, satisfying:

$$\begin{aligned}
\forall k, l \in K, \forall \bar{m} \in \bar{K}, \quad (kl) * \bar{m} &= \sigma(kl)m = \sigma(k)\sigma(l)m = k * (l * \bar{m}) \\
\forall \bar{k} \in \bar{K}, \qquad 1 * \bar{k} &= \sigma(1) * \bar{k} = \bar{1}\bar{k} = \bar{k} \\
\forall k, l \in K, \forall \bar{m} \in \bar{K}, (k + l) * \bar{m} &= \sigma(k + l)\bar{m} = \sigma(k)\bar{m} + \sigma(l)\bar{m} = k * \bar{m} + l * \bar{m} \\
\forall k \in K, \forall \bar{l}, \bar{m} \in \bar{K}, k * (\bar{l} + \bar{m}) &= \sigma(k)(\bar{l} + \bar{m}) = \sigma(k)\bar{l} + \sigma(k)\bar{m} = k * \bar{l} + k * \bar{m}
\end{aligned}$$

□

Proposition 2.8. (**Tower Theorem**)
Let K, L be fields, M be a ring with unity, and $\sigma : K \to L, \tau : L \to M$ be ring homomorphisms. Equip L, M with the vector space structures by $\sigma, \tau, \tau \circ \sigma$.

$$\left.\begin{array}{c} L \text{ has a } K\text{-basis } (l_\lambda)_{\lambda \in I} \\ M \text{ has a } L\text{-basis } (m_\mu)_{\mu \in I} \end{array}\right\} \implies M \text{ has a } K\text{-basis } (l_\lambda * m_\mu)_{\lambda \in I, \mu \in J}$$

Proof. We may divide our proof into two parts.

(1) We prove that $(l_\lambda * m_\mu)_{\lambda \in I, \mu \in J}$ K-spans M:

$$\begin{aligned}
\overbrace{\gamma}^{\text{in } M} = \overbrace{\beta_\mu}^{\text{in } L} * m_\mu &= (\overbrace{\alpha_{\lambda,\mu}}^{\text{in } K} * l_\lambda) * m_\mu = \tau(\sigma(\alpha_{\lambda,\mu}) l_\lambda) m_\mu \\
&= \tau(\sigma(\alpha_{\lambda,\mu}))\tau(l_\lambda) m_\mu = \overbrace{\alpha_{\lambda,\mu}}^{\text{in } K} * (l_\lambda * m_\mu)
\end{aligned}$$

(2) We prove that $(l_\lambda * m_\mu)_{\lambda\in I,\mu\in J}$ is K-linearly independent:

$$\begin{aligned}\overbrace{\alpha_{\lambda,\mu}}^{\text{in } K} * (l_\lambda * m_\mu) = 0 &\implies \overbrace{(\alpha_{\lambda,\mu} * l_\lambda)}^{\text{in } L} * m_\mu = 0 \\ &\implies \overbrace{\alpha_{\lambda,\mu}}^{\text{in } K} * l_\lambda = 0 \implies \alpha_{\lambda,\mu} = 0\end{aligned}$$

□

Proposition 2.9. (**The Freshman's Dream**)
Let R be a commutative ring with unity.
If **Char**(R) is a prime number p, then for all $r, s \in R$, $(r+s)^p = r^p + s^p$.

Proof. For all $0 < k < p$:

$$\binom{p}{k} = \frac{(p)(p-1)\cdots(p-k+2)(p-k+1)}{(k)(k-1)\cdots(2)(1)} = 0 \text{ in } R$$

Hence:

$$(r+s)^p = \binom{p}{0} r^p + \binom{p}{1} r^{p-1}s + \cdots + \binom{p}{p-1} rs^{p-1} + \binom{p}{p} s^p = r^p + s^p \text{ in } R$$

□

Proposition 2.10. (**Frobenius Endomorphism**)
Let R be a commutative ring with unity.
If **Char**(R) is a prime number p, then $\sigma : R \to R, r \mapsto r^p$ is a ring endomorphism.

Proof.

$$\begin{aligned}\forall r, s \in R, \sigma(r+s) &= (r+s)^p = r^p + s^p = \sigma(r) + \sigma(s) \\ \forall r, s \in R, \quad \sigma(rs) &= (rs)^p = r^p s^p = \sigma(r)\sigma(s) \\ \sigma(1) &= 1^p = 1\end{aligned}$$

□

Remark: If R is an integral domain, then σ is injective.
If R is a finite field, then σ is bijective, thus an automorphism.
We will return to this in **subsection 4.1.**.

Definition 2.11. (**Prime Homomorphism**)
Let K be a field.

(1) If $\mathbf{Char}(K) = 0$,
then define $\sigma : \mathbb{Q} \to K, \frac{p}{q} \mapsto \frac{p}{q}$ as the prime homomorphism of K.

(2) If $\mathbf{Char}(K)$ is a prime number p,
then define $\sigma : \mathbb{Z}/p\mathbb{Z} \to K, \bar{q} \mapsto q$ as the prime homomorphism of K.

Example 2.12. (**The Universal Property of Prime Homomorphism**)
Let $K, \bar{K}$ be fields, and $\sigma : K \to \bar{K}, \tau : L \to K, \bar{\tau} : L \to \bar{K}$ be field homomorphisms with $\sigma \circ \tau = \bar{\tau}$. τ is prime iff $\bar{\tau}$ is prime.

$$\begin{tikzcd}
 & \bar{K} \\
L \arrow[ru, "\bar{\tau}"] \arrow[r, "\tau"'] & K \arrow[u, "\sigma"']
\end{tikzcd}$$

Proposition 2.13. Let K be a finite field.
For some prime integer p, for some positive integer n, $|K| = p^n$.

Proof. On one hand, $\mathbf{Char}(K)$ is a prime number p.
On the other hand, the $\mathbb{Z}/p\mathbb{Z}$-dimension of K is a positive integer n. □

Proposition 2.14. Let R be an integral domain.

$$(r_0, s_0) \sim (r_1, s_1) \text{ if } r_0 s_1 = s_0 r_1 \text{ is an equivalence relation on } R \times (R \backslash \{0\})$$

Proof.

$$\begin{aligned}
rs = sr &\implies (r, s) \sim (r, s) \\
(r_0, s_0) \sim (r_1, s_1) &\implies r_0 s_1 = s_0 r_1 \\
&\implies r_1 s_0 = s_1 r_0 \implies (r_1, s_1) \sim (r_0, s_0) \\
(r_0, s_0) \sim (r_1, s_1), (r_1, s_1) \sim (r_2, s_2) &\implies r_0 s_1 = s_0 r_1, r_1 s_2 = s_1 r_2 \\
&\implies r_0 s_1 s_2 = s_0 r_1 s_2 = s_0 s_1 r_2 \\
&\implies r_0 s_2 = s_0 r_2 \implies (r_0, s_0) \sim (r_2, s_2)
\end{aligned}$$

□

Definition 2.15. (**Fraction**)
Let R be an integral domain, and $r \in R, s \in R \backslash \{0\}$.
The equivalence class $\frac{r}{s} \in \mathbf{Frac}(R)$ of (r, s) is a fraction.

Proposition 2.16. Let R be an integral domain, and $K = \mathbf{Frac}(R)$.

R brings a field structure to K

Proof. We may divide our proof into two parts.

(1) The map $(\frac{r_0}{s_0}, \frac{r_1}{s_1}) \mapsto \frac{r_0 s_1 + s_0 r_1}{s_0 s_1}$ is well-defined:

$$\begin{aligned}
\frac{r_0}{s_0} = \frac{r_1}{s_1}, \frac{r_2}{s_2} = \frac{r_3}{s_3} &\implies r_0 s_1 = s_0 r_1, r_2 s_3 = s_2 r_3 \\
&\implies (r_0 s_2 + s_0 r_2) s_1 s_3 = (r_1 s_3 + s_1 r_3) s_0 s_2 \\
&\implies \frac{r_0 s_2 + s_0 r_2}{s_0 s_2} = \frac{r_1 s_3 + s_1 r_3}{s_1 s_3}
\end{aligned}$$

(2) The map $(\frac{r_0}{s_0}, \frac{r_1}{s_1}) \mapsto \frac{r_0 s_1 + s_0 r_1}{s_0 s_1}$ is an addition:

$$\begin{aligned}
\forall \frac{r_0}{s_0}, \frac{r_1}{s_1}, \frac{r_2}{s_2} \in K, &\left(\frac{r_0}{s_0} + \frac{r_1}{s_1}\right) + \frac{r_2}{s_2} = \frac{r_0 s_1 s_2 + s_0 r_1 s_2 + s_0 s_1 r_2}{s_0 s_1 s_2} = \frac{r_0}{s_0} + \left(\frac{r_1}{s_1} + \frac{r_2}{s_2}\right) \\
\forall \frac{r_0}{s_0}, \frac{r_1}{s_1} \in K, &\quad \frac{r_0}{s_0} + \frac{r_1}{s_1} = \frac{r_0 s_1 + s_0 r_1}{s_0 s_1} = \frac{r_1 s_0 + s_1 r_0}{s_1 s_0} = \frac{r_1}{s_1} + \frac{r_0}{s_0} \\
\exists \frac{0}{1} \in K, \forall \frac{r}{s} \in K, &\quad \frac{0}{1} + \frac{r}{s} = \frac{0s + 1r}{1s} = \frac{r}{s} \\
\forall \frac{r}{s} \in K, \exists \frac{-r}{s} \in K, &\quad \frac{-r}{s} + \frac{r}{s} = \frac{(-r)s + sr}{ss} = \frac{0}{1}
\end{aligned}$$

(3) The map $(\frac{r_0}{s_0}, \frac{r_1}{s_1}) \mapsto \frac{r_0 r_1}{s_0 s_1}$ is well-defined:

$$\begin{aligned}
\frac{r_0}{s_0} = \frac{r_1}{s_1}, \frac{r_2}{s_2} = \frac{r_3}{s_3} &\implies r_0 s_1 = s_0 r_1, r_2 s_3 = s_2 r_3 \\
&\implies r_0 r_2 s_1 s_3 = s_0 s_2 r_1 r_3 \implies \frac{r_0 r_2}{s_0 s_2} = \frac{r_1 r_3}{s_1 s_3}
\end{aligned}$$

(4) The map $(\frac{r_0}{s_0}, \frac{r_1}{s_1}) \mapsto \frac{r_0 r_1}{s_0 s_1}$ is a multiplication:

$$\begin{aligned}
\forall \frac{r_0}{s_0}, \frac{r_1}{s_1}, \frac{r_2}{s_2} \in K, &\quad \left(\frac{r_0}{s_0} \frac{r_1}{s_1}\right) \frac{r_2}{s_2} = \frac{r_0 r_1 r_2}{s_0 s_1 s_2} = \frac{r_0}{s_0} \left(\frac{r_1}{s_1} \frac{r_2}{s_2}\right) \\
\forall \frac{r_0}{s_0}, \frac{r_1}{s_1} \in K, &\quad \frac{r_0}{s_0} \frac{r_1}{s_1} = \frac{r_0 r_1}{s_0 s_1} = \frac{r_1 r_0}{s_1 s_0} = \frac{r_1}{s_1} \frac{r_0}{s_0} \\
\exists \frac{1}{1} \in K \setminus \left\{\frac{0}{1}\right\}, \forall \frac{r}{s} \in K, &\quad \frac{1}{1} \frac{r}{s} = \frac{1r}{1s} = \frac{r}{s} \\
\forall \frac{r}{s} \in K \setminus \left\{\frac{0}{1}\right\}, \exists \frac{s}{r} \in K, &\quad \frac{s}{r} \frac{r}{s} = \frac{1}{1} \\
\forall \frac{r_0}{s_0}, \frac{r_1}{s_1}, \frac{r_2}{s_2} \in K, &\frac{r_0}{s_0} \left(\frac{r_1}{s_1} + \frac{r_2}{s_2}\right) = \frac{r_0 r_1 s_2 + r_0 s_1 r_2}{s_0 s_1 s_2} = \frac{r_0}{s_0} \frac{r_1}{s_1} + \frac{r_0}{s_0} \frac{r_2}{s_2}
\end{aligned}$$

□

Proposition 2.17.

$$\mathrm{e}^x = \sum_{i=0}^{+\infty} \frac{x^i}{i!} \notin \mathbb{Z}(\!(x)\!)$$

Proof. Assume to the contrary that:

$$\exists \sum_{i=0}^{+\infty} a_i x^i \in \mathbb{Z}[\![x]\!], \exists \sum_{i=0}^{+\infty} b_i x^i \in \mathbb{Z}[\![x]\!]\backslash\{0\}, \sum_{i=0}^{+\infty} a_i x^i = \sum_{i=0}^{+\infty} b_i x^i \sum_{i=0}^{+\infty} \frac{x^i}{i!}$$

As $\sum_{i=0}^{+\infty} b_i x^i \in \mathbb{Z}[\![x]\!]\backslash\{0\}$, there exists a unique $b_j \in \mathbb{Z}\backslash\{0\}$ with minimal $j \geq 0$. The coefficient $a_{|b_j|+j+1}$ gives a contradiction:

$$\begin{aligned} a_{|b_j|+j+1} &= \frac{b_{|b_j|+j+1}}{0!} + \cdots + \frac{b_{j+1}}{|b_j|!} + \frac{b_j}{(|b_j|+1)!} \\ \frac{b_j}{|b_j|+1} &= |b_j|! \left[a_{|b_j|+j+1} - \frac{b_{|b_j|+j+1}}{0!} - \cdots - \frac{b_{j+1}}{|b_j|!} \right] \in \mathbb{Z} \end{aligned}$$

□

Remark: Recall that:

(1) If R is a commutative ring with unity, then the ring of polynomials $R[x_0, \cdots, x_{m-1}]$ collects all finite sum $r_{i_0,\cdots,i_{m-1}} x_0^{i_0} \cdots x_{m-1}^{i_{m-1}}$, where we follow Einstein's summation convention and omit $\sum$. If R is an integral domain, then $R[x_0, \cdots, x_{m-1}]$ is an integral domain. If R is a unique factorization domain, then $R[x_0, \cdots, x_{m-1}]$ is a unique factorization domain. If R is Noetherian, then $R[x_0, \cdots, x_{m-1}]$ is Noetherian. If R is a field, then $R[x]$ is a Euclidean domain.

(2) If R is a commutative ring with unity, then the ring of formal Maclaurin series $R[\![x_0, \cdots, x_{m-1}]\!]$ collects all infinite sum $r_{i_0,\cdots,i_{m-1}} x_0^{i_0} \cdots x_{m-1}^{i_{m-1}}$. If R is a field, then $R[\![x]\!]$ is a Euclidean domain with a unique maximal ideal $\langle x \rangle$.

(3) If $R, \bar{R}$ are commutative rings with unity, $\sigma : R \to \bar{R}$ is a ring homomorphism, and $\bar{r}_0, \cdots, \bar{r}_{m-1} \in \bar{R}$, then the subring of polynomials $R[\bar{r}_0, \cdots, \bar{r}_{m-1}]$ of $\bar{R}$ collects all finite sum $\sigma(r_{i_0,\cdots,i_{m-1}}) \bar{r}_0^{i_0} \cdots \bar{r}_{m-1}^{i_{m-1}}$.

(4) If R is an integral domain, then the field of rational functions $R(x_0, \cdots, x_{m-1}) = \mathbf{Frac}(R[x_0, \cdots, x_{m-1}])$ collects all fraction of finite sum $\frac{r_{i_0,\cdots,i_{m-1}} x_0^{i_0} \cdots x_{m-1}^{i_{m-1}}}{s_{j_0,\cdots,j_{m-1}} x_0^{j_0} \cdots x_{m-1}^{j_{m-1}}}$.

(5) For univariable case, if R is an integral domain, then the field of formal Laurent series $R(\!(x)\!) = \mathbf{Frac}(R[\![x]\!])$ collects all fraction of infinite sum $\frac{r_i x^i}{s_j x^j}$. For the multivariable case, the notation for $\mathbf{Frac}(R[\![x]\!])$ is out of scope.

(6) If $R, \bar{R}$ are integral domains, $\sigma : R \to \bar{R}$ is a ring homomorphism, and $\bar{r}_0, \cdots, \bar{r}_{m-1} \in \bar{R}$, then the subfield of rational functions $R(\bar{r}_0, \cdots, \bar{r}_{m-1}) = \mathbf{Frac}(R[\bar{r}_0, \cdots, \bar{r}_{m-1}])$ of $\mathbf{Frac}(\bar{R})$ collects all fraction of finite sum $\frac{\sigma(r_{i_0,\cdots,i_{m-1}}) \bar{r}_0^{i_0} \cdots \bar{r}_{m-1}^{i_{m-1}}}{\sigma(s_{j_0,\cdots,j_{m-1}}) \bar{r}_0^{j_0} \cdots \bar{r}_{m-1}^{j_{m-1}}}$.

Let R be an integral domain, and $K = \mathbf{Frac}(R)$. $R(x)$ is obviously isomorphic to $K(x)$. Our argument shows that $R(\!(x)\!)$ may be a proper subfield of $K(\!(x)\!)$.

Example 2.18. (**The Universal Property of Field of Fractions**)
Let R be an integral domain, and K be a field.
For some ring homomorphism:

$$\iota : R \to \mathbf{Frac}(R), r \mapsto r$$

For all ring homomorphism:

$$\sigma : R \to K$$

For some unique field homomorphism:

$$\mathbf{Frac}(\sigma) : \mathbf{Frac}(R) \to K, \frac{r}{s} \mapsto \frac{\sigma(r)}{\sigma(s)}$$

The diagram below commutes:

$$\begin{tikzcd}
R \arrow[r, "\iota"] \arrow[dr, "\sigma"'] & \mathbf{Frac}(R) \arrow[d, "\mathbf{Frac}(\sigma)"] \\
 & K
\end{tikzcd}$$

Proposition 2.19. Let R be a commutative ring with unity, and $P \trianglelefteq R$.

$$\begin{tikzcd}
P \text{ is maximal} \arrow[r, Leftrightarrow] \arrow[d, Rightarrow] & R/P \text{ is a field} \arrow[d, Rightarrow] \\
P \text{ is prime} \arrow[r, Leftrightarrow] & R/P \text{ is an integral domain}
\end{tikzcd}$$

Proof. We may divide our proof into three parts.

(1) We prove that P is maximal iff R/P is a field.
On one hand, $P \neq R$ iff $R/P \neq \{P\}$.
On the other hand, for all $r \in R \backslash P$, $\langle r \rangle + P = R$ iff $r + P$ is a unit of R/P.

(2) We prove that P is prime iff R/P is an integral domain.
On one hand, $P \neq R$ iff $R/P \neq \{P\}$.
On the other hand, for all $r, s \in R \backslash P$, $rs \in R \backslash P$ iff $rs + P$ is nonzero in R/P.

(3) We prove that K is a field implies K is an integral domain.
On one hand, $K \neq \{0\}$ implies $K \neq \{0\}$.
On the other hand, for all $k \in K \backslash \{0\}$, k is a unit implies k is not a zero divisor.

□

Example 2.20.

(1) $\langle x \rangle \trianglelefteq \mathbb{Z}[x]$ is not maximal and prime.

(2) $\langle x^2 \rangle \trianglelefteq \mathbb{Z}[x]$ is not maximal and not prime.

Proposition 2.21. Let K be a commutative ring with unity.

$$K \text{ is a finite integral domain} \implies K \text{ is a field}$$

Proof. For all $k \in K\backslash\{0\}$, $\ell_k : K\backslash\{0\} \to K\backslash\{0\}, l \mapsto kl$ is well-defined and injective. As $K\backslash\{0\}$ is a finite set containing 1, $k^{-1} = \ell_k^{-1}(1)$ exists. □

Proposition 2.22. Let R be a commutative ring with unity, and $P \trianglelefteq R$.

$$P \text{ is nonzero, principal and prime} \iff P \text{ is generated by a prime element}$$

Proof. Assume that P is generated by a not necessarily prime element $p \in R$. $P \neq \{0\}$ iff p is nonzero, $P \neq R$ iff p is not a unit, and for all $r, s \in R$:

$$\begin{tikzcd}
P \ni rs \arrow[r, Leftrightarrow] \arrow[d, Rightarrow] & p \mid rs \arrow[d, Rightarrow] \\
P \ni r \text{ or } P \ni s \arrow[r, Leftrightarrow] & p \mid r \text{ or } p \mid s
\end{tikzcd}$$

□

Proposition 2.23. Let R be a commutative ring with unity, and $p \in R$.

$$p \text{ is prime and not a zero divisor} \implies p \text{ is irreducible}$$

Proof. p is nonzero and nonunit, and for all $r, s \in R$, $p = rs$ implies $p \mid rs$. WLOG, assume that $p \mid r$. As p is not a zero divisor, we may cancel p, so $\frac{r}{p}s = 1$, s is a unit. □

Example 2.24.

(1) $4 \in \mathbb{Z}$ is not prime, not a zero divisor, and reducible.

(2) $\bar{2} \in \mathbb{Z}/\langle 6 \rangle$ is prime, a zero divisor, and reducible.

(3) $\bar{4} \in \mathbb{Z}/\langle 8 \rangle$ is not prime, a zero divisor, and reducible.

(4) $\bar{2} \in \mathbb{Z}[x]/\langle x^2 \rangle$ is not prime, not a zero divisor, and irreducible.

(5) $\bar{x} \in \mathbb{Z}[x]/\langle x^2 \rangle$ is prime, a zero divisor, and irreducible.

(6) $\bar{2} \in \mathbb{Z}[x]/\langle 4, x^2 \rangle$ is not prime, a zero divisor, and irreducible.

Proposition 2.25. Let R be a commutative ring with unity, and $p \in R$.

$$p \text{ is irreducible } \implies \langle p \rangle \text{ is maximal among proper principal ideals}$$

Proof. For all $r \in R$:

$$\langle r \rangle \supseteq \langle p \rangle \implies r \mid p \implies r \sim p \text{ or } r \sim 1 \implies \langle r \rangle = \langle p \rangle \text{ or } \langle r \rangle = R$$

□

Example 2.26. Let R be a principal ideal domain, and $P \trianglelefteq R$. TFAE:

(1) P is nonzero and maximal.

(2) P is nonzero and R/P is a field.

(3) P is nonzero and prime.

(4) P is nonzero and R/P is an integral domain.

(5) P is generated by a prime element.

(6) P is generated by an irreducible element.

Remark: As a consequence, if $K, \bar{K}$ are fields, $\sigma : K \to \bar{K}$ is a field homomorphism, and $\bar{\kappa} \in \bar{K}$ has a minimal polynomial $k(x)$ over K, then $\langle k(t) \rangle$ is maximal in $K[t]$, and $K[\bar{\kappa}] = K(\bar{\kappa}) \cong K[t]/\langle k(t) \rangle$ is a field.

2.2 Definition and Example

Definition 2.27. (**Splitting Map**)
Let $K, \bar{K}$ be fields, $k_m x^m + \cdots + k_0 \in K[x]$, $\bar{k}_m x^m + \cdots + \bar{k}_0 \in \bar{K}[x]$, and $\sigma : K \to \bar{K}$ be a field homomorphism sending the coefficients of $k_m x^m + \cdots + k_0$ to the coefficients of $\bar{k}_m x^m + \cdots + \bar{k}_0$. If for some $\bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1} \in \bar{K}$, $\bar{k}_m x^m + \cdots + \bar{k}_0 = \bar{k}_m (x - \bar{\kappa}_0) \cdots (x - \bar{\kappa}_{m-1})$, then σ splits $k_m x^m + \cdots + k_0$ into $\bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1}$.

Remark: Splitting map is a special field homomorphism. If we view $k_m x^m + \cdots + k_0$ as a base point in K, then $\bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1}$ are the corresponding base points in $\bar{K}$. If we view Galois homomorphism as a Galois covering map, then we shall define deck transformation group correspondingly. Indeed, the two categories are isomorphic. However, this note will omit this category part, only focusing on the basics of Galois theory.

Definition 2.28. (**Splitting Map Homomorphism**)
Let $K, \bar{K}, L, \bar{L}$ be fields, $k_m x^m + \cdots + k_0 \in K[x], \bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1} \in \bar{K}, l_m x^m + \cdots + l_0 \in L[x], \bar{\ell}_0, \cdots, \bar{\ell}_{m-1} \in \bar{L}$, $f : K \to L$ be a field homomorphism sending the coefficients of $k_m x^m + \cdots + k_0$ to the coefficients of $l_m x^m + \cdots + l_0$, $\bar{f} : \bar{K} \to \bar{L}$ be a field homomorphism sending $\bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1}$ to $\bar{\ell}_0, \cdots, \bar{\ell}_{m-1}$, $\sigma : K \to \bar{K}$ split $k_m x^m + \cdots + k_0$ into $\bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1}$, and $\tau : L \to \bar{L}$ split $l_m x^m + \cdots + l_0$ into $\bar{\ell}_0, \cdots, \bar{\ell}_{m-1}$. If the diagram below commutes:

$$\begin{tikzcd}
(\bar{K}, \bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1}) \arrow[r, "\bar{f}"] & (\bar{L}, \bar{\ell}_0, \cdots, \bar{\ell}_{m-1}) \\
(K, k_m x^m + \cdots + k_0) \arrow[u, "\sigma"] \arrow[r, "f"'] & (L, l_m x^m + \cdots + l_0) \arrow[u, "\tau"']
\end{tikzcd}$$

Then $(f, \bar{f}) \in \mathbf{Hom}(\sigma, \tau)$ is a splitting map homomorphism.

Remark: We will introduce deck transformation group $\mathbf{Deck}(\sigma)$ later. Isomorphic σ, τ induce isomorphic $\mathbf{Deck}(\sigma), \mathbf{Deck}(\tau)$, and we will have a simple way to compute $\mathbf{Deck}(\sigma)$ when σ is induced by a finite subgroup G of $\mathbf{Aut}(\bar{K})$.

Example 2.29. $\bar{K}/K$ splits $k(x)$ into $\bar{\kappa}_0, \bar{\kappa}_1, \bar{\kappa}_2$, where:

$$\zeta = \mathrm{e}^{\frac{2\pi \mathrm{i}}{3}}$$
$$\bar{K}/K = \mathbb{Q}[\bar{\kappa}_0, \zeta]/\mathbb{Q}$$
$$k(x) = x^3 - 3$$
$$\bar{\kappa}_0, \bar{\kappa}_1, \bar{\kappa}_2 = 3^{\frac{1}{3}}, 3^{\frac{1}{3}}\zeta, 3^{\frac{1}{3}}\zeta^2$$

Remark: We will show that $\mathbf{Deck}(\mathbb{Q}[\bar{\kappa}_0, \bar{\kappa}_1, \bar{\kappa}_2]/\mathbb{Q}) = \mathbf{Sym}(\bar{\kappa}_0, \bar{\kappa}_1, \bar{\kappa}_2)$.

Example 2.30. $\bar{K}/K$ splits $l(x)$ into $\bar{\ell}_0, \bar{\ell}_1, \bar{\ell}_2, \bar{\ell}_3$, where:

$$\bar{K}/K = \mathbb{Q}[\bar{\ell}_0, \mathrm{i}]/\mathbb{Q}$$
$$l(x) = x^4 - 3$$
$$\bar{\ell}_0, \bar{\ell}_1, \bar{\ell}_2, \bar{\ell}_3 = 3^{\frac{1}{4}}, 3^{\frac{1}{4}}\mathrm{i}, -3^{\frac{1}{4}}, -3^{\frac{1}{4}}\mathrm{i}$$

Remark: We will show that $\mathbf{Deck}(\mathbb{Q}[\bar{\ell}_0, \bar{\ell}_1, \bar{\ell}_2, \bar{\ell}_3]/\mathbb{Q}) = \mathbf{Dih}\begin{pmatrix} \bar{\ell}_3 & \bar{\ell}_2 \\ \bar{\ell}_0 & \bar{\ell}_1 \end{pmatrix}$.

Example 2.31. $\bar{K}/K$ splits $k(x)$ into $\bar{\kappa}_0, \bar{\kappa}_1, \bar{\kappa}_2, \bar{\kappa}_3, \bar{\kappa}_4, \bar{\kappa}_5$, where:

$$\begin{aligned}
\zeta &= \mathrm{e}^{\frac{2\pi \mathrm{i}}{7}} \\
\bar{K}/K &= \mathbb{Q}[\bar{\kappa}_0, \bar{\kappa}_1, \bar{\kappa}_2, \bar{\kappa}_3, \bar{\kappa}_4, \bar{\kappa}_5]/\mathbb{Q} = \mathbb{Q}[\bar{\kappa}_0]/\mathbb{Q} \\
k(x) &= \frac{x^7 - 1}{x - 1} \\
\bar{\kappa}_0, \bar{\kappa}_1, \bar{\kappa}_2, \bar{\kappa}_3, \bar{\kappa}_4, \bar{\kappa}_5 &= \zeta, \zeta^3, \zeta^2, \zeta^6, \zeta^4, \zeta^5
\end{aligned}$$

Remark: We will show that $\mathbf{Deck}(\mathbb{Q}[\bar{\kappa}_0, \bar{\kappa}_1, \bar{\kappa}_2, \bar{\kappa}_3, \bar{\kappa}_4, \bar{\kappa}_5]/\mathbb{Q}) = \langle(\bar{\kappa}_0, \bar{\kappa}_1, \bar{\kappa}_2, \bar{\kappa}_3, \bar{\kappa}_4, \bar{\kappa}_5)\rangle$.

Example 2.32. $\bar{K}/K$ splits $k(x), l(x)$ into $\bar{\kappa}_0, \bar{\kappa}_1, \bar{\kappa}_2, \bar{\ell}_0, \bar{\ell}_1, \bar{\ell}_2, \bar{\ell}_3$, where:

$$\begin{aligned}
\zeta &= \mathrm{e}^{\frac{2\pi \mathrm{i}}{7}} \\
\bar{K}/K &= \mathbb{Q}[\bar{\kappa}_0, \bar{\kappa}_1, \bar{\kappa}_2]/\mathbb{Q} = \mathbb{Q}[\bar{\ell}_0, \bar{\ell}_1, \bar{\ell}_2, \bar{\ell}_3]/\mathbb{Q} \\
k(x) &= x^6 + x^4 - 2x^2 - 1 \\
\bar{\kappa}_0, \bar{\kappa}_1, \bar{\kappa}_2 &= \sqrt{\zeta + \zeta^6}, \sqrt{\zeta^2 + \zeta^5}, \sqrt{\zeta^4 + \zeta^3} \text{ with } \mathbf{Im}(\bar{\kappa}_0, \bar{\kappa}_1, \bar{\kappa}_2) \geq 0 \\
l(x) &= x^4 + 2x^2 + 8x + 9 \\
\bar{\ell}_0, \bar{\ell}_1, \bar{\ell}_2, \bar{\ell}_3 &= +\bar{\kappa}_0 + \bar{\kappa}_1 + \bar{\kappa}_2, -\bar{\kappa}_0 - \bar{\kappa}_1 + \bar{\kappa}_2, -\bar{\kappa}_0 + \bar{\kappa}_1 - \bar{\kappa}_2, +\bar{\kappa}_0 - \bar{\kappa}_1 - \bar{\kappa}_2
\end{aligned}$$

Remark: We will show that $\mathbf{Deck}(\mathbb{Q}[\bar{\ell}_0, \bar{\ell}_1, \bar{\ell}_2, \bar{\ell}_3]/\mathbb{Q}) = \mathbf{Alt}(\bar{\ell}_0, \bar{\ell}_1, \bar{\ell}_2, \bar{\ell}_3)$.

Example 2.33. $\bar{K}/K$ splits $k(x), l(x)$ into $\bar{\kappa}_0, \bar{\kappa}_1, \bar{\kappa}_2, \bar{\ell}_0, \bar{\ell}_1, \bar{\ell}_2, \bar{\ell}_3$, where:

$$\begin{aligned}
\zeta &= \mathrm{e}^{\frac{2\pi \mathrm{i}}{3}} \\
\bar{K}/K &= \mathbb{Q}[\bar{\kappa}_0, \bar{\kappa}_1, \bar{\kappa}_2]/\mathbb{Q} = \mathbb{Q}[\bar{\ell}_0, \bar{\ell}_1, \bar{\ell}_2, \bar{\ell}_3]/\mathbb{Q} \\
k(x) &= x^6 - 81x^2 - 324 \\
\bar{\kappa}_0, \bar{\kappa}_1, \bar{\kappa}_2 &= \sqrt{3^{\frac{4}{3}} + 3^{\frac{5}{3}}}, \sqrt{3^{\frac{4}{3}}\zeta + 3^{\frac{5}{3}}\zeta^2}, \sqrt{3^{\frac{4}{3}}\zeta^2 + 3^{\frac{5}{3}}\zeta} \text{ with } \mathbf{Re}(\bar{\kappa}_0, \bar{\kappa}_1, \bar{\kappa}_2) \geq 0 \\
l(x) &= x^4 - 144x + 324 \\
\bar{\ell}_0, \bar{\ell}_1, \bar{\ell}_2, \bar{\ell}_3 &= +\bar{\kappa}_0 + \bar{\kappa}_1 + \bar{\kappa}_2, -\bar{\kappa}_0 - \bar{\kappa}_1 + \bar{\kappa}_2, -\bar{\kappa}_0 + \bar{\kappa}_1 - \bar{\kappa}_2, +\bar{\kappa}_0 - \bar{\kappa}_1 - \bar{\kappa}_2
\end{aligned}$$

Remark: We will show that $\mathbf{Deck}(\mathbb{Q}[\bar{\ell}_0, \bar{\ell}_1, \bar{\ell}_2, \bar{\ell}_3]/\mathbb{Q}) = \mathbf{Sym}(\bar{\ell}_0, \bar{\ell}_1, \bar{\ell}_2, \bar{\ell}_3)$.

2.3 Universal Splitting Map

Definition 2.34. (**Universal Splitting Map**)
Let $K, \bar{K}$ be fields, $k_m x^m + \cdots + k_0 \in K[x]$, $\bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1} \in \bar{K}$, and $\sigma : K \to \bar{K}$ splits $k_m x^m + \cdots + k_0$ into $\bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1}$. If $\bar{K} = K[\bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1}]$, then σ splits $k_m x^m + \cdots + k_0$ into $\bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1}$ universally.

Proposition 2.35. (**The Existence of Universal Splitting Map**)
Let K be a field, and $k_m x^m + \cdots + k_0 \in K[x]$ with $m \geq 1, k_m \neq 0$. For some field $\bar{K}$, for some $\bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1} \in \bar{K}$, for some field homomorphism $\sigma : K \to \bar{K}$, σ splits $k_m x^m + \cdots + k_0$ into $\bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1}$ universally.

Proof. We prove by inducition on the degree m of $k_m x^m + \cdots + k_0$.
Basis Step: When $m = 1$, for some field $\bar{K} = K$, for some $\bar{\kappa}_0 = -\frac{k_0}{k_1} \in \bar{K}$, for some field homomorphism $\sigma = id_K$, σ splits $k_1 x + k_0$ into $\bar{\kappa}_0$ universally.
Inductive Hypothesis: For all $s \geq 1$, when $m = s$, assume the statement.
Inductive Step: When $m = s + 1$, we find some field $\bar{\bar{K}}$, some $\bar{\bar{\kappa}}_0, \bar{\bar{\kappa}}_1, \cdots, \bar{\bar{\kappa}}_{m-1} \in \bar{\bar{K}}$, and some field homomorphism $\sigma : K \to \bar{\bar{K}}$, such that σ splits $k_m x^m + \cdots + k_0$ into $\bar{\bar{\kappa}}_0, \bar{\bar{\kappa}}_1, \cdots, \bar{\bar{\kappa}}_{m-1}$ universally.

(1) As $K[x]$ is a Euclid domain, $k_m x^m + \cdots + k_0$ has an irreducible factor $k'_n x^n + \cdots + k'_0$, $\bar{K} = K[t]/\langle k'_n t^n + \cdots + k'_0 \rangle$ is a field, $\mu : K \to \bar{K}, k \mapsto k$ is a field homomorphism, and the image $\bar{k}_m x^m + \cdots + \bar{k}_0$ of $k_m x^m + \cdots + k_0$ under μ has a root $\bar{\kappa}_0 = \bar{t} \in \bar{K}$.

(2) As the degree of $\frac{\bar{k}_m x^m + \cdots + \bar{k}_0}{x - \bar{\kappa}_0}$ is $m - 1$, it follows from **inductive hypothesis** that for some field $\bar{\bar{K}}$, for some $\bar{\bar{\kappa}}_1, \cdots, \bar{\bar{\kappa}}_{m-1} \in \bar{\bar{K}}$, for some field homomorphism $\nu : \bar{K} \to \bar{\bar{K}}$, ν splits $\frac{\bar{k}_m x^m + \cdots + \bar{k}_0}{x - \bar{\kappa}_0}$ into $\bar{\bar{\kappa}}_1, \cdots, \bar{\bar{\kappa}}_{m-1}$ universally.

(3) For some field $\bar{\bar{K}}$, for some $\bar{\bar{\kappa}}_0 = \nu(\bar{\kappa}_0), \bar{\bar{\kappa}}_1, \cdots, \bar{\bar{\kappa}}_{m-1} \in \bar{\bar{K}}$, for some field homomorphism $\sigma = \nu \circ \mu$, σ splits $k_m x^m + \cdots + k_0$ into $\bar{\bar{\kappa}}_0, \bar{\bar{\kappa}}_1, \cdots, \bar{\bar{\kappa}}_{m-1}$ universally.

$$\begin{tikzcd}
 & (\bar{\bar{K}}, \bar{\bar{\kappa}}_0, \bar{\bar{\kappa}}_1, \cdots, \bar{\bar{\kappa}}_{m-1}) \\
(K, k_m x^m + \cdots + k_0) \arrow[ur, dashed, "\exists\sigma"] \arrow[r, "\mu"] & (\bar{K}, \bar{\kappa}_0, \frac{\bar{k}_m x^m + \cdots + \bar{k}_0}{x - \bar{\kappa}_0}) \arrow[u, dashed, "\exists\nu"']
\end{tikzcd}$$

□

Definition 2.36. (**Lift**)
Let $\bar{K}, K, L$ be fields, $k_m x^m + \cdots + k_0 \in K[x]$, $\bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1} \in \bar{K}$, $\ell_0, \cdots, \ell_{m-1} \in L$, $\bar{\tau} : \bar{K} \to L$ be a field homomorphism sending $\bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1}$ to $\ell_0, \cdots, \ell_{m-1}$, $\sigma : K \to \bar{K}$ split $k_m x^m + \cdots + k_0$ into $\bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1}$, and $\tau : K \to L$ split $k_m x^m + \cdots + k_0$ into $\bar{\ell}_0, \cdots, \bar{\ell}_{m-1}$. If the diagram below commutes:

$$\begin{tikzcd}
 & (\bar{K}, \bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1}) \arrow[dl, "\bar{\tau}"'] \\
(L, \ell_0, \cdots, \ell_{m-1}) & (K, k_m x^m + \cdots + k_0) \arrow[l, "\tau"] \arrow[u, "\sigma"']
\end{tikzcd}$$

Then $\bar{\tau}$ is a lift of τ under σ.

Remark: $\bar{\tau}$ is a lift of τ under σ iff $(id_K, \bar{\tau}) \in \mathbf{Hom}(\sigma, \tau)$.

Proposition 2.37. (**The Universal Property of Splitting Map**)
Let $K, \bar{K}$ be fields, $k_m x^m + \cdots + k_0 \in K[x]$ with $m \geq 1, k_m \neq 0$, $\bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1} \in \bar{K}$, and $\sigma : K \to \bar{K}$ split $k_m x^m + \cdots + k_0$ into $\bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1}$. σ is universal iff for all field L, for all $\ell_0, \cdots, \ell_{m-1} \in L$, for all $\tau : K \to L$ that splits $k_m x^m + \cdots + k_0$ into $\ell_0, \cdots, \ell_{m-1}$, there exists $\xi \in \mathbf{Sym}(\ell_0, \cdots, \ell_{m-1})$ that extends to a unique lift $\bar{\tau}$ of the permuted τ under σ, such that the diagram below commutes:

$$\begin{tikzcd}
 & (\bar{K}, \bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1}) \arrow[ld, dashed, "\exists! \bar{\tau}"'] \\
(L, \xi(\ell_0, \cdots, \ell_{m-1})) & (K, k_m x^m + \cdots + k_0) \arrow[l, "\tau"] \arrow[u, "\sigma"']
\end{tikzcd}$$

In addition, if σ is universal, then for all valid $\xi_0, \xi_1 \in \mathbf{Sym}(\ell_0, \cdots, \ell_{m-1})$, the corresponding lifts $\bar{\tau}_0, \bar{\tau}_1$ have identical image $\mathbf{Im}(\bar{\tau}_0) = \mathbf{Im}(\bar{\tau}_1)$.

Proof. The additional part follows from $K[\xi(\ell_0, \cdots, \ell_{m-1})] = K[\ell_0, \cdots, \ell_{m-1}]$.
To prove our main result, we may divide our proof into two directions.
"if" direction:
Assume that for all field L, for all $\ell_0, \cdots, \ell_{m-1} \in L$, for all $\tau : K \to L$ that splits $k_m x^m + \cdots + k_0$ into $\ell_0, \cdots, \ell_{m-1}$, there exists $\xi \in \mathbf{Sym}(\ell_0, \cdots, \ell_{m-1})$ that extends to a unique lift $\bar{\tau}$ of the permuted τ under σ, such that the diagram below commutes:

$$\begin{tikzcd}
 & (\bar{K}, \bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1}) \arrow[ld, dashed, "\exists! \bar{\tau}"'] \\
(L, \xi(\ell_0, \cdots, \ell_{m-1})) & (K, k_m x^m + \cdots + k_0) \arrow[l, "\tau"] \arrow[u, "\sigma"']
\end{tikzcd}$$

If we choose τ as the restriction of σ to $K[\bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1}] \leq \bar{K}$,
then by the injectivity of $\bar{\tau}$, $K[\bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1}] = \bar{K}$, σ is universal.
"only if" direction:
Assume that σ is universal. We prove by induction on the degree m of $k_m x^m + \cdots + k_0$.
Basis Step: When $m = 1$, t is trivial and $\bar{\tau} = \tau \circ \sigma^{-1}$.
Inductive Hypothesis: For all $s \geq 1$, when $m = s$, assume the statement.
Inductive Step: When $m = s + 1$:

(1) As $K[x]$ is a Euclid domain, $k_m x^m + \cdots + k_0$ has an irreducible factor $k'_n x^n + \cdots + k'_0$.

(2) As σ, τ split $k_m x^m + \cdots + k_0$ into $\bar{\kappa}_0, \bar{\kappa}_1, \cdots, \bar{\kappa}_{m-1}, \ell_0, \ell_1, \cdots, \ell_{m-1}$, they also split $k'_n x^n + \cdots + k'_0$ into some subcollections of $\bar{\kappa}_0, \bar{\kappa}_1, \cdots, \bar{\kappa}_{m-1}, \ell_0, \ell_1, \cdots, \ell_{m-1}$.

(3) As we are free to permute $\ell_0, \ell_1, \cdots, \ell_{m-1}$, we may assume WLOG that the subcollections are $\bar{\kappa}_0, \bar{\kappa}_1, \cdots, \bar{\kappa}_{n-1}, \ell_0, \ell_1, \cdots, \ell_{n-1}$.

(4) As $\ell_0, \bar{\kappa}_0$ share a minimal polynomial $k'_n x^n + \cdots + k'_0$ over K, τ has a unique lift $\bar{\tau}_0 : K[\bar{\kappa}_0] \to L$ under the restriction σ_0 of σ to $K[\bar{\kappa}_0] \leq \bar{K}$, sending $\bar{\kappa}_0$ to ℓ_0.

(5) As the degree of $\frac{\bar{k}_m x^m + \cdots + \bar{k}_0}{x - \bar{\kappa}_0}$ is $m-1$ and we are free to permute $\ell_0, \ell_1, \cdots, \ell_{m-1}$, we may assume WLOG that $\bar{\tau}_0$ has a unique lift $\bar{\tau}$ under $\iota : K[\bar{\kappa}_0] \to \bar{K}, \bar{k} \mapsto \bar{k}$, sending $\bar{\kappa}_0$ to $\bar{\tau}_0(\bar{\kappa}_0) = \ell_0$, and sending $\bar{\kappa}_1, \cdots, \bar{\kappa}_{m-1}$ to $\ell_1, \cdots, \ell_{m-1}$.

(6) τ has a unique lift $\bar{\tau}$ under σ, sending $\bar{\kappa}_0, \bar{\kappa}_1, \cdots, \bar{\kappa}_{m-1}$ to $\ell_0, \ell_1, \cdots, \ell_{m-1}$.

$$\begin{tikzcd}
 & (\bar{K}, \bar{\kappa}_0, \bar{\kappa}_1, \cdots, \bar{\kappa}_{m-1}) \arrow[ddl, dashed, "\exists!\bar{\tau}"'] \\
 & (K[\bar{\kappa}_0], \bar{\kappa}_0, \frac{\bar{k}_m x^m + \cdots + \bar{k}_0}{x - \bar{\kappa}_0}) \arrow[u, "\iota"'] \arrow[dl, dashed, "\exists!\bar{\tau}_0"'] \\
(L, \ell_0, \ell_1, \cdots, \ell_{m-1}) & (K, k_m x^m + \cdots + k_0) \arrow[l, "\tau"'] \arrow[u, "\sigma_0"']
\end{tikzcd}$$

□

Remark: In other words, a splitting map σ of $k_m x^m + \cdots + k_0$ is universal iff it is below every splitting map τ of $k_m x^m + \cdots + k_0$, and all lifts $\bar{\tau}_0, \bar{\tau}_1$ of τ under a universal splitting map σ have identical image $\mathbf{Im}(\bar{\tau}_0) = \mathbf{Im}(\bar{\tau}_1)$.

Proposition 2.38. (**The Uniqueness of Universal Splitting Map**)
Let $\bar{K}, K, L$ be fields, $k_m x^m + \cdots + k_0 \in K[x]$, $\bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1} \in \bar{K}$, $\ell_0, \cdots, \ell_{m-1} \in L$, $\sigma : K \to \bar{K}$ split $k_m x^m + \cdots + k_0$ into $\bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1}$ universally, and $\tau : K \to L$ split $k_m x^m + \cdots + k_0$ into $\ell_0, \cdots, \ell_{m-1}$ universally. $\sigma \cong \tau$.

Proof. As σ is universal, there exists $\xi \in \mathbf{Sym}(\ell_0, \cdots, \ell_{m-1})$ that extends to a unique lift $\bar{\tau}$ of the permuted τ under σ, such that the diagram below commutes:

$$\begin{tikzcd}
 & (\bar{K}, \bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1}) \arrow[dl, dashed, "\exists!\bar{\tau}"'] \\
(L, \xi(\ell_0, \cdots, \ell_{m-1})) & (K, k_m x^m + \cdots + k_0) \arrow[l, "\tau"'] \arrow[u, "\sigma"']
\end{tikzcd}$$

As τ is also universal, $\bar{\tau}$ is surjective, so $(id_K, \bar{\tau})$ is a splitting map isomorphism. □

3 Galois Theory

3.1 Algebraic Element and Resultant

Definition 3.1. (**Algebraic Element**)
Let $K, \bar{K}$ be fields, $\sigma : K \to \bar{K}$ be a field homomorphism, and $\bar{k} \in \bar{K}$. TFAE:

(1) The K-dimension of $K[\bar{k}]$ is finite.

(2) $\bar{k}$ is a root of some $k_m x^m + \cdots + k_0 = 0$ with $k_m \neq 0$.

If both conditions above hold, then $\bar{k}$ is algebraic over K.

Remark: Given that $\bar{\kappa}, \bar{\ell} \in \bar{K}$ are algebraic over K, we have two ways to show that $\bar{\kappa}+\bar{\ell}$ is algebraic over K. If we follow (1), then this is a simple consequence of $K[\bar{\kappa}+\bar{\ell}] \leq K[\bar{\kappa}, \bar{\ell}]$. If we follow (2), then the tool, i.e., the resultant, will be useful later.

Definition 3.2. (**Resultant**)
Let K be a field, and $k(x,y) = k_m x^m + \cdots + k_0 y^m, l(x,y) = l_n x^n + \cdots + l_0 y^n$ be homogeneous. Define their resultant $\mathbf{Res}(k(x,y), l(x,y))$ as an $m+n$ by $m+n$ determinant of their coefficients. If $m = 3, n = 2$, then $\mathbf{Res}(k(x,y), l(x,y))$ is:

$$\begin{vmatrix} k_3 & k_2 & k_1 & k_0 & 0 \\ 0 & k_3 & k_2 & k_1 & k_0 \\ l_2 & l_1 & l_0 & 0 & 0 \\ 0 & l_2 & l_1 & l_0 & 0 \\ 0 & 0 & l_2 & l_1 & l_0 \end{vmatrix}$$

$$k_3^2 l_0^3 - k_3 k_2 l_1 l_0^2 - 2k_3 k_1 l_2 l_0^2 + k_3 k_1 l_1^2 l_0 + 3k_3 k_0 l_2 l_1 l_0 - k_3 k_0 l_1^3 + k_2^2 l_2 l_0^2$$
$$- k_2 k_1 l_2 l_1 l_0 - 2k_2 k_0 l_2^2 l_0 + k_2 k_0 l_2 l_1^2 + k_1^2 l_2^2 l_0 - k_1 k_0 l_2^2 l_1 + k_0^2 l_2^3$$

Remark: If we evaluate the indeterminate y at 1, then we may define $\mathbf{Res}(k(x), l(x))$.

Proposition 3.3. (**Factorization of Resultant**)

$$\begin{aligned} k(x,y), l(x,y) &= \prod_{0 \leq j \leq m-1} \begin{vmatrix} x & b_j \\ y & d_j \end{vmatrix}, \prod_{0 \leq i \leq n-1} \begin{vmatrix} a_i & x \\ c_i & y \end{vmatrix} \\ \mathbf{Res}(k(x,y), l(x,y)) &= \prod_{0 \leq i \leq n-1, 0 \leq j \leq m-1} \begin{vmatrix} a_i & b_j \\ c_i & d_j \end{vmatrix} \\ &= \prod_{0 \leq i \leq n-1} k(a_i, c_i) = \prod_{0 \leq j \leq m-1} l(b_j, d_j) \end{aligned}$$

Proof. If we multiply $\mathbf{Res}(k(x,y),l(x,y))$ by the Vandermonde determinant below:

$$\begin{vmatrix} a_0^{m+n-1} & \cdots & a_{n-1}^{m+n-1} & b_0^{m+n-1} & \cdots & b_{m-1}^{m+n-1} \\ \vdots & & \vdots & \vdots & & \vdots \\ c_0^{m+n-1} & \cdots & c_{n-1}^{m+n-1} & d_0^{m+n-1} & \cdots & d_{m-1}^{m+n-1} \end{vmatrix}$$

That is:

$$\prod_{0\le i<j\le n-1} \begin{vmatrix} a_i & a_j \\ c_i & c_j \end{vmatrix} \prod_{0\le i\le n-1, 0\le j\le m-1} \begin{vmatrix} a_i & b_j \\ c_i & d_j \end{vmatrix} \prod_{0\le i<j\le m-1} \begin{vmatrix} b_i & b_j \\ d_i & d_j \end{vmatrix}$$

Then $\mathbf{Res}(k(x,y),l(x,y))$ becomes:

$$\begin{vmatrix} k(a_0,c_0)a_0^{n-1} & \cdots & k(a_{n-1},c_{n-1})a_{n-1}^{n-1} & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ k(a_0,c_0)c_0^{n-1} & \cdots & k(a_{n-1},c_{n-1})c_{n-1}^{n-1} & 0 & \cdots & 0 \\ 0 & \cdots & 0 & l(b_0,d_0)b_0^{m-1} & \cdots & l(b_{m-1},d_{m-1})b_{m-1}^{m-1} \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & l(b_0,d_0)d_0^{m-1} & \cdots & l(b_{m-1},d_{m-1})d_{m-1}^{m-1} \end{vmatrix}$$

That is:

$$\prod_{0\le i<j\le n-1} \begin{vmatrix} a_i & a_j \\ c_i & c_j \end{vmatrix} \prod_{0\le i\le n-1, 0\le j\le m-1} \begin{vmatrix} a_i & b_j \\ c_i & d_j \end{vmatrix}^2 \prod_{0\le i<j\le m-1} \begin{vmatrix} b_i & b_j \\ d_i & d_j \end{vmatrix}$$

It suffices to divide the common factors. □

Remark: As a consequence:

$$\begin{aligned} k(x), l(x) &= \prod_{0\le j\le m-1} \begin{vmatrix} x & \kappa_j \\ 1 & 1 \end{vmatrix}, \prod_{0\le i\le n-1} \begin{vmatrix} -\ell_i & x \\ -1 & 1 \end{vmatrix} \\ \mathbf{Res}(k(x), l(x)) &= \prod_{0\le i\le n-1, 0\le j\le m-1} \begin{vmatrix} -\ell_i & \kappa_j \\ -1 & 1 \end{vmatrix} \\ &= (-1)^{mn} \prod_{0\le i\le n-1} k(\ell_i) = \prod_{0\le j\le m-1} l(\kappa_j) \end{aligned}$$

Example 3.4. (**Factorization of Resultant**)

$$\begin{aligned} k(x,y), l(x,y) &= \prod_{0\le j\le m-1} k_j(x,y), \prod_{0\le i\le n-1} l_i(x,y) \\ \mathbf{Res}(k(x,y), l(x,y)) &= \prod_{0\le i\le n-1, 0\le j\le m-1} \mathbf{Res}(k_j(x,y), l_i(x,y)) \end{aligned}$$

Remark: As a consequence:

$$\begin{aligned} k(x), l(x) &= \prod_{0\le j\le m-1} k_j(x), \prod_{0\le i\le n-1} l_i(x) \\ \mathbf{Res}(k(x), l(x)) &= \prod_{0\le i\le n-1, 0\le j\le m-1} \mathbf{Res}(k_j(x), l_i(x)) \end{aligned}$$

Proposition 3.5. (**Change of Variables**)

$$\begin{aligned} K(x,y), L(x,y) &= k_m x^m + \cdots + k_0 y^m, l_n x^n + \cdots + l_0 y^n \\ X(u,v), Y(u,v) &= x_s u^s + \cdots + x_0 v^s, y_s u^s + \cdots + y_0 v^s \\ k(u,v), l(u,v) &= K(X(u,v), Y(u,v)), L(X(u,v), Y(u,v)) \\ \mathbf{Res}(k(u,v), l(u,v)) &= \mathbf{Res}(K(x,y), L(x,y))^s \mathbf{Res}(X(u,v), Y(u,v))^{mn} \end{aligned}$$

Proof. For the case $m = n = 1$, the result is direct. For the general case:

$$\begin{aligned} K(x,y), L(x,y) &= \prod_{0\le j\le m-1} \begin{vmatrix} x & B_j \\ y & D_j \end{vmatrix}, \prod_{0\le i\le n-1} \begin{vmatrix} A_i & x \\ C_i & y \end{vmatrix} \\ \mathbf{Res}(k(u,v), l(u,v)) &= \prod_{0\le i\le n-1, 0\le j\le m-1} \mathbf{Res}\left(\begin{vmatrix} X(u,v) & B_j \\ Y(u,v) & D_j \end{vmatrix}, \begin{vmatrix} A_i & X(u,v) \\ C_i & Y(u,v) \end{vmatrix} \right) \\ &= \prod_{0\le i\le n-1, 0\le j\le m-1} \begin{vmatrix} A_i & B_j \\ C_i & D_j \end{vmatrix}^s \mathbf{Res}(X(u,v), Y(u,v)) \\ &= \mathbf{Res}(K(x,y), L(x,y))^s \mathbf{Res}(X(u,v), Y(u,v))^{mn} \end{aligned}$$

□

Remark: As a consequence:

$$\begin{aligned} K(x), L(x) &= k_m x^m + \cdots + k_0, l_n x^n + \cdots + l_0 \\ X(u) &= x_s u^s + \cdots + x_0 \\ k(u), l(u) &= K(X(u)), L(X(u)) \\ \mathbf{Res}(k(u), l(u)) &= \mathbf{Res}(K(x), L(x))^s x_s^{mns} \end{aligned}$$

Proposition 3.6. Let $K, \bar{K}$ be fields, $\sigma : K \to \bar{K}$ be a field homomorphism, and $\bar{\kappa}, \bar{\ell} \in \bar{K}$ be algebraic over K. $\bar{\kappa} + \bar{\ell}$ is algebraic over K.

Proof. Assume that $\bar{\kappa}, \bar{\ell}$ are roots of some $k_m x^m + \cdots + k_0, l_n x^n + \cdots + l_0 \in K[x]$ with $k_m \neq 0, l_n \neq 0$ respectively. $y = \bar{k} + \bar{l}$ is also algebraic over K, because is a root of:

$$\mathbf{Res}_x(k_m x^m + \cdots + k_0, l_n (y-x)^n + \cdots + l_0) \in K[y] \text{ with } k_m^n l_n^m \neq 0$$

□

3.2 Normal Homomorphism

Definition 3.7. (**Finite Homomorphism**)
Let $K, \bar{K}$ be fields, and $\sigma : K \to \bar{K}$ be a field homomorphism.
If the K-dimension of $\bar{K}$ is finite, then σ is finite.

Definition 3.8. (**Normal Homomorphism**)
Let $K, \bar{K}$ be fields, and $\sigma : K \to \bar{K}$ be a field homomorphism.
If for all irreducible $k_m x^m + \cdots + k_0 \in K[x]$ with some root $\bar{\kappa}_0 \in \bar{K}$,
σ splits $k_m x^m + \cdots + k_0$ into some $\bar{\kappa}_0, \bar{\kappa}_1, \cdots, \bar{\kappa}_{m-1} \in \bar{K}$, then σ is normal.

Proposition 3.9. (**The Universal Property of Normal Homomorphism**)
Let $K, \bar{K}$ be fields, and $\sigma : K \to \bar{K}$ be a field homomorphism. TFAE:

(1) σ is finite and normal.

(2) For some $k_m x^m + \cdots + k_0 \in K[x]$ with $m \geq 1, k_m \neq 0$, for some $\bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1} \in \bar{K}$, σ splits $k_m x^m + \cdots + k_0$ into $\bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1}$ universally.

Proof. We may divide our proof into two parts.
Part 1: Assume that σ is finite and normal.
Choose a K-basis of $\bar{K}$. It suffices to multiply the minimal polynomials of the members.
Part 2: Assume that for some $k_m x^m + \cdots + k_0 \in K[x]$ with $m \geq 1, k_m \neq 0$, for some $\bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1} \in \bar{K}$, σ splits $k_m x^m + \cdots + k_0$ into $\bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1}$ universally. For all irreducible $l_n x^n + \cdots + l_0 \in K[x]$ with some root $\bar{\ell}_0 \in \bar{K}$, choose some field $\bar{\bar{K}}$, some $\bar{\bar{\kappa}}_0, \cdots, \bar{\bar{\kappa}}_{m-1}, \bar{\bar{\ell}}_0, \bar{\bar{\ell}}_1, \cdots, \bar{\bar{\ell}}_{n-1} \in \bar{\bar{K}}$, and some field homomorphism $\bar{\sigma}$, such that $\bar{\sigma}$ split $(k_m x^m + \cdots + k_0)(l_n x^n + \cdots + l_0)$ into $\bar{\bar{\kappa}}_0, \cdots, \bar{\bar{\kappa}}_{m-1}, \bar{\bar{\ell}}_0, \bar{\bar{\ell}}_1, \cdots, \bar{\bar{\ell}}_{n-1}$ universally. Apply **the universal property of splitting map** to the universal splitting map σ of $k_m x^m + \cdots + k_0$. We may permute $\bar{\bar{\kappa}}_0, \cdots, \bar{\bar{\kappa}}_{m-1}, \bar{\bar{\ell}}_0, \bar{\bar{\ell}}_1, \cdots, \bar{\bar{\ell}}_{n-1}$, such that the diagram below commutes:

$$\begin{tikzcd}
 & (\bar{\bar{K}}, \bar{\bar{\kappa}}_0, \cdots, \bar{\bar{\kappa}}_{m-1}, \bar{\bar{\ell}}_0, \bar{\bar{\ell}}_1, \cdots, \bar{\bar{\ell}}_{n-1}) \\
(K, k_m x^m + \cdots + k_0, l_n x^n + \cdots + l_0) \arrow[ru, "\bar{\sigma}"] \arrow[r, "\sigma"'] & (\bar{K}, \bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1}, \bar{\ell}_0, \frac{\bar{l}_n x^n + \cdots + \bar{l}_0}{x - \bar{\ell}_0}) \arrow[u, dashed, "\exists ! \tau_0"']
\end{tikzcd}$$

To show that $l_n x^n + \cdots + l_0$ splits into some $\bar{\ell}_0, \bar{\ell}_1, \cdots, \bar{\ell}_{n-1}$ over $\bar{K}$, it suffices to show that $\bar{\bar{\ell}}_1$ has a preimage $\bar{\ell}_1$ under τ_0 and factorize $\bar{l}_n x^n + \cdots + \bar{l}_0$ inductively, so consider the diagram below:

$$\begin{tikzcd}
 & (\bar{\bar{K}}, \xi(\bar{\bar{\kappa}}_0, \cdots, \bar{\bar{\kappa}}_{m-1}), \bar{\bar{\ell}}_1) \\
(K[t]/\langle l_n t^n + \cdots + l_0 \rangle, k_m x^m + \cdots + k_0, \bar{t}) \arrow[ur, "\bar{\mu}"] \arrow[r, "\mu"'] & (\bar{K}, \bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1}, \bar{\ell}_0) \arrow[u, dashed, "\exists ! \tau_1"']
\end{tikzcd}$$

We explain the information of each map:

(1) μ is an extension of σ, sending the coset $\bar{t}$ of t to $\bar{\ell}_0 \in \bar{K}$.
As $l_n x^n + \cdots + l_0$ is a minimal polynomial of $\bar{\ell}_0 \in \bar{K}$ over K, μ is well-defined.
As σ splits $k_m x^m + \cdots + k_0$ into $\bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1}$ universally, so is μ.

(2) $\bar{\mu}$ is an extension of $\bar{\sigma}$, sending the coset of t to $\bar{\bar{\ell}}_1 \in \bar{\bar{K}}$.
As $l_n x^n + \cdots + l_0$ is a minimal polynomial of $\bar{\bar{\ell}}_1 \in \bar{\bar{K}}$ over K, $\bar{\mu}$ is well-defined.
As $\bar{\sigma}$ splits $k_m x^m + \cdots + k_0$ into $\bar{\bar{\kappa}}_0, \cdots, \bar{\bar{\kappa}}_{m-1}$, so is $\bar{\mu}$.

(3) ξ is a permutation of $\bar{\bar{\kappa}}_0, \cdots, \bar{\bar{\kappa}}_{m-1}$ that extends to a unique lift τ_1 of the permuted $\bar{\mu}$ under μ. Note that $\tau_1(\bar{\ell}_0) = \tau_1(\mu(\bar{t})) = \bar{\mu}(\bar{t}) = \bar{\bar{\ell}}_1$.

Apply **the universal property of splitting map** to the universal splitting map σ of $k_m x^m + \cdots + k_0$, $\bar{\bar{\ell}}_1 \in \mathbf{Im}(\tau_1) = \mathbf{Im}(\tau_0)$ has a preimage $\bar{\ell}_1$ under τ_0. □

Example 3.10. Consider the subfield lattice below, where:

$$\zeta = \mathrm{e}^{\frac{2\pi \mathrm{i}}{3}}$$
$$\bar{\kappa}_0, \bar{\kappa}_1, \bar{\kappa}_2 = 3^{\frac{1}{3}}, 3^{\frac{1}{3}}\zeta, 3^{\frac{1}{3}}\zeta^2$$

All intermediate field homomorphisms are normal, except:

$$\mathbb{Q}[\bar{\kappa}_0]/\mathbb{Q}, \mathbb{Q}[\bar{\kappa}_1]/\mathbb{Q}, \mathbb{Q}[\bar{\kappa}_2]/\mathbb{Q}$$

Remark: We will correspond this with the subgroup lattice of $\mathbf{Sym}(\bar{\kappa}_0, \bar{\kappa}_1, \bar{\kappa}_2)$.

Example 3.11. Consider the subfield lattice below, where:

$$\bar{\ell}_0, \bar{\ell}_1, \bar{\ell}_2, \bar{\ell}_3 = 3^{\frac{1}{4}}, 3^{\frac{1}{4}}\mathrm{i}, -3^{\frac{1}{4}}, -3^{\frac{1}{4}}\mathrm{i}$$

All intermediate field homomorphisms are normal, except:

$$\mathbb{Q}[\bar{\ell}_0]/\mathbb{Q}, \mathbb{Q}[\bar{\ell}_1]/\mathbb{Q}, \mathbb{Q}[\bar{\ell}_0 + \bar{\ell}_1]/\mathbb{Q}, \mathbb{Q}[\bar{\ell}_0 - \bar{\ell}_1]/\mathbb{Q}$$

Remark: We will correspond this with the subgroup lattice of $\mathbf{Dih}\begin{pmatrix} \bar{\ell}_3 & \bar{\ell}_2 \\ \bar{\ell}_0 & \bar{\ell}_1 \end{pmatrix}$.

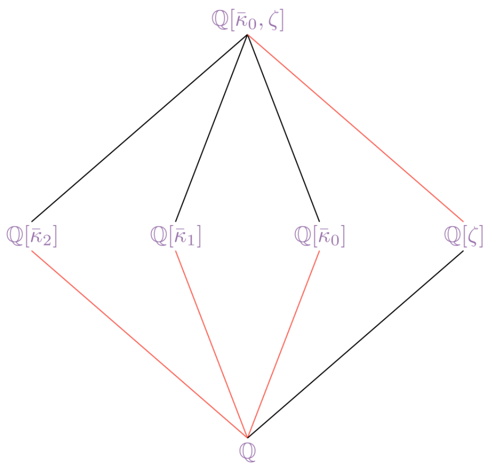
$\mathbb{Q}[\bar{\kappa}_0, \zeta]$
$\mathbb{Q}[\bar{\kappa}_2]$
$\mathbb{Q}[\bar{\kappa}_1]$
$\mathbb{Q}[\bar{\kappa}_0]$
$\mathbb{Q}[\zeta]$
$\mathbb{Q}$

Figure 1: The Subfield Lattice in **Example 3.10.**

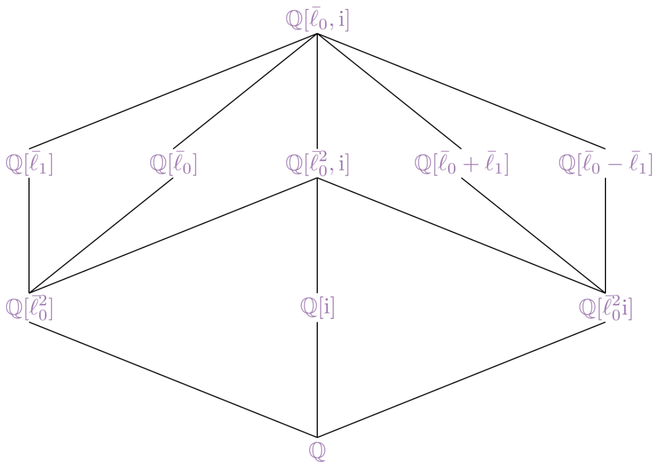
$\mathbb{Q}[\bar{\ell}_0, \mathrm{i}]$
$\mathbb{Q}[\bar{\ell}_1]$
$\mathbb{Q}[\bar{\ell}_0]$
$\mathbb{Q}[\bar{\ell}_0^2, \mathrm{i}]$
$\mathbb{Q}[\bar{\ell}_0 + \bar{\ell}_1]$
$\mathbb{Q}[\bar{\ell}_0 - \bar{\ell}_1]$
$\mathbb{Q}[\bar{\ell}_0^2]$
$\mathbb{Q}[\mathrm{i}]$
$\mathbb{Q}[\bar{\ell}_0^2 \mathrm{i}]$
$\mathbb{Q}$

Figure 2: The Subfield Lattice in **Example 3.11.**

Example 3.12. Consider the subfield lattice below, where:

$$\zeta = \mathrm{e}^{\frac{2\pi \mathrm{i}}{7}}$$

$$\bar{\kappa}_0, \bar{\kappa}_1, \bar{\kappa}_2, \bar{\kappa}_3, \bar{\kappa}_4, \bar{\kappa}_5 = \zeta, \zeta^3, \zeta^2, \zeta^6, \zeta^4, \zeta^5$$

All intermediate field homomorphisms are normal.

Remark: We will correspond this with the subgroup lattice of $\langle(\bar{\kappa}_0, \bar{\kappa}_1, \bar{\kappa}_2, \bar{\kappa}_3, \bar{\kappa}_4, \bar{\kappa}_5)\rangle$.

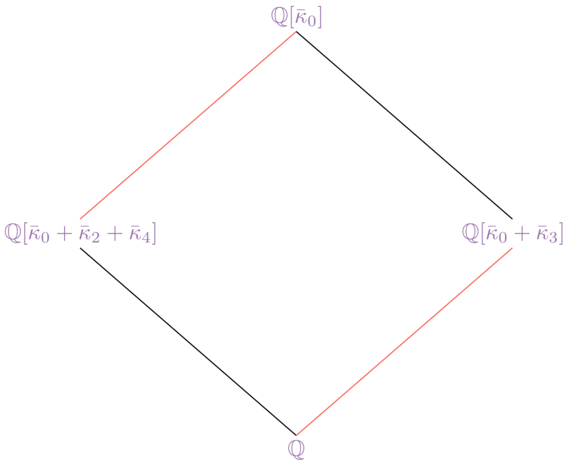
$\mathbb{Q}[\bar{\kappa}_0]$
$\mathbb{Q}[\bar{\kappa}_0 + \bar{\kappa}_2 + \bar{\kappa}_4]$
$\mathbb{Q}[\bar{\kappa}_0 + \bar{\kappa}_3]$
$\mathbb{Q}$

Figure 3: The Subfield Lattice in **Example 3.12.**

Example 3.13. Consider the subfield lattice below, where:

$$\zeta = \mathrm{e}^{\frac{2\pi \mathrm{i}}{7}}$$

$$\bar{\kappa}_0, \bar{\kappa}_1, \bar{\kappa}_2 = \sqrt{\zeta + \zeta^6}, \sqrt{\zeta^2 + \zeta^5}, \sqrt{\zeta^4 + \zeta^3} \text{ with } \mathbf{Im}(\bar{\kappa}_0, \bar{\kappa}_1, \bar{\kappa}_2) \geq 0$$

$$\bar{\ell}_0, \bar{\ell}_1, \bar{\ell}_2, \bar{\ell}_3 = +\bar{\kappa}_0 + \bar{\kappa}_1 + \bar{\kappa}_2, -\bar{\kappa}_0 - \bar{\kappa}_1 + \bar{\kappa}_2, -\bar{\kappa}_0 + \bar{\kappa}_1 - \bar{\kappa}_2, +\bar{\kappa}_0 - \bar{\kappa}_1 - \bar{\kappa}_2$$

All intermediate field homomorphisms are normal, except:

$$\mathbb{Q}[\bar{\kappa}_0]/\mathbb{Q}, \mathbb{Q}[\bar{\kappa}_1]/\mathbb{Q}, \mathbb{Q}[\bar{\kappa}_2]/\mathbb{Q}, \mathbb{Q}[\bar{\ell}_0]/\mathbb{Q}, \mathbb{Q}[\bar{\ell}_1]/\mathbb{Q}, \mathbb{Q}[\bar{\ell}_2]/\mathbb{Q}, \mathbb{Q}[\bar{\ell}_3]/\mathbb{Q}$$

Remark: We will correspond this with the subgroup lattice of $\mathbf{Alt}(\bar{\ell}_0, \bar{\ell}_1, \bar{\ell}_2, \bar{\ell}_3)$.

Example 3.14. Consider the subfield lattice below, where:

$$\zeta = \mathrm{e}^{\frac{2\pi \mathrm{i}}{3}}$$

$$\bar{\kappa}_0, \bar{\kappa}_1, \bar{\kappa}_2 = \sqrt{3^{\frac{4}{3}} + 3^{\frac{5}{3}}}, \sqrt{3^{\frac{4}{3}}\zeta + 3^{\frac{5}{3}}\zeta^2}, \sqrt{3^{\frac{4}{3}}\zeta^2 + 3^{\frac{5}{3}}\zeta} \text{ with } \mathbf{Re}(\bar{\kappa}_0, \bar{\kappa}_1, \bar{\kappa}_2) \geq 0$$

$$\bar{\ell}_0, \bar{\ell}_1, \bar{\ell}_2, \bar{\ell}_3 = +\bar{\kappa}_0 + \bar{\kappa}_1 + \bar{\kappa}_2, -\bar{\kappa}_0 - \bar{\kappa}_1, \bar{\kappa}_2 + -\bar{\kappa}_0 + \bar{\kappa}_1 - \bar{\kappa}_2, +\bar{\kappa}_0 - \bar{\kappa}_1 - \bar{\kappa}_2$$

There are many intermediate field homomorphisms that are not normal.

Remark: We will correspond this with the subgroup lattice of $\mathbf{Sym}(\bar{\ell}_0, \bar{\ell}_1, \bar{\ell}_2, \bar{\ell}_3)$.

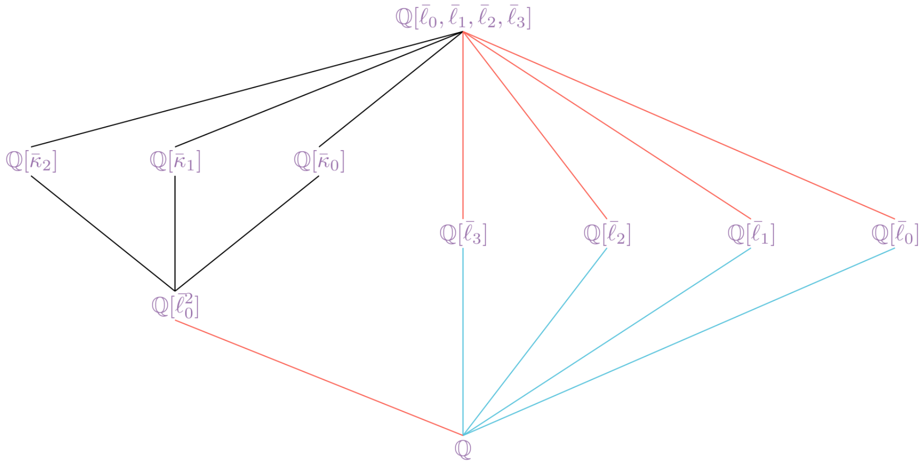
$\mathbb{Q}[\bar{\ell}_0, \bar{\ell}_1, \bar{\ell}_2, \bar{\ell}_3]$
$\mathbb{Q}[\bar{\kappa}_2]$
$\mathbb{Q}[\bar{\kappa}_1]$
$\mathbb{Q}[\bar{\kappa}_0]$
$\mathbb{Q}[\bar{\ell}_3]$
$\mathbb{Q}[\bar{\ell}_2]$
$\mathbb{Q}[\bar{\ell}_1]$
$\mathbb{Q}[\bar{\ell}_0]$
$\mathbb{Q}[\bar{\ell}_0^2]$
$\mathbb{Q}$

Figure 4: The Subfield Lattice in **Example 3.13.**

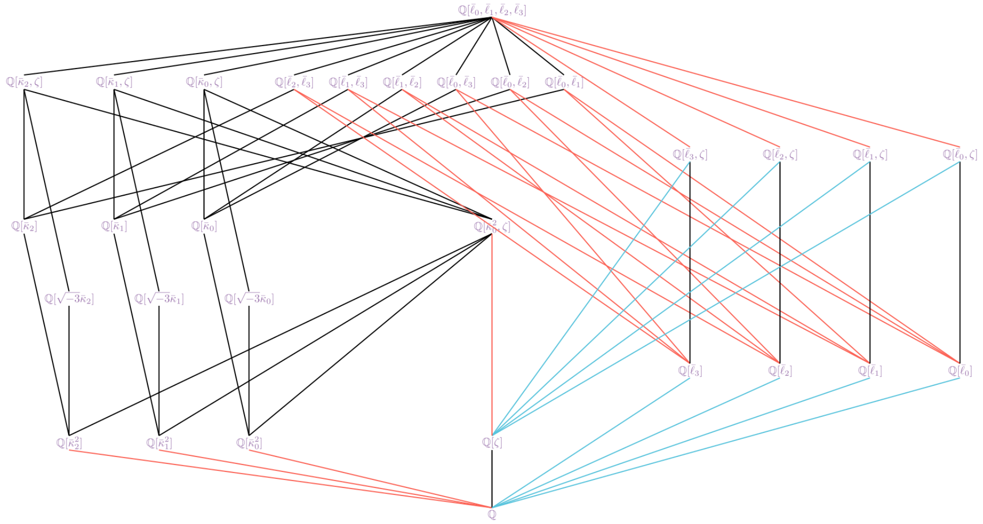
$\mathbb{Q}[\bar{\ell}_0, \bar{\ell}_1, \bar{\ell}_2, \bar{\ell}_3]$
$\mathbb{Q}[\bar{\kappa}_2, \zeta]$
$\mathbb{Q}[\bar{\kappa}_1, \zeta]$
$\mathbb{Q}[\bar{\kappa}_0, \zeta]$
$\mathbb{Q}[\bar{\ell}_2, \bar{\ell}_3]$
$\mathbb{Q}[\bar{\ell}_1, \bar{\ell}_3]$
$\mathbb{Q}[\bar{\ell}_1, \bar{\ell}_2]$
$\mathbb{Q}[\bar{\ell}_0, \bar{\ell}_3]$
$\mathbb{Q}[\bar{\ell}_0, \bar{\ell}_2]$
$\mathbb{Q}[\bar{\ell}_0, \bar{\ell}_1]$
$\mathbb{Q}[\bar{\ell}_3, \zeta]$
$\mathbb{Q}[\bar{\ell}_2, \zeta]$
$\mathbb{Q}[\bar{\ell}_1, \zeta]$
$\mathbb{Q}[\bar{\ell}_0, \zeta]$
$\mathbb{Q}[\bar{\kappa}_2]$
$\mathbb{Q}[\bar{\kappa}_1]$
$\mathbb{Q}[\bar{\kappa}_0]$
$\mathbb{Q}[\bar{\kappa}_0^2, \zeta]$
$\mathbb{Q}[\sqrt{-3}\bar{\kappa}_2]$
$\mathbb{Q}[\sqrt{-3}\bar{\kappa}_1]$
$\mathbb{Q}[\sqrt{-3}\bar{\kappa}_0]$
$\mathbb{Q}[\bar{\ell}_3]$
$\mathbb{Q}[\bar{\ell}_2]$
$\mathbb{Q}[\bar{\ell}_1]$
$\mathbb{Q}[\bar{\ell}_0]$
$\mathbb{Q}[\bar{\kappa}_2^2]$
$\mathbb{Q}[\bar{\kappa}_1^2]$
$\mathbb{Q}[\bar{\kappa}_0^2]$
$\mathbb{Q}[\zeta]$
$\mathbb{Q}$

Figure 5: The Subfield Lattice in **Example 3.14.**

3.3 Separable Homomorphism and Discriminant

Definition 3.15. (**Separable Polynomial**)
Let K be a field, and $k_m x^m + \cdots + k_0 \in K[x]$. TFAE:

(1) $k_m x^m + \cdots + k_0, (k_m x^m + \cdots + k_0)'$ are coprime.

(2) For all field homomorphism $\sigma : K \to \bar{K}$, $\bar{k}_m x^m + \cdots + \bar{k}_0$ has distinct roots.

If both conditions above hold, then $k_m x^m + \cdots + k_0$ is separable over K.

Remark: To prove the equivalence, solve Bézout equation.

Proposition 3.16. Let K be a field, and $k_m x^m + \cdots + k_0 \in K[x]$ be irreducible.

(1) If $\textbf{Char}(K) = 0$,
then $k_m x^m + \cdots + k_0$ is separable over K.

(2) If $\textbf{Char}(K)$ is a prime number p, and for some $n \geq 0$, $nk_n \in K^\times$,
then $k_m x^m + \cdots + k_0$ is separable over K.

(3) If $\textbf{Char}(K)$ is a prime number p, and for all $n \geq 0$, $\sqrt[p]{k_n} \in K$,
then $k_m x^m + \cdots + k_0$ is separable over K.

Proof. For (1) and (2), it suffices to notice that the degree of $(k_m x^m + \cdots + k_0)'$ is strictly between $-\infty$ and the degree of $k_m x^m + \cdots + k_0$. For (3), we prove that for some $n \geq 0$, $nk_n \in K^\times$ by contradiction, so the result will follow from (2). Assume to the contrary that for all $n \geq 0$, $nk_n = 0$, we arrive at a contradiction where $k_m x^m + \cdots + k_0 = (\sqrt[p]{k_m} x^{\frac{m}{p}} + \cdots + \sqrt[p]{k_0})^p$ is both irreducible and reducible. □

Proposition 3.17. Let K be a field, where $\textbf{Char}(K)$ is a prime number p, and $L = K(x^p)$. $y^p - x^p \in L[y]$ is irreducible and inseparable over L.

Proof. Define a field $M = K(x)$ and an inclusion field homomorphism $\sigma : L \to M$. σ splits $y^p - x^p$ into $x, \cdots, x \in M$, so $y^p - x^p$ is inseparable. To see that $y^p - x^p = (y - x)^p \in L[y]$ is irreducible over L, it suffices to notice that $n = p$ is the minimum positive integer such that $(y - x)^n \in L[y] \leq M[y]$. □

Definition 3.18. (**Discriminant**)
Let K be a field, and $k(x) = k_m x^m + \cdots + k_0 \in K[x]$ with $k_m \neq 0$.
Define the discriminant of $k(x)$ as:

$$\textbf{Disc}(k(x)) = \frac{(-1)^{\frac{m(m-1)}{2}}}{k_m} \textbf{Res}(k(x), k'(x))$$

If $m = 3$, then $\textbf{Disc}(k(x))$ is:

$$-\frac{1}{k_3} \begin{vmatrix} k_3 & k_2 & k_1 & k_0 & 0 \\ 0 & k_3 & k_2 & k_1 & k_0 \\ 3k_3 & 2k_2 & k_1 & 0 & 0 \\ 0 & 3k_3 & 2k_2 & k_1 & 0 \\ 0 & 0 & 3k_3 & 2k_2 & k_1 \end{vmatrix}$$

$$-27k_3^2k_0^2 + 18k_3k_2k_1k_0 - 4k_3k_1^3 + k_2^2k_1^2 - 4k_2^3k_0$$

Proposition 3.19. (**Factorization of Discriminant**)

$$k(x) = k_m \prod_{0 \leq i \leq m-1} (x - x_i)$$

$$\mathbf{Disc}(k(x)) = k_m^{2m-2} \prod_{0 \leq i < j \leq m-1} (x_i - x_j)^2$$

Proof. For the case $k_m = 1$, note that:

$$k(x) = \prod_{0 \leq i \leq m-1} (x - x_i) = \prod_{0 \leq i \leq m-1} \begin{vmatrix} x & x_i \\ 1 & 1 \end{vmatrix}$$

Therefore, according to **factorization of resultant**:

$$\begin{aligned} \mathbf{Disc}(k(x)) &= (-1)^{\frac{m(m-1)}{2}} \mathbf{Res}(k(x), k'(x)) \\ &= (-1)^{\frac{m(m-1)}{2}} \prod_{0 \leq j \leq m-1} k'(x_j) \\ &= (-1)^{\frac{m(m-1)}{2}} \prod_{0 \leq j \leq m-1} \prod_{0 \leq i \leq m-1, i \neq j} (x_j - x_i) \\ &= \prod_{0 \leq i < j \leq m-1} (x_i - x_j)^2 \end{aligned}$$

For the general case, note that:

$$\begin{aligned} \mathbf{Disc}(k(x)) &= \frac{(-1)^{\frac{m(m-1)}{2}}}{k_m} \mathbf{Res}(k(x), k'(x)) \\ &= (-1)^{\frac{m(m-1)}{2}} k_m^{2m-2} \mathbf{Res}\left(\frac{k(x)}{k_m}, \frac{k'(x)}{k_m}\right) \\ &= k_m^{2m-2} \prod_{0 \leq i < j \leq m-1} (x_i - x_j)^2 \end{aligned}$$

□

Remark: This implies:

$$k(x) \text{ is separable } \iff \mathbf{Disc}(k(x)) \neq 0$$

Definition 3.20. (**Simple Homomorphism**)
Let $K, \bar{K}$ be fields, and $\sigma : K \to \bar{K}$ be a field homomorphism.
If for some $\bar{\kappa} \in \bar{K}$, $\bar{K} = K(\bar{\kappa})$, then σ is simple.

Proposition 3.21. (**Steinitz's Theorem**)
Let K, M be fields, $K \leq M$, and the K-dimension of M is finite.
The inclusion map $\sigma : K \to M$ is simple iff $\#(L \text{ is a field} : K \leq L \leq M) < +\infty$.

Proof. When K is finite, M is also finite, and every generator $\bar{k}$ of $\bar{K}^{\times}$ is a primitive element, i.e., satisfies $K[\bar{k}] = \bar{K}$. In addition, $\{L \text{ is a field} : K \leq L \leq M\}$ is always finite. When K is infinite, We may divide our proof into two directions.

"if" direction:

Assume that $0 \leq n = \#(L \text{ is a field} : K \leq L \lneq M) < +\infty$.

We find an element m in the complement of $\bigcup_{K \leq L \lneq M} L$ in M by induction on n.

Basis Step: When $n = 0$ or 1, choose $m = 1$ or m in the complement of K in M.

Inductive Hypothesis: For all $s \geq 1$, when $n = s$, assume the statement.

Inductive Step: When $n = s + 1$, assume that $\{L \text{ is a field} : K \leq L \lneq M\}$ collects $L_0, L_1, \cdots, L_{n-2}, L_{n-1}$. Choose m_0, m_{n-1} in the complements of $L_1 \cup \cdots \cup L_{n-2} \cup L_{n-1}, L_0 \cup L_1 \cup \cdots \cup L_{n-2}$ in M. It follows from elementary geometry that the infinite line $\ell = \{k_0 m_0 + k_{n-1} m_{n-1} \in M : k_0, k_{n-1} \in K, k_0 + k_{n-1} = 1\}$ intersects each L_i at at most 1 point, so we may remove these points and choose $m \in \ell$.

"only if" direction:

Assume that for some $m \in M$ with the monic minimal polynomial $k(x)$ over K, $M = K[m]$. For all $K \leq L \leq M$, the monic minimal polynomial $l(x)$ of m over L is a factor of $k(x)$. As the monic minimal polynomial of m over $K[\text{The coefficients of } l(x)]$ is also $l(x)$, it follows from **tower theorem** that $K[\text{The coefficients of } l(x)] = L$, so it suffices to notice that $k(x)$ has finitely monic factors. □

Example 3.22. Let K be an infinite field, where $\mathbf{Char}(K)$ is a prime number p. As $K(x, y)^p \leq K(x^p, y^p)$ and the $K(x^p, y^p)$-dimension of $K(x, y)$ is $p^2 > p$, $\sigma : K(x^p, y^p) \to K(x, y), k(x^p, y^p) \mapsto k(x^p, y^p)$ is not simple, and $\{L \text{ is a field} : K(x^p, y^p) \leq L \leq K(x, y)\}$ contains an infinite set $\{K(x^p, y^p, ax + by) : a, b \in K\}$.

Definition 3.23. (**Separable Homomorphism**)

Let $K, \bar{K}$ be fields, and $\sigma : K \to \bar{K}$ be a field homomorphism.

If for all irreducible $k_m x^m + \cdots + k_0 \in K[x]$ with some root $\bar{\kappa} \in \bar{K}$,

$k_m x^m + \cdots + k_0$ is separable over K, then σ is separable.

Remark: If $\mathbf{Char}(K) = 0$, then σ is separable. If $\mathbf{Char}(K)$ is a prime number p, and $\sqrt[p]{K} \leq K$, then σ is separable. Hence, inseparable field homomorphism is rare.

Proposition 3.24. (**Primitive Element Theorem**)

Let $K, \bar{K}$ be fields, and $\sigma : K \to \bar{K}$ be a field homomorphism.

If σ is finite and separable, then σ is simple.

Proof. When K is finite, $\bar{K}$ is also finite, and every generator $\bar{k}$ of $\bar{K}^{\times}$ is a primitive element. When K is infinite, it suffices to show that for all algebraic elements $\bar{\kappa}_0, \bar{\ell}_0$ in $\bar{K}$ over K, the restriction of σ to $K[\bar{\kappa}_0, \bar{\ell}_0] \leq \bar{K}$ is simple. For all $\bar{c} \in \bar{K}$, assume that $K[\bar{\kappa}_0 + \bar{c}\bar{\ell}_0] \lneq \bar{L} = K[\bar{\kappa}_0, \bar{\ell}_0]$. If we can confine c to a finite set, then we may avoid this finite set and choose a primitive element.

(1) Choose minimal polynomials $\bar{k}_m x^m + \cdots + \bar{k}_0, \bar{l}_n x^n + \cdots + \bar{l}_0$ of $\bar{\kappa}_0, \bar{\ell}_0$ over $K[\bar{\kappa}_0 + \bar{c}\bar{\ell}_0]$. Choose some field $\bar{\bar{K}}$, some $\bar{\bar{\kappa}}_0, \cdots, \bar{\bar{\kappa}}_{m-1}, \bar{\bar{\ell}}_0, \bar{\bar{\ell}}_1, \cdots, \bar{\bar{\ell}}_{n-1} \in \bar{\bar{K}}$, and some $\tau \in \mathbf{Hom}(K[\bar{\kappa}_0 + \bar{c}\bar{\ell}_0], \bar{\bar{K}})$, such that σ splits $(\bar{k}_m x^m + \cdots + \bar{k}_0)(\bar{l}_n x^n + \cdots + \bar{l}_0)$ into $\bar{\bar{\kappa}}_0, \cdots, \bar{\bar{\kappa}}_{m-1}, \bar{\bar{\ell}}_0, \bar{\bar{\ell}}_1, \cdots, \bar{\bar{\ell}}_{n-1}$ universally. As $K[\bar{\kappa}_0 + \bar{c}\bar{\ell}_0] \lneq \bar{L}$, $n \geq 2$.

(2) As σ is separable, $\bar{l}_n x^n + \cdots + \bar{l}_0$ is separable, so $\bar{\bar{\ell}}_0 \neq \bar{\bar{\ell}}_1$.

(3) As the minimal polynomial of $\bar{\bar{\ell}}_0, \bar{\bar{\ell}}_1 \in \bar{\bar{K}}$ over $K[\bar{\bar{\kappa}}_0 + c\bar{\bar{\ell}}_0]$ is $\bar{\bar{l}}_n x^n + \cdots + \bar{\bar{l}}_0$, the extensions $\mu_0, \mu_1 : \bar{\bar{L}} = K[\bar{\bar{\kappa}}_0, \bar{\bar{\ell}}_0] \to \bar{\bar{K}}$ of τ sending $\bar{\bar{\ell}}_0$ to $\bar{\bar{\ell}}_0, \bar{\bar{\ell}}_1$ are well-defined.

(4) Apply **the universal property of splitting map** to the universal splitting map μ_0 of $\bar{\bar{k}}_m x^m + \cdots + \bar{\bar{k}}_0$, there exists $\xi \in \mathbf{Sym}(\bar{\bar{\kappa}}_0, \cdots, \bar{\bar{\kappa}}_{m-1}, \bar{\bar{\ell}}_0, \bar{\bar{\ell}}_1, \cdots, \bar{\bar{\ell}}_{n-1})$ fixing $\bar{\bar{\ell}}_1$ that extends to a unique lift $\bar{\bar{\mu}}_1$ of the permuted μ_1 under μ_0, such that the diagram below commutes:

$$\begin{tikzcd}
 & (\bar{\bar{K}}, \bar{\bar{\ell}}_0, \bar{\bar{\kappa}}_0, \cdots, \bar{\bar{\kappa}}_{m-1}, \bar{\bar{\ell}}_1, \cdots, \bar{\bar{\ell}}_{n-1}) \arrow[dl, dashed, "\exists! \bar{\bar{\mu}}_1"'] \\
(\bar{\bar{K}}, \bar{\bar{\ell}}_1, t(\bar{\bar{\kappa}}_0, \cdots, \bar{\bar{\kappa}}_{m-1}, \bar{\bar{\ell}}_0, \cdots, \bar{\bar{\ell}}_{n-1})) & (\bar{\bar{L}}, \bar{\bar{\ell}}_0, \bar{\bar{k}}_m x^m + \cdots + \bar{\bar{k}}_0, \frac{\bar{\bar{l}}_n x^n + \cdots + \bar{\bar{l}}_0}{x - \bar{\bar{\ell}}_0}) \arrow[l, "\mu_1"'] \arrow[u, "\mu_0"']
\end{tikzcd}$$

(5) As τ sends $\bar{c}, \bar{\kappa}_0 + \bar{c}\bar{\ell}_0$ to $\bar{\bar{c}}, \bar{\bar{\kappa}}_0 + \bar{\bar{c}}\bar{\bar{\bar{\ell}}}_0$, its extensions $\mu_0, \mu_1, \bar{\bar{\mu}}_1$ fix $\bar{\bar{c}}, \bar{\bar{\kappa}}_0 + \bar{\bar{c}}\bar{\bar{\bar{\ell}}}_0$.

(6) As $\bar{\bar{\mu}}_1$ sends $\bar{\bar{\kappa}}_0, \bar{\bar{c}}, \bar{\bar{\ell}}_0$ to $\bar{\bar{\kappa}}_i, \bar{\bar{c}}, \bar{\bar{\ell}}_1$, where $\bar{\bar{\ell}}_0 \neq \bar{\bar{\ell}}_1$, $\bar{\bar{c}}$ is confined to $\frac{\bar{\bar{\kappa}}_i - \bar{\bar{\kappa}}_0}{\bar{\bar{\ell}}_0 - \bar{\bar{\ell}}_1}$.

(7) As $\{\bar{\bar{\kappa}}_0, \cdots, \bar{\bar{\kappa}}_{m-1}, \bar{\bar{\ell}}_1, \cdots, \bar{\bar{\ell}}_{n-1}\}$ is a finite set, c is confined to a finite set.

□

3.4 G-fixed Subfield and Deck Transformation

Definition 3.25. (**G-fixed Subfield**)
Let K be a field, and G be a subgroup of $\mathbf{Aut}(K)$.
Define the G-fixed subfield of K as $K^G = \{k \in K : \forall g \in G, g(k) = k\}$.

Definition 3.26. (**Deck Transformation**)
Let $K, \bar{K}$ be fields, $\sigma : K \to \bar{K}$ be a field homomorphism, and $\bar{\tau} \in \mathbf{Aut}(\bar{K})$. If:

$$\begin{tikzcd}
\bar{K} \arrow[rr, "\bar{\tau}"] & & \bar{K} \\
 & K \arrow[ul, "\sigma"] \arrow[ur, "\sigma"'] &
\end{tikzcd}$$

Then $\bar{\tau} \in \mathbf{Deck}(\sigma)$ is a deck transformation.

Proposition 3.27. (**Artin's Theorem**)
Let $\bar{K}$ be a field, $\bar{G} \leq \mathbf{Aut}(\bar{K})$ be finite, and $\sigma : \bar{K}^{\bar{G}} \to \bar{K}$ be the inclusion map.

(1) σ is separable, normal and finite.

(2) $\mathbf{Deck}(\sigma) = \bar{G}$.

Proof. We may divide our proof into four parts.

(1) For all $\bar{\kappa}_0 \in \bar{K}$, $\bar{G} * \bar{\kappa}_0$ has $m \leq |\bar{G}|$ distinct elements $\bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1}$. As the minimal polynomial $(x - \bar{\kappa}_0) \cdots (x - \bar{\kappa}_{m-1})$ of $\bar{\kappa}_0$ over $\bar{K}^{\bar{G}}$ is separable, σ is separable.

(2) For all $\bar{\kappa}_0 \in \bar{K}$, the $\bar{K}^{\bar{G}}$-dimension $d(\bar{\kappa}_0) = m$ of $\bar{K}^{\bar{G}}[\bar{\kappa}_0]$ is bounded by $|\bar{G}|$, so we may choose $\bar{\kappa}_0 \in \bar{K}$ with minimal polynomial $k(x)$ over $\bar{K}^{\bar{G}}$ and maximal $d(\bar{\kappa}_0)$.

(3) For all $\bar{\ell}_0 \in \bar{K}$, the restriction of σ to $\bar{K}^{\bar{G}}[\bar{\kappa}_0, \bar{\ell}_0]$ is finite and separable, thus simple. It follows from the maximality of $d(\bar{\kappa}_0)$ that $\bar{K}^{\bar{G}}[\bar{\kappa}_0, \bar{\ell}_0] = \bar{K}^{\bar{G}}[\bar{\kappa}_0]$, so $\bar{K}^{\bar{G}}[\bar{\kappa}_0] = \bar{K}$, and the universal splitting map σ of $(x - \bar{\kappa}_0) \cdots (x - \bar{\kappa}_{m-1})$ is normal and finite.

(4) As $\bar{K}^{\bar{G}}[\bar{\kappa}_0] = \bar{K}$, every $\bar{\tau} \in \mathbf{Aut}(\bar{K})$ is determined by $\bar{\tau}(\bar{\kappa}_0)$, so $\mathbf{Deck}(\sigma) = \bar{G}$.

□

Proposition 3.28. (**The Universal Property of Deck Transformation**)
Let $K, \bar{K}$ be fields, $k_m x^m + \cdots + k_0 \in K[x]$ with $m \geq 1, k_m \neq 0$, $\bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1} \in \bar{K}$, and $\sigma : K \to \bar{K}$ split $k_m x^m + \cdots + k_0$ into $\bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1}$ universally.

(1) For all irreducible $l_n x^n + \cdots + l_0 \in K[x]$, for all $\bar{\ell}_0, \cdots, \bar{\ell}_{n-1} \in \bar{K}$, if σ splits $l_n x^n + \cdots + l_0$ into $\bar{\ell}_0, \cdots, \bar{\ell}_{n-1}$, then $\mathbf{Deck}(\sigma)$ is transitive on $\bar{\ell}_0, \cdots, \bar{\ell}_{n-1}$.

(2) If we assume further that σ is separable, then $\bar{K}^{\mathbf{Deck}(\sigma)} = \mathbf{Im}(\sigma)$.

Proof. We may divide our proof into three parts.

(1) For all $\bar{\ell}_i$, as its minimal polynomial over K is $l_n x^n + \cdots + l_0$, the extension $\sigma_i : K[t]/\langle l_n t^n + \cdots + l_0 \rangle \to \bar{K}$ of σ sending the coset $\bar{t}$ of t to $\bar{\ell}_i$ is well-defined, and it splits $k_m x^m + \cdots + k_0$ into $\bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1}$ universally.

(2) For all $\bar{\ell}_i, \bar{\ell}_j$, apply **the universal property of splitting map** to the universal splitting map σ_i of $k_m x^m + \cdots + k_0$. There exists $\xi_{ij} \in \mathbf{Sym}(\bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1})$ that extends to a unique lift $\bar{\tau}_{ij}$ of the permuted σ_j under σ_i, i.e., a deck transformation of σ sending $\bar{\ell}_i$ to $\bar{\ell}_j$, such that the diagram below commutes:

$$\begin{tikzcd}
 & (\bar{K}, \bar{\ell}_i, \bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1}) \arrow[ld, dashed, "\exists! \bar{\tau}_{ij}"'] \\
(\bar{K}, \bar{\ell}_j, \xi(\bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1})) & (K[t]/\langle l_n t^n + \cdots + l_0 \rangle, k_m x^m + \cdots + k_0) \arrow[l, "\sigma_j"'] \arrow[u, "\sigma_i"']
\end{tikzcd}$$

(3) Assume that σ is separable, for all $\bar{k} \in \bar{K}$, $\bar{k} \in \bar{K}^{\mathbf{Deck}(\sigma)}$ iff the minimal polynomial of $\bar{k}$ over K has a unique simple root, i.e., $\bar{k} \in \mathbf{Im}(\sigma)$, so $\bar{K}^{\mathbf{Deck}(\sigma)} = \mathbf{Im}(\sigma)$.

□

3.5 Galois Homomorphism

Definition 3.29. (**Galois Homomorphism**)
Let $K, \bar{K}$ be fields, and $\sigma : K \to \bar{K}$ be a field homomorphism. TFAE:

(1) σ is finite, separable and normal.

(2) For some separable $k_m x^m + \cdots + k_0 \in K[x]$ with $m \geq 1, k_m \neq 0$, for some $\bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1} \in \bar{K}$, σ splits $k_m x^m + \cdots + k_0$ into $\bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1}$ universally.

(3) σ is finite, and $\mathbf{Im}(\sigma) = \bar{K}^{\mathbf{Deck}(\sigma)}$.

(4) σ is finite, and the K-dimension of $\bar{K}$ is $|\mathbf{Deck}(\sigma)|$.

If all conditions above hold, then σ is Galois.

Example 3.30. (**The Galois Correspondence**)
Let K, M be fields with $K \leq M$, where the inclusion map $\sigma : K \to M$ is Galois with $G = \mathbf{Deck}(\sigma)$. The maps below are inverses to each other.

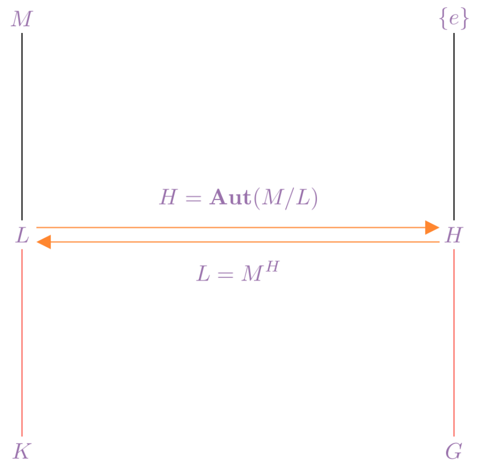

Figure 6: The Galois correspondence

4 Application

4.1 Finite Field

Proposition 4.1. (**Classification of** $\mathbf{GF}(p^m)$)
Let p be prime, and $m \geq 1$.

(1) For some field $\bar{K}$, $|\bar{K}| = p^m$.

(2) For all fields $\bar{K}, L$ with $|\bar{K}| = |L| = p^m$, $\bar{K} \cong L$.

Proof. We may divide our proof into four steps.

(1) According to **the existence of universal splitting map**, for some field $\bar{K}$, for some $\bar{\kappa}_0, \cdots, \bar{\kappa}_{p^m-1} \in \bar{K}$, for some field homomorphism $\sigma : \mathbb{Z}/p\mathbb{Z} \to \bar{K}$, σ splits $x^{p^m} - x$ into $\bar{\kappa}_0, \cdots, \bar{\kappa}_{p^m-1}$ universally.

(2) According to **Frobenius endomorphism**, $\{\bar{\kappa}_0, \cdots, \bar{\kappa}_{p^m-1}\}$ is the $\langle \bar{k} \mapsto \bar{k}^{p^m} \rangle$-fixed subfield of $\bar{K}$, so it follows from σ is universal that $\bar{K} = \{\bar{\kappa}_0, \cdots, \bar{\kappa}_{p^m-1}\}$.

(3) As $(x^{p^m} - x)'$ is a nonzero constant -1, $x^{p^m} - x$ is separable, so $|\bar{K}| = p^m$.

(4) For all fields $\bar{K}, L$ with order p^m, choose **prime homomorphisms** $\sigma : \mathbb{Z}/p\mathbb{Z} \to \bar{K}, \tau : \mathbb{Z}/p\mathbb{Z} \to L$ that split $x^{p^m} - x$ into $\bar{\kappa}_0, \cdots, \bar{\kappa}_{p^m-1}, \ell_0, \cdots, \ell_{p^m-1}$ universally. According to **the uniqueness of universal splitting map**, $\sigma \cong \tau$, so $\bar{K} \cong L$.

$$\begin{tikzcd}
& (\bar{K}, \bar{\kappa}_0, \cdots, \bar{\kappa}_{p^m-1}) \arrow[dl, dashed, "\exists! \bar{\tau}"'] \\
(L, \xi(\ell_0, \cdots, \ell_{p^m-1})) & (\mathbb{Z}/p\mathbb{Z}, x^{p^m} - x) \arrow[l, "\tau"] \arrow[u, "\sigma"']
\end{tikzcd}$$

□

Remark: When the context is clear, we denote this field as $\mathbf{GF}(p^m)$.

Proposition 4.2. (**Classification of** $\mathbf{Hom}(\mathbf{GF}(p^m), \mathbf{GF}(p^n))$)
Let p be prime, and $m, n \geq 1$.

(1) $\mathbf{Hom}(\mathbf{GF}(p^m), \mathbf{GF}(p^n)) \neq \emptyset$ iff $m \mid n$.

(2) For all $\bar{\tau}_0, \bar{\tau}_1 \in \mathbf{Hom}(\mathbf{GF}(p^m), \mathbf{GF}(p^n))$, $\mathbf{Im}(\bar{\tau}_0) = \mathbf{Im}(\bar{\tau}_1)$.

(3) $\mathbf{Deck}(\mathbf{GF}(p^n)/\mathbf{GF}(p^m)) = \langle \bar{k} \mapsto \bar{k}^{p^m} \rangle$.

Proof. We may divide our proof into three parts.

(1) If $\mathbf{Hom}(\mathbf{GF}(p^m), \mathbf{GF}(p^n)) \neq \emptyset$, then $\mathbf{GF}(p^n)$ is a $\mathbf{GF}(p^m)$-vector space, so $m \mid n$.

(2) If $m \mid n$, then take **prime homomorphisms** $\sigma : \mathbf{GF}(p) \to \mathbf{GF}(p^m), \tau : \mathbf{GF}(p) \to \mathbf{GF}(p^n)$ that split $x^{p^m} - x, x^{p^n} - x$ into $\bar{\kappa}_0, \cdots, \bar{\kappa}_{p^m-1}, \ell_0, \cdots, \ell_{p^n-1}$ universally. As $x^{p^m} - x \mid x^{p^n} - x$, we may assume WLOG that τ splits $x^{p^m} - x$ into $\ell_0, \cdots, \ell_{p^m-1}$. Apply **the universal property of splitting map** to the universal splitting map σ of $x^{p^m} - x$, there exists $\xi \in \mathbf{Sym}(\ell_0, \cdots, \ell_{p^m-1})$ that extends to a unique lift $\bar{\tau} \in \mathbf{Hom}(\mathbf{GF}(p^m), \mathbf{GF}(p^n))$ of the permuted τ under σ, and for all valid $\xi_0, \xi_1 \in \mathbf{Sym}(\ell_0, \cdots, \ell_{p^m-1})$, the corresponding lifts $\bar{\tau}_0, \bar{\tau}_1 \in \mathbf{Hom}(\mathbf{GF}(p^m), \mathbf{GF}(p^n))$ have identical image $\mathbf{Im}(\bar{\tau}_0) = \mathbf{Im}(\bar{\tau}_1)$.

$$\begin{tikzcd}
 & (\mathbf{GF}(p^m), \bar{\kappa}_0, \cdots, \bar{\kappa}_{p^m-1}) \arrow[dl, dashed, "\exists! \bar{\tau}"'] \\
(\mathbf{GF}(p^n), \xi(\ell_0, \cdots, \ell_{p^m-1})) & (\mathbf{GF}(p), x^{p^m} - x) \arrow[l, "\tau"] \arrow[u, "\sigma"']
\end{tikzcd}$$

(3) As $\mathbf{GF}(p^m)$ is fixed under $\langle \bar{k} \mapsto \bar{k}^{p^m} \rangle$, $\langle \bar{k} \mapsto \bar{k}^{p^m} \rangle \leq \mathbf{Deck}(\mathbf{GF}(p^n)/\mathbf{GF}(p^m))$. As $|\mathbf{Deck}(\mathbf{GF}(p^n)/\mathbf{GF}(p^m))| = |\langle \bar{k} \mapsto \bar{k}^{p^m} \rangle|$, $\mathbf{Deck}(\mathbf{GF}(p^n)/\mathbf{GF}(p^m)) = \langle \bar{k} \mapsto \bar{k}^{p^m} \rangle$.

□

Proposition 4.3. **(Classification of Irreducible $k(x) \in \mathbf{GF}(p^m)[x]$)**
Let p be prime, and m be a positive integer.

(1) For all positive integer n,
there exists an irreducible $k(x) \in \mathbf{GF}(p^m)[x]$ of degree n.

(2) For all positive integer n, for all irreducible $k(x) \in \mathbf{GF}(p^m)[x]$ of degree n, every $\sigma \in \mathbf{Hom}(\mathbf{GF}(p^m), \mathbf{GF}(p^{mn}))$ is a universal splitting map of $k(x)$.

(3) For all positive integer n, $x^{p^{mn}} - x$ is the product of all monic irreducible $k(x) \in \mathbf{GF}(p^m)[x]$ of degree $d \mid n$.

Proof. We may divide our proof into three steps.

(1) For all positive integer n, choose a generator $\bar{\kappa}$ of $\mathbf{GF}(p^{mn})^\times$ with minimal polynomial $k(x)$ over $\mathbf{GF}(p^m)$. As $\mathbf{GF}(p^m)[t]/\langle k(t) \rangle \cong \mathbf{GF}(p^{mn})$ has $\mathbf{GF}(p^m)$-dimension n, the irreducible polynomial $k(x) \in \mathbf{GF}(p^m)[x]$ has degree n.

(2) For all positive integer n, for all irreducible $k(x) \in \mathbf{GF}(p^m)[x]$ of degree n, for some field $\mathbf{GF}(p^l)$, for some $\bar{\kappa}_0, \cdots, \bar{\kappa}_{n-1} \in \mathbf{GF}(p^l)$, for some $\sigma \in \mathbf{Hom}(\mathbf{GF}(p^m), \mathbf{GF}(p^l))$, σ splits $k(x)$ into $\bar{\kappa}_0, \cdots, \bar{\kappa}_{n-1}$ universally. For all $\bar{\kappa}_i$, as its minimal polynomial over $\mathbf{GF}(p^m)$ is $k(x)$, there exists $\sigma_i \in \mathbf{Hom}(\mathbf{GF}(p^m)[t]/\langle k(x) \rangle, \mathbf{GF}(p^k))$ sending the coset $\bar{t}$ of t to $\bar{\kappa}_i$. As $\mathbf{GF}(p^m)[t]/\langle k_n x^n + \cdots + k_0 \rangle \cong \mathbf{GF}(p^{mn})$, $\mathbf{Im}(\sigma_0) = \cdots = \mathbf{Im}(\sigma_{n-1})$, so $k = mn$.

(3) For all positive integer n, $\bar{k} \sim \bar{l}$ if $\bar{k}, \bar{l}$ share the monic minimal polynomial over $\mathbf{GF}(p^m)$ is an equivalence relation on $\mathbf{GF}(p^{mn})$, so the product of all such min-

imal polynomials is $\prod_{\bar{k}\in\mathbf{GF}(p^{mn})}(x-\bar{k}) = x^{p^{mn}} - x$. It suffices to notice that $k(x)$ is one of such minimal polynomial iff there exists a field homomorphism $\bar{\tau} : \mathbf{GF}(p^m)[t]/\langle k(t)\rangle \to \mathbf{GF}(p^{mn})$, i.e., the degree d of $k(x)$ divides n.

□

4.2 Cubic Polynomial

Proposition 4.4. Let $K, \bar{K}$ be fields with $\mathbf{Char}(K) \neq 2$, $k_m x^m + \cdots + k_0 \in K[x]$ with $m \geq 1, k_m \neq 0$, $\bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1} \in \bar{K}$ be distinct, and $\sigma : K \to \bar{K}$ be separable and split $k_m x^m + \cdots + k_0$ into $\bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1}$ universally.

$$\mathbf{Disc}(k_m x^m + \cdots + k_0) \in K^2 \iff \mathbf{Deck}(\sigma) \leq \mathbf{Alt}(\bar{\kappa}_0, \cdots, \bar{\kappa}_{m-1})$$

Proof. It suffices to notice that $K = \bar{K}^{\mathbf{Deck}(\sigma)}$, $1 \neq -1$, and for all $\bar{\tau} \in \mathbf{Deck}(\sigma)$:

$$\bar{\tau} \text{ sends } \begin{vmatrix} 1 & \cdots & 1 \\ \vdots & & \vdots \\ \bar{\kappa}_0^{m-1} & \cdots & \bar{\kappa}_{m-1}^{m-1} \end{vmatrix} \in K^\times \text{ to } \mathbf{Sign}(\bar{\tau}) \begin{vmatrix} 1 & \cdots & 1 \\ \vdots & & \vdots \\ \bar{\kappa}_0^{m-1} & \cdots & \bar{\kappa}_{m-1}^{m-1} \end{vmatrix} \in K^\times$$

□

Proposition 4.5. $\mathbf{Deck}(\mathbb{Q}[\bar{\kappa}_0, \bar{\kappa}_1, \bar{\kappa}_2]/\mathbb{Q}) = \mathbf{Sym}(\bar{\kappa}_0, \bar{\kappa}_1, \bar{\kappa}_2)$, where:

$$\zeta = \mathrm{e}^{\frac{2\pi\mathrm{i}}{3}}$$
$$\bar{\kappa}_0, \bar{\kappa}_1, \bar{\kappa}_2 = 3^{\frac{1}{3}}, 3^{\frac{1}{3}}\zeta, 3^{\frac{1}{3}}\zeta^2$$

Proof. Realize $\mathbb{Q}[\bar{\kappa}_0, \bar{\kappa}_1, \bar{\kappa}_2]/\mathbb{Q}$ as a universal splitting map of:

$$k(x) = x^3 - 3$$

(1) As $k(x) \in \mathbb{Q}[x]$ is irreducible, $\mathbf{Deck}(\mathbb{Q}[\bar{\kappa}_0, \bar{\kappa}_1, \bar{\kappa}_2]/\mathbb{Q})$ is transitive on $\bar{\kappa}_0, \bar{\kappa}_1, \bar{\kappa}_2$.

(2) As $\mathbf{Disc}(k(x)) = -243 \notin \mathbb{Q}^2$, $\mathbf{Deck}(\mathbb{Q}[\bar{\kappa}_0, \bar{\kappa}_1, \bar{\kappa}_2]/\mathbb{Q}) \not\leq \mathbf{Alt}(\bar{\kappa}_0, \bar{\kappa}_1, \bar{\kappa}_2)$.

Hence, $\mathbf{Deck}(\mathbb{Q}[\bar{\kappa}_0, \bar{\kappa}_1, \bar{\kappa}_2]/\mathbb{Q}) = \mathbf{Sym}(\bar{\kappa}_0, \bar{\kappa}_1, \bar{\kappa}_2)$. □

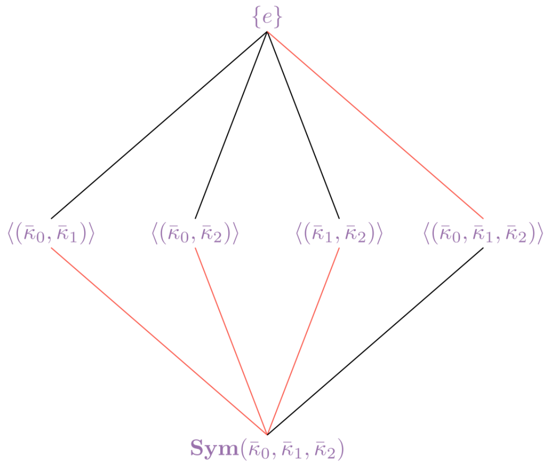
$\{e\}$
$\langle(\bar\kappa_0,\bar\kappa_1)\rangle$
$\langle(\bar\kappa_0,\bar\kappa_2)\rangle$
$\langle(\bar\kappa_1,\bar\kappa_2)\rangle$
$\langle(\bar\kappa_0,\bar\kappa_1,\bar\kappa_2)\rangle$
$\mathbf{Sym}(\bar\kappa_0,\bar\kappa_1,\bar\kappa_2)$

Figure 7: The Subgroup Lattice in **Proposition 4.5.**

4.3 Quartic Polynomial

Proposition 4.6. Let $K, \bar{K}$ be fields, $l_4x^4 + l_3x^3 + l_2x^2 + l_1x + l_0 \in K[x]$, $\bar\ell_0, \bar\ell_1, \bar\ell_2, \bar\ell_3 \in \bar{K}$ be distinct, and $\sigma : K \to \bar{K}$ be separable and split $l_4x^4 + l_3x^3 + l_2x^2 + l_1x + l_0$ into $\bar\ell_0, \bar\ell_1, \bar\ell_2, \bar\ell_3$ universally.

$$\bar\ell_0\bar\ell_1 + \bar\ell_2\bar\ell_3 \in K \iff \mathbf{Deck}(\sigma) \le \mathbf{Dih}\begin{pmatrix} \bar\ell_3 & \bar\ell_1 \\ \bar\ell_0 & \bar\ell_2 \end{pmatrix}$$

$$\bar\ell_0\bar\ell_2 + \bar\ell_1\bar\ell_3 \in K \iff \mathbf{Deck}(\sigma) \le \mathbf{Dih}\begin{pmatrix} \bar\ell_3 & \bar\ell_2 \\ \bar\ell_0 & \bar\ell_1 \end{pmatrix}$$

$$\bar\ell_0\bar\ell_3 + \bar\ell_1\bar\ell_2 \in K \iff \mathbf{Deck}(\sigma) \le \mathbf{Dih}\begin{pmatrix} \bar\ell_2 & \bar\ell_3 \\ \bar\ell_0 & \bar\ell_1 \end{pmatrix}$$

Proof. As the three groups are conjugates, it suffices to prove the first equivalence.

(1) $\bar\ell_0\bar\ell_1 + \bar\ell_2\bar\ell_3, \bar\ell_0\bar\ell_2 + \bar\ell_1\bar\ell_3, \bar\ell_0\bar\ell_3 + \bar\ell_1\bar\ell_2$ are distinct, because:

$$(\bar\ell_0\bar\ell_1 + \bar\ell_2\bar\ell_3) - (\bar\ell_0\bar\ell_2 + \bar\ell_1\bar\ell_3) = (\bar\ell_0 - \bar\ell_3)(\bar\ell_1 - \bar\ell_2) \neq \bar0$$
$$(\bar\ell_0\bar\ell_1 + \bar\ell_2\bar\ell_3) - (\bar\ell_0\bar\ell_3 + \bar\ell_1\bar\ell_2) = (\bar\ell_0 - \bar\ell_2)(\bar\ell_1 - \bar\ell_2) \neq \bar0$$
$$(\bar\ell_0\bar\ell_2 + \bar\ell_1\bar\ell_3) - (\bar\ell_0\bar\ell_3 + \bar\ell_1\bar\ell_2) = (\bar\ell_0 - \bar\ell_1)(\bar\ell_2 - \bar\ell_3) \neq \bar0$$

(2) As $\langle(\bar\ell_1, \bar\ell_2, \bar\ell_3)\rangle * \bar\ell_0\bar\ell_1 + \bar\ell_2\bar\ell_3 = \{\bar\ell_0\bar\ell_1 + \bar\ell_2\bar\ell_3, \bar\ell_0\bar\ell_2 + \bar\ell_1\bar\ell_3, \bar\ell_0\bar\ell_3 + \bar\ell_1\bar\ell_2\}$, $\mathbf{Sym}(\bar\ell_0\bar\ell_1 + \bar\ell_2\bar\ell_3) * \bar\ell_0\bar\ell_1 + \bar\ell_2\bar\ell_3 = \{\bar\ell_0\bar\ell_1 + \bar\ell_2\bar\ell_3, \bar\ell_0\bar\ell_2 + \bar\ell_1\bar\ell_3, \bar\ell_0\bar\ell_3 + \bar\ell_1\bar\ell_2\}$.

(3) As $\mathbf{Dih}\begin{pmatrix} \bar\ell_3 & \bar\ell_1 \\ \bar\ell_0 & \bar\ell_2 \end{pmatrix}$ stabilizes $\bar\ell_0\bar\ell_1 + \bar\ell_2\bar\ell_3$, and $\left|\mathbf{Dih}\begin{pmatrix} \bar\ell_3 & \bar\ell_1 \\ \bar\ell_0 & \bar\ell_2 \end{pmatrix}\right| |\mathbf{Sym}(\bar\ell_0, \bar\ell_1, \bar\ell_2, \bar\ell_3) *$

$\bar{\ell}_0\bar{\ell}_1+\bar{\ell}_2\bar{\ell}_3| = |\mathbf{Sym}(\bar{\ell}_0,\bar{\ell}_1,\bar{\ell}_2,\bar{\ell}_3)|$, $\mathbf{Dih}\begin{pmatrix}\bar{\ell}_3 & \bar{\ell}_1\\ \bar{\ell}_0 & \bar{\ell}_2\end{pmatrix} \leq \mathbf{Sym}(\bar{\ell}_0,\bar{\ell}_1,\bar{\ell}_2,\bar{\ell}_3)$ is the entire stabilizer subgroup of $\bar{\ell}_0\bar{\ell}_1+\bar{\ell}_2\bar{\ell}_3$, which implies our result.

□

Remark: If $\mathbf{Char}(K) \neq 2$, then we may replace these polynomials by $\bar{\kappa}_0^2, \bar{\kappa}_1^2, \bar{\kappa}_2^2$, where:

$$\begin{aligned}\bar{\ell}_0 &= +\bar{\kappa}_0+\bar{\kappa}_1+\bar{\kappa}_2\\ \bar{\ell}_1 &= -\bar{\kappa}_0-\bar{\kappa}_1+\bar{\kappa}_2\\ \bar{\ell}_2 &= -\bar{\kappa}_0+\bar{\kappa}_1-\bar{\kappa}_2\\ \bar{\ell}_3 &= +\bar{\kappa}_0-\bar{\kappa}_1-\bar{\kappa}_2\end{aligned}$$

Proposition 4.7. $\mathbf{Deck}(\mathbb{Q}[\bar{\ell}_0,\bar{\ell}_1,\bar{\ell}_2,\bar{\ell}_3]/\mathbb{Q}) = \mathbf{Dih}\begin{pmatrix}\bar{\ell}_3 & \bar{\ell}_2\\ \bar{\ell}_0 & \bar{\ell}_1\end{pmatrix}$, where:

$$\bar{\ell}_0,\bar{\ell}_1,\bar{\ell}_2,\bar{\ell}_3 = 3^{\frac{1}{4}}, 3^{\frac{1}{4}}\mathrm{i}, -3^{\frac{1}{4}}, -3^{\frac{1}{4}}\mathrm{i}$$

Proof. Realize $\mathbb{Q}[\bar{\ell}_0,\bar{\ell}_1,\bar{\ell}_2,\bar{\ell}_3]/\mathbb{Q}$ as a universal splitting map of:

$$l(x) = x^4 - 3$$

(1) As $l(x) \in \mathbb{Q}[x]$ is irreducible, $\mathbf{Deck}(\mathbb{Q}[\bar{\ell}_0,\bar{\ell}_1,\bar{\ell}_2,\bar{\ell}_3]/\mathbb{Q})$ is transitive on $\bar{\ell}_0,\bar{\ell}_1,\bar{\ell}_2,\bar{\ell}_3$.

(2) As $\mathbf{Disc}(l(x)) = -6912 \notin \mathbb{Q}^2$, $\mathbf{Deck}(\mathbb{Q}[\bar{\ell}_0,\bar{\ell}_1,\bar{\ell}_2,\bar{\ell}_3]/\mathbb{Q}) \not\leq \mathbf{Alt}(\bar{\ell}_0,\bar{\ell}_1,\bar{\ell}_2,\bar{\ell}_3)$.

(3) As $\bar{\ell}_0\bar{\ell}_1+\bar{\ell}_2\bar{\ell}_3 = +2\sqrt{-3} \notin \mathbb{Q}$, $\mathbf{Deck}(\mathbb{Q}[\bar{\ell}_0,\bar{\ell}_1,\bar{\ell}_2,\bar{\ell}_3]/\mathbb{Q}) \not\leq \mathbf{Dih}\begin{pmatrix}\bar{\ell}_3 & \bar{\ell}_1\\ \bar{\ell}_0 & \bar{\ell}_2\end{pmatrix}$.

(4) As $\bar{\ell}_0\bar{\ell}_2+\bar{\ell}_1\bar{\ell}_3 = 0 \in \mathbb{Q}$, $\mathbf{Deck}(\mathbb{Q}[\bar{\ell}_0,\bar{\ell}_1,\bar{\ell}_2,\bar{\ell}_3]/\mathbb{Q}) \leq \mathbf{Dih}\begin{pmatrix}\bar{\ell}_3 & \bar{\ell}_2\\ \bar{\ell}_0 & \bar{\ell}_1\end{pmatrix}$.

(5) As $\bar{\ell}_0\bar{\ell}_3+\bar{\ell}_1\bar{\ell}_2 = -2\sqrt{-3} \notin \mathbb{Q}$, $\mathbf{Deck}(\mathbb{Q}[\bar{\ell}_0,\bar{\ell}_1,\bar{\ell}_2,\bar{\ell}_3]/\mathbb{Q}) \not\leq \mathbf{Dih}\begin{pmatrix}\bar{\ell}_2 & \bar{\ell}_3\\ \bar{\ell}_0 & \bar{\ell}_1\end{pmatrix}$.

By **tower theorem**, $\mathbf{Deck}(\mathbb{Q}[\bar{\ell}_0,\bar{\ell}_1,\bar{\ell}_2,\bar{\ell}_3]/\mathbb{Q}) = \mathbf{Dih}\begin{pmatrix}\bar{\ell}_3 & \bar{\ell}_2\\ \bar{\ell}_0 & \bar{\ell}_1\end{pmatrix}$ instead of $\langle(\bar{\ell}_0,\bar{\ell}_1,\bar{\ell}_2,\bar{\ell}_3)\rangle$.

□

Proposition 4.8. $\mathbf{Deck}(\mathbb{Q}[\bar{\ell}_0,\bar{\ell}_1,\bar{\ell}_2,\bar{\ell}_3]/\mathbb{Q}) = \mathbf{Alt}(\bar{\ell}_0,\bar{\ell}_1,\bar{\ell}_2,\bar{\ell}_3)$, where:

$$\begin{gathered}\zeta = \mathrm{e}^{\frac{2\pi\mathrm{i}}{7}}\\ \bar{\kappa}_0,\bar{\kappa}_1,\bar{\kappa}_2 = \sqrt{\zeta+\zeta^6}, \sqrt{\zeta^2+\zeta^5}, \sqrt{\zeta^4+\zeta^3} \text{ with } \mathbf{Im}(\bar{\kappa}_0,\bar{\kappa}_1,\bar{\kappa}_2) \geq 0\\ \bar{\ell}_0,\bar{\ell}_1,\bar{\ell}_2,\bar{\ell}_3 = +\bar{\kappa}_0+\bar{\kappa}_1+\bar{\kappa}_2, -\bar{\kappa}_0-\bar{\kappa}_1+\bar{\kappa}_2, -\bar{\kappa}_0+\bar{\kappa}_1-\bar{\kappa}_2, +\bar{\kappa}_0-\bar{\kappa}_1-\bar{\kappa}_2\end{gathered}$$

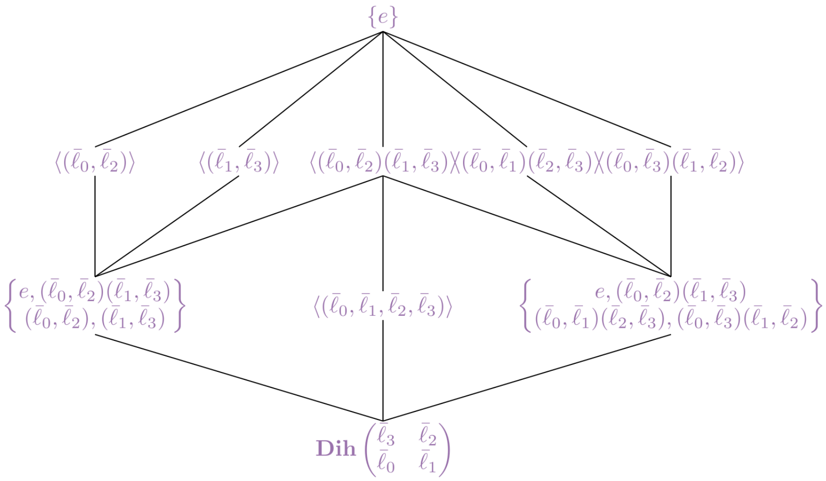
$\{e\}$
$\langle(\bar{\ell}_0,\bar{\ell}_2)\rangle$
$\langle(\bar{\ell}_1,\bar{\ell}_3)\rangle$
$\langle(\bar{\ell}_0,\bar{\ell}_2)(\bar{\ell}_1,\bar{\ell}_3)\rangle\langle(\bar{\ell}_0,\bar{\ell}_1)(\bar{\ell}_2,\bar{\ell}_3)\rangle\langle(\bar{\ell}_0,\bar{\ell}_3)(\bar{\ell}_1,\bar{\ell}_2)\rangle$
$\left\{\begin{matrix} e,(\bar{\ell}_0,\bar{\ell}_2)(\bar{\ell}_1,\bar{\ell}_3) \\ (\bar{\ell}_0,\bar{\ell}_2),(\bar{\ell}_1,\bar{\ell}_3) \end{matrix}\right\}$
$\langle(\bar{\ell}_0,\bar{\ell}_1,\bar{\ell}_2,\bar{\ell}_3)\rangle$
$\left\{\begin{matrix} e,(\bar{\ell}_0,\bar{\ell}_2)(\bar{\ell}_1,\bar{\ell}_3) \\ (\bar{\ell}_0,\bar{\ell}_1)(\bar{\ell}_2,\bar{\ell}_3),(\bar{\ell}_0,\bar{\ell}_3)(\bar{\ell}_1,\bar{\ell}_2) \end{matrix}\right\}$
$\mathbf{Dih}\begin{pmatrix} \bar{\ell}_3 & \bar{\ell}_2 \\ \bar{\ell}_0 & \bar{\ell}_1 \end{pmatrix}$

Figure 8: The Subgroup Lattice in **Proposition 4.7.**

Proof. Realize $\mathbb{Q}[\bar{\ell}_0,\bar{\ell}_1,\bar{\ell}_2,\bar{\ell}_3]/\mathbb{Q}$ as a universal splitting map of:

$$l(x) = x^4 + 2x^2 + 8x + 9$$

(1) As $l(x) \in \mathbb{Q}[x]$ is irreducible, $\mathbf{Deck}(\mathbb{Q}[\bar{\ell}_0,\bar{\ell}_1,\bar{\ell}_2,\bar{\ell}_3]/\mathbb{Q})$ is transitive on $\bar{\ell}_0,\bar{\ell}_1,\bar{\ell}_2,\bar{\ell}_3$.

(2) As $\mathbf{Disc}(l(x)) = 200704 \in \mathbb{Q}^2$, $\mathbf{Deck}(\mathbb{Q}[\bar{\ell}_0,\bar{\ell}_1,\bar{\ell}_2,\bar{\ell}_3]/\mathbb{Q}) \leq \mathbf{Alt}(\bar{\ell}_0,\bar{\ell}_1,\bar{\ell}_2,\bar{\ell}_3)$.

(3) As $\bar{\kappa}_0^2 = \zeta + \zeta^6 \notin \mathbb{Q}$, $\mathbf{Deck}(\mathbb{Q}[\bar{\ell}_0,\bar{\ell}_1,\bar{\ell}_2,\bar{\ell}_3]/\mathbb{Q}) \not\leq \mathbf{Dih}\begin{pmatrix} \bar{\ell}_2 & \bar{\ell}_3 \\ \bar{\ell}_0 & \bar{\ell}_1 \end{pmatrix}$.

(4) As $\bar{\kappa}_1^2 = \zeta^2 + \zeta^5 \notin \mathbb{Q}$, $\mathbf{Deck}(\mathbb{Q}[\bar{\ell}_0,\bar{\ell}_1,\bar{\ell}_2,\bar{\ell}_3]/\mathbb{Q}) \not\leq \mathbf{Dih}\begin{pmatrix} \bar{\ell}_3 & \bar{\ell}_2 \\ \bar{\ell}_0 & \bar{\ell}_1 \end{pmatrix}$.

(5) As $\bar{\kappa}_2^2 = \zeta^4 + \zeta^3 \notin \mathbb{Q}$, $\mathbf{Deck}(\mathbb{Q}[\bar{\ell}_0,\bar{\ell}_1,\bar{\ell}_2,\bar{\ell}_3]/\mathbb{Q}) \not\leq \mathbf{Dih}\begin{pmatrix} \bar{\ell}_3 & \bar{\ell}_1 \\ \bar{\ell}_0 & \bar{\ell}_2 \end{pmatrix}$.

Hence, $\mathbf{Deck}(\mathbb{Q}[\bar{\ell}_0,\bar{\ell}_1,\bar{\ell}_2,\bar{\ell}_3]/\mathbb{Q}) = \mathbf{Alt}(\bar{\ell}_0,\bar{\ell}_1,\bar{\ell}_2,\bar{\ell}_3)$. □

Proposition 4.9. $\mathbf{Deck}(\mathbb{Q}[\bar{\ell}_0,\bar{\ell}_1,\bar{\ell}_2,\bar{\ell}_3]/\mathbb{Q}) = \mathbf{Sym}(\bar{\ell}_0,\bar{\ell}_1,\bar{\ell}_2,\bar{\ell}_3)$, where:

$$\zeta = \mathrm{e}^{\frac{2\pi \mathrm{i}}{3}}$$

$$\bar{\kappa}_0,\bar{\kappa}_1,\bar{\kappa}_2 = \sqrt{3^{\frac{4}{3}} + 3^{\frac{5}{3}}}, \sqrt{3^{\frac{4}{3}}\zeta + 3^{\frac{5}{3}}\zeta^2}, \sqrt{3^{\frac{4}{3}}\zeta^2 + 3^{\frac{5}{3}}\zeta} \text{ with } \mathbf{Re}(\bar{\kappa}_0,\bar{\kappa}_1,\bar{\kappa}_2) \geq 0$$

$$\bar{\ell}_0,\bar{\ell}_1,\bar{\ell}_2,\bar{\ell}_3 = +\bar{\kappa}_0 + \bar{\kappa}_1 + \bar{\kappa}_2, -\bar{\kappa}_0 - \bar{\kappa}_1 + \bar{\kappa}_2, -\bar{\kappa}_0 + \bar{\kappa}_1 - \bar{\kappa}_2, +\bar{\kappa}_0 - \bar{\kappa}_1 - \bar{\kappa}_2$$

Proof. Realize $\mathbb{Q}[\bar{\ell}_0,\bar{\ell}_1,\bar{\ell}_2,\bar{\ell}_3]/\mathbb{Q}$ as a universal splitting map of:

$$l(x) = x^4 - 144x + 324$$

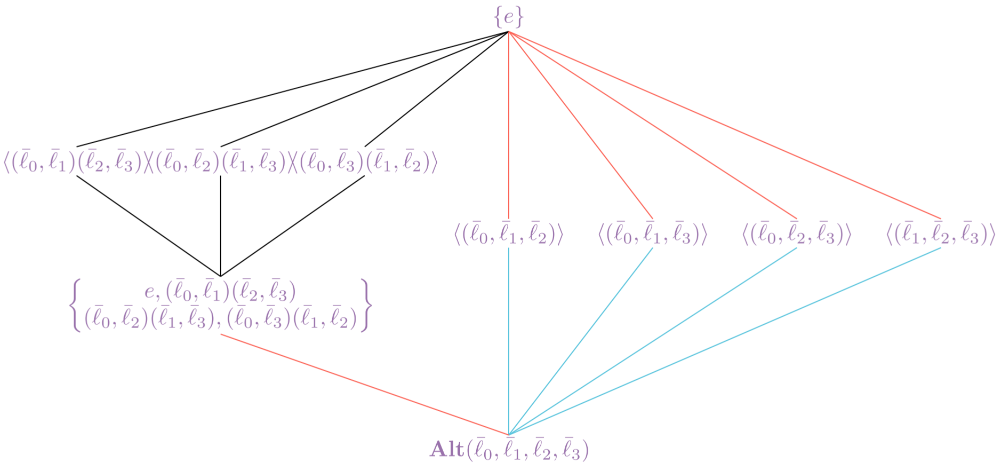
$\{e\}$
$\langle(\bar\ell_0,\bar\ell_1)(\bar\ell_2,\bar\ell_3)\rangle\langle(\bar\ell_0,\bar\ell_2)(\bar\ell_1,\bar\ell_3)\rangle\langle(\bar\ell_0,\bar\ell_3)(\bar\ell_1,\bar\ell_2)\rangle$
$\langle(\bar\ell_0,\bar\ell_1,\bar\ell_2)\rangle$
$\langle(\bar\ell_0,\bar\ell_1,\bar\ell_3)\rangle$
$\langle(\bar\ell_0,\bar\ell_2,\bar\ell_3)\rangle$
$\langle(\bar\ell_1,\bar\ell_2,\bar\ell_3)\rangle$
$\left\{\begin{matrix} e,(\bar\ell_0,\bar\ell_1)(\bar\ell_2,\bar\ell_3)\\ (\bar\ell_0,\bar\ell_2)(\bar\ell_1,\bar\ell_3),(\bar\ell_0,\bar\ell_3)(\bar\ell_1,\bar\ell_2)\end{matrix}\right\}$
$\mathbf{Alt}(\bar\ell_0,\bar\ell_1,\bar\ell_2,\bar\ell_3)$

Figure 9: The Subgroup Lattice in **Proposition 4.8.**

(1) As $l(x)\in\mathbb{Q}[x]$ is irreducible, $\mathbf{Deck}(\mathbb{Q}[\bar\ell_0,\bar\ell_1,\bar\ell_2,\bar\ell_3]/\mathbb{Q})$ is transitive on $\bar\ell_0,\bar\ell_1,\bar\ell_2,\bar\ell_3$.

(2) As $\mathbf{Disc}(l(x))=-2902376448\notin\mathbb{Q}^2$, $\mathbf{Deck}(\mathbb{Q}[\bar\ell_0,\bar\ell_1,\bar\ell_2,\bar\ell_3]/\mathbb{Q})\not\leq\mathbf{Alt}(\bar\ell_0,\bar\ell_1,\bar\ell_2,\bar\ell_3)$.

(3) As $\bar\kappa_0^2=3^{\frac{4}{3}}+3^{\frac{5}{3}}\notin\mathbb{Q}$, $\mathbf{Deck}(\mathbb{Q}[\bar\ell_0,\bar\ell_1,\bar\ell_2,\bar\ell_3]/\mathbb{Q})\not\leq\mathbf{Dih}\begin{pmatrix}\bar\ell_2 & \bar\ell_3\\ \bar\ell_0 & \bar\ell_1\end{pmatrix}$.

(4) As $\bar\kappa_1^2=3^{\frac{4}{3}}\zeta+3^{\frac{5}{3}}\zeta^2\notin\mathbb{Q}$, $\mathbf{Deck}(\mathbb{Q}[\bar\ell_0,\bar\ell_1,\bar\ell_2,\bar\ell_3]/\mathbb{Q})\not\leq\mathbf{Dih}\begin{pmatrix}\bar\ell_3 & \bar\ell_2\\ \bar\ell_0 & \bar\ell_1\end{pmatrix}$.

(5) As $\bar\kappa_2^2=3^{\frac{4}{3}}\zeta^2+3^{\frac{5}{3}}\zeta\notin\mathbb{Q}$, $\mathbf{Deck}(\mathbb{Q}[\bar\ell_0,\bar\ell_1,\bar\ell_2,\bar\ell_3]/\mathbb{Q})\not\leq\mathbf{Dih}\begin{pmatrix}\bar\ell_3 & \bar\ell_1\\ \bar\ell_0 & \bar\ell_2\end{pmatrix}$.

Hence, $\mathbf{Deck}(\mathbb{Q}[\bar\ell_0,\bar\ell_1,\bar\ell_2,\bar\ell_3]/\mathbb{Q})=\mathbf{Sym}(\bar\ell_0,\bar\ell_1,\bar\ell_2,\bar\ell_3)$. □

4.4 Cyclotomic Polynomial

Definition 4.10. (**Möbius Transformation**)
Let K be a field, and k_m,l_m be nonzero K-sequences over $m\geq 1$.
Define the Möbius transformation between k_m and l_m as:

$$k_m=\prod_{n|m}l_n \iff l_m=\prod_{n|m}k_n^{\mu(\frac{m}{n})}$$

Here, for all $m\geq 1$:

(1) If m is a product of $n\geq 0$ distinct primes, then $\mu(m)=(-1)^n$.

(2) If m is divisible by the square of a prime, then $\mu(m)=0$.

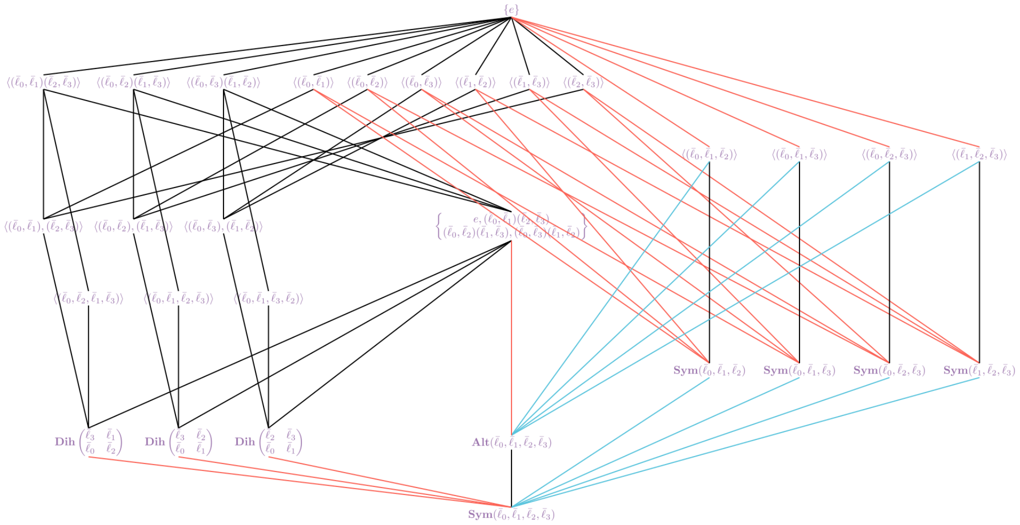
$\{e\}$
$\langle(\bar\ell_0,\bar\ell_1)(\bar\ell_2,\bar\ell_3)\rangle$
$\langle(\bar\ell_0,\bar\ell_2)(\bar\ell_1,\bar\ell_3)\rangle$
$\langle(\bar\ell_0,\bar\ell_3)(\bar\ell_1,\bar\ell_2)\rangle$
$\langle(\bar\ell_0,\bar\ell_1)\rangle$
$\langle(\bar\ell_0,\bar\ell_2)\rangle$
$\langle(\bar\ell_0,\bar\ell_3)\rangle$
$\langle(\bar\ell_1,\bar\ell_2)\rangle$
$\langle(\bar\ell_1,\bar\ell_3)\rangle$
$\langle(\bar\ell_2,\bar\ell_3)\rangle$
$\langle(\bar\ell_0,\bar\ell_1,\bar\ell_2)\rangle$
$\langle(\bar\ell_0,\bar\ell_1,\bar\ell_3)\rangle$
$\langle(\bar\ell_0,\bar\ell_2,\bar\ell_3)\rangle$
$\langle(\bar\ell_1,\bar\ell_2,\bar\ell_3)\rangle$
$\langle(\bar\ell_0,\bar\ell_1),(\bar\ell_2,\bar\ell_3)\rangle$
$\langle(\bar\ell_0,\bar\ell_2),(\bar\ell_1,\bar\ell_3)\rangle$
$\langle(\bar\ell_0,\bar\ell_3),(\bar\ell_1,\bar\ell_2)\rangle$
$\left\{\begin{matrix} e,(\bar\ell_0,\bar\ell_1)(\bar\ell_2,\bar\ell_3) \\ (\bar\ell_0,\bar\ell_2)(\bar\ell_1,\bar\ell_3),(\bar\ell_0,\bar\ell_3)(\bar\ell_1,\bar\ell_2)\end{matrix}\right\}$
$\langle(\bar\ell_0,\bar\ell_2,\bar\ell_1,\bar\ell_3)\rangle$
$\langle(\bar\ell_0,\bar\ell_1,\bar\ell_2,\bar\ell_3)\rangle$
$\langle(\bar\ell_0,\bar\ell_1,\bar\ell_3,\bar\ell_2)\rangle$
$\mathbf{Sym}(\bar\ell_0,\bar\ell_1,\bar\ell_2)$
$\mathbf{Sym}(\bar\ell_0,\bar\ell_1,\bar\ell_3)$
$\mathbf{Sym}(\bar\ell_0,\bar\ell_2,\bar\ell_3)$
$\mathbf{Sym}(\bar\ell_1,\bar\ell_2,\bar\ell_3)$
$\mathbf{Dih}\begin{pmatrix}\bar\ell_3 & \bar\ell_1 \\ \bar\ell_0 & \bar\ell_2\end{pmatrix}$
$\mathbf{Dih}\begin{pmatrix}\bar\ell_3 & \bar\ell_2 \\ \bar\ell_0 & \bar\ell_1\end{pmatrix}$
$\mathbf{Dih}\begin{pmatrix}\bar\ell_2 & \bar\ell_3 \\ \bar\ell_0 & \bar\ell_1\end{pmatrix}$
$\mathbf{Alt}(\bar\ell_0,\bar\ell_1,\bar\ell_2,\bar\ell_3)$
$\mathbf{Sym}(\bar\ell_0,\bar\ell_1,\bar\ell_2,\bar\ell_3)$

Figure 10: The Subgroup Lattice in **Proposition 4.9.**

Definition 4.11. (**Cyclotomic Polynomial**)
Let K be a field, and $m \geq 1$. Define the m^{th}-cyclotomic polynomial over K as:

$$x^m - 1 = \prod_{n|m} \Phi_n(x) \iff \Phi_m(x) = \prod_{n|m} (x^n - 1)^{\mu(\frac{m}{n})}$$

Remark: $k(x)^{-1}$ is taken in $K(\!(x)\!)$. According to geometric series, $\Phi_m(x)$ is an integer coefficient formal power series. We factorize it and show that it is of degree $\varphi(m)$.

Proposition 4.12. (**Factorization of $\Phi_m(x)$**)
Let K be a field, $m \geq 1$, and $\zeta \in K^\times$ be of order m.

$$\Phi_m(x) = \prod_{(m,n)=1} (x - \zeta^n)$$

Proof. We prove by induction on the degree m of $x^m - 1$.
Basis Step: When $m = 1$, $\zeta = 1$ and $\Phi_1(x) = x - 1$.
Inductive Hypothesis: For all $s \geq 1$, when $1 \leq m \leq s$, assume the statement.
Inductive Step: When $m = s + 1$, according to **Möbius transformation**:

$$\Phi_m(x) = \frac{x^m - 1}{\prod_{k|m, k \neq m} \Phi_k(x)} = \frac{\prod_k (x - \zeta^k)}{\prod_{(m,n)\neq 1} (x - \zeta^n)} = \prod_{(m,n)=1} (x - \zeta^n)$$

□

Remark: When the characteristic 0 or p of K doesn't divide m, we may extend K if necessary, such that there exists $\zeta \in K^\times$ of order m. This shows that $\Phi_m(x)$ is of degree $\varphi(m)$. However, if the characteristic p of K divides m, then write m as $p^k l$, where $k \geq 1$ is maximal. For all $\zeta \in K^\times$, $(\zeta^l - 1)^{p^k} = \zeta^m - 1 = 0$ implies $\zeta^l - 1 = 0$, so ζ fails to have order m. We need another approach to study the degree of $\Phi_m(x)$.

Proposition 4.13. (**Factorization of** $\Phi_m(x^p)$)
Let K be a field, $m \geq 1$, and p be prime.

$$\Phi_m(x^p) = \begin{cases} \Phi_{pm}(x) & \text{if} \quad p \mid m; \\ \Phi_m(x)\Phi_{pm}(x) & \text{if} \quad p \nmid m; \end{cases}$$

Proof. According to **Möbius transformation**:

$$\Phi_m(x^p) = \prod_{n|m}(x^{pn} - 1)^{\mu(\frac{m}{n})} = \prod_{p|k|pm}(x^k - 1)^{\mu(\frac{pm}{k})}$$

This motivates us to consider the decomposition below:

$$\prod_{k|pm}(x^k - 1)^{\mu(\frac{pm}{k})} = \prod_{p|k|pm}(x^k - 1)^{\mu(\frac{pm}{k})} \prod_{p\nmid k|pm}(x^k - 1)^{\mu(\frac{pm}{k})}$$

(1) If $p \mid m$, then $p \nmid k \mid pm$ implies $\mu(\frac{pm}{k}) = 0$, so:

$$\Phi_{pm}(x) = \Phi_m(x^p)$$

(2) If $p \nmid m$, then $p \nmid k \mid pm$ iff $k \mid m$, and $\mu(\frac{pm}{k}) = -\mu(\frac{m}{k})$, so:

$$\Phi_{pm}(x) = \Phi_m(x^p)\Phi_m(x)^{-1}$$

□

Remark: When the characteristic p of K divides m, then write m as $p^k l$, where $k \geq 1$ is maximal. It follows from $\Phi_m(x) = \Phi_l(x)^{p^k - p^{k-1}}$ that $\Phi_m(x)$ is of degree $\varphi(m)$. As $\Phi_m(x)$ is indeed a polynomial instead of a formal power series, we may do evaluation.

Proposition 4.14. (**Evaluation of** $\Phi_m(x)$)
Let K be a field, and $m \geq 1$.

$$\Phi_m(0) = \begin{cases} -1 & \text{if} \quad m = 1; \\ 1 & \text{if} \quad m \geq 2; \end{cases}$$

$$\Phi_m(1) = \begin{cases} 0 & \text{if} \quad m = 1; \\ p & \text{if} \quad \exists k \geq 1, \exists \text{ prime } p, m = p^k; \\ 1 & \text{if} \quad \text{otherwise}; \end{cases}$$

Proof. We may divide our proof into three parts.

(1) We evaluate $\Phi_m(0)$.
Basis Step: When $m = 1$, $\Phi_1(x) = x - 1$, $\Phi_1(0) = -1$.
Inductive Hypothesis: For all $s \geq 1$, when $1 \leq m \leq s$, assume the statement.
Inductive Step: When $m = s + 1$:

$$\Phi_m(0) = \frac{0^m - 1}{\prod_{n|m,n\neq m} \Phi_n(0)} = \frac{-1}{-1} = 1$$

(2) We evaluate $\Phi_m(1)$ when the characteristic 0 or p of K doesn't divide m.
Basis Step: When $m = 1$, $\Phi_1(x) = x - 1$, $\Phi_1(1) = 0$.
When $m = q^k$, where $k \geq 1$ and q is prime, $\Phi_m(x) = \frac{x^{q^k}-1}{x^{q^{k-1}}-1}$, $\Phi_m(1) = q$.
Inductive Hypothesis: For all $s \geq 1$, when $p \nmid m$, and m has at most s factors, assume the statement. Note that these factors are invertible in K.
Inductive Step: When $p \nmid m$, and m has $s+1$ factors $q_0, \cdots, q_s$, assume that m has a prime factorization $m = q_0^{k_0} \cdots q_t^{k_t}$. According to **Möbius transformation**:

$$\Phi_m(1) = \frac{m}{\prod_{n|m,n\neq 1,n\neq m} \Phi_n(1)} = \frac{q_0^{k_0} \cdots q_s^{k_s}}{q_0^{k_0} \cdots q_s^{k_s}} = 1$$

(3) We evaluate $\Phi_m(1)$ when the characteristic p of K divides m.
Write m as $p^k l$, where $k \geq 1$ is maximal.

$$\Phi_m(1) = \Phi_l(1)^{p^k - p^{k-1}} = \left\{ \begin{array}{lll} p & \text{if} & l = 1, m = p^k; \\ 1 & \text{if} & \text{otherwise;} \end{array} \right.$$

□

Remark: Let $m, n \geq 2$, $m \nmid n$, and $n \nmid m$. We wish to show that:

$$\exists u(x), v(x) \in \mathbb{Z}[x], u(x)\Phi_m(x) + v(x)\Phi_n(x) = 1$$

To see this, it suffices to show that:

$$\textbf{Res}(\Phi_m(x), \Phi_n(x)) = 1$$

Proposition 4.15. (**Resultant of** $\Phi_m(x), \Phi_n(x)$)
Let $m, n \geq 1$, $m \nmid n$, and $n \nmid m$.

$$\textbf{Res}(\Phi_m(x), \Phi_n(x)) = 1$$

Proof. Assume that the greatest common divisor of m, n is $(m, n) \geq 1$.
It follows from **Möbius transformation** that:

$$\frac{x^m - 1}{x^{(m,n)} - 1}, \frac{x^n - 1}{x^{(m,n)} - 1} = \prod_{k|m,k\nmid(m,n)} \Phi_k(x), \prod_{l|n,l\nmid(m,n)} \Phi_l(x)$$

It follows from **Euclid algorithm** on m, n and $\frac{x^m-1}{x^{(m,n)}-1}, \frac{x^n-1}{x^{(m,n)}-1}$ that:

$$\mathbf{Res}\left(\frac{x^m-1}{x^{(m,n)}-1}, \frac{x^n-1}{x^{(m,n)}-1}\right) = 1$$

We prove by induction, first on the upperbound $\gamma \geq 1$ of (m, n), then on the sum of $\alpha = \#(k : k \mid m, k \nmid (m,n)), \beta = \#(l : l \mid n, l \nmid (m,n))$. As $m \nmid n$ and $n \nmid m$, $\alpha + \beta \geq 2$.

(1) **Basis Step of γ:**
When $\gamma = 1$, $(m, n) = 1$,
so for all $k \mid m, k \nmid 1$ and $l \mid n, l \nmid 1$, $k \nmid l$ and $l \nmid k$ and $(k, l) = 1$.

(1.1) **Basis Step of $\alpha + \beta$ When $\gamma = 1$:**
When $\alpha + \beta = 2$, $\alpha = \beta = 1$, so:

$$\frac{x^m-1}{x-1} = \Phi_m(x), \frac{x^n-1}{x-1} = \Phi_n(x)$$
$$\mathbf{Res}(\Phi_m(x), \Phi_n(x)) = \mathbf{Res}\left(\frac{x^m-1}{x-1}, \frac{x^n-1}{x-1}\right) = 1$$

(1.2) **Inductive Hypothesis of $\alpha + \beta$ When $\gamma = 1$:**
For all $\mu \geq 2$, when $\alpha + \beta \leq \mu$, assume the statement.

(1.3) **Inductive Step of $\alpha + \beta$ When $\gamma = 1$:**
When $\alpha + \beta = \mu + 1$, for all $k \mid m, k \nmid 1$ and $l \mid n, l \nmid 1$:
Case 1: $(k, l) = 1$ and ($k \neq m$ or $l \neq n$).
Strategy 1: Apply the **inductive hypothesis of $\alpha + \beta$ when** $\gamma = 1$.
Hence, separate the leading term $(k, l) = (m, n)$:

$$\mathbf{Res}(\Phi_m(x), \Phi_n(x)) = \frac{\mathbf{Res}\left(\frac{x^m-1}{x-1}, \frac{x^n-1}{x-1}\right)}{\prod_{k\neq m \text{ or } l\neq n} \mathbf{Res}(\Phi_k(x), \Phi_l(x))} = \frac{1}{1} = 1$$

(2) **Inductive Hypothesis of γ:**
For all $\sigma \geq 1$, when $\gamma = \sigma$, regardless of α, β, assume the statement.

(3) **Inductive Step of γ:**
When $\gamma = \sigma + 1$, $(m, n) \leq \sigma + 1$,
so for all $k \mid m, k \nmid (m, n)$ and $l \mid n, l \nmid (m, n)$, $k \nmid l$ and $l \nmid k$ and $(k, l) \leq \sigma + 1$.

(3.1) **Basis Step of $\alpha + \beta$ When $\gamma = \sigma + 1$:**
When $\alpha + \beta = 2$, $\alpha = \beta = 1$, so:

$$\frac{x^m-1}{x^{(m,n)}-1} = \Phi_m(x), \frac{x^n-1}{x^{(m,n)}-1} = \Phi_n(x)$$
$$\mathbf{Res}(\Phi_m(x), \Phi_n(x)) = \mathbf{Res}\left(\frac{x^m-1}{x^{(m,n)}-1}, \frac{x^n-1}{x^{(m,n)}-1}\right) = 1$$

(3.2) **Inductive Hypothesis of $\alpha + \beta$ When $\gamma = \sigma + 1$:**
For all $\mu \geq 2$, when $\alpha + \beta \leq \mu$, assume the statement.

(3.3) **Inductive Step of α, β When $\gamma = \sigma + 1$:**
When $\alpha + \beta = \mu + 1$, for all $k \mid m, k \nmid (m, n)$ and $l \mid n, l \nmid (m, n)$:
Case 1: $(k, l) = \sigma + 1$ and $(k \neq m$ or $l \neq n)$.
Strategy 1: Apply the **inductive hypothesis of $\alpha + \beta$ when $\gamma = \sigma + 1$**.
Case 2: $(k, l) \leq \sigma$.
Strategy 2: Apply the **inductive hypothesis of γ**.
Hence, separate the leading term $(k, l) = (m, n)$:

$$\mathbf{Res}(\Phi_m(x), \Phi_n(x)) = \frac{\mathbf{Res}\left(\frac{x^m-1}{x^g-1}, \frac{x^n-1}{x^g-1}\right)}{\prod_{k \neq m \text{ or } l \neq n} \mathbf{Res}(\Phi_k(x), \Phi_l(x))} = \frac{1}{1} = 1$$

□

Remark: Therefore, $\Phi_n(x)$ is a special integer coefficient linear combination. We only prove the case where n is a product of distinct primes, and the general case is similar.

Proposition 4.16. Let p_k be $m \geq 2$ distinct primes, and $n_K = \prod_{k \notin K} p_k$.

$$\exists u_k(x) \in \mathbb{Z}[x], \sum_{0 \leq k \leq m-1} u_k(x) \frac{x^n - 1}{x^{n_k} - 1} = \Phi_n(x)$$

Proof. We prove the statement by induction on m.
Basis Step: When $m = 2$, the equation reduces to:

$$u_0(x) \frac{x^{p_0} - 1}{x - 1} + u_1(x) \frac{x^{p_1} - 1}{x - 1} = 1$$

Inductive Hypothesis: For all $s \geq 2$, when $m = s$, assume the statement.
Inductive Step: When $m = s + 1$:

(1) According to **inductive hypothesis**, for some $u_k(x) \in \mathbb{Z}[x]$:

$$\begin{aligned} \sum_{k \neq m-1} u_k(x) \frac{x^{n_{m-1}} - 1}{x^{n_{k,m-1}} - 1} &= \Phi_{n_{m-1}}(x) \\ \sum_{k \neq m-1} u_k(x^{p_{m-1}}) \frac{x^n - 1}{x^{n_k} - 1} &= \Phi_{n_{m-1}}(x^{p_{m-1}}) \\ &= \Phi_{n_{m-1}}(x) \Phi_n(x) \end{aligned}$$

(2) According to **inductive hypothesis**, for some $v_k(x) \in \mathbb{Z}[x]$:

$$\begin{aligned} \sum_{k \neq 0} v_k(x) \frac{x^{n_0} - 1}{x^{n_{0,k}} - 1} &= \Phi_{n_0}(x) \\ \sum_{k \neq 0} v_k(x^{p_0}) \frac{x^n - 1}{x^{n_k} - 1} &= \Phi_{n_0}(x^{p_0}) \\ &= \Phi_{n_0}(x) \Phi_n(x) \end{aligned}$$

(3) As $\mathbf{Res}(\Phi_{n_{m-1}}(x), \Phi_{n_0}(x)) = 1$, for some $w_{m-1}(x), w_0(x) \in \mathbb{Z}[x]$:

$$\begin{aligned} w_{m-1}(x)\Phi_{n_{m-1}}(x) + w_0(x)\Phi_{n_0}(x) &= 1 \\ w_{m-1}(x) \sum_{k \neq m-1} u_k(x^{p_{m-1}}) \frac{x^n - 1}{x^{n_k} - 1} + w_0(x) \sum_{k \neq 0} v_k(x^{p_0}) \frac{x^n - 1}{x^{n_k} - 1} &= 1 \end{aligned}$$

□

Remark: The combinatorial properties before show that $x^m - 1 \in \mathbb{Z}[x]$ is far from irreducible. We show that $\Phi_m(x) \in \mathbb{Z}[x]$ is already irreducible, and every Abelian group G is embedded in a cyclotomic deck transformation group $\mathbf{Deck}(\mathbb{Q}[\mathrm{e}^{\frac{2\pi \mathrm{i}}{n}}]/\mathbb{Q})$.

Proposition 4.17. Let $m \geq 1$. $\Phi_m(x) \in \mathbb{Z}[x]$ is irreducible.

Proof. As $\Phi_m(x)$ is monic, it suffices to show that:

$$\begin{aligned} \forall \text{ irreducible monic } f_1(x) \mid \Phi_m(x), \\ \forall \text{ prime } p \nmid m, \\ \forall \xi_0 \in \mathbb{C}, \\ f_1(\xi_0) = \bar{0} \text{ implies } f_1(\xi_0^p) = \bar{0} \end{aligned}$$

Consider the diagram below:

$$\begin{tikzcd}
(\bar{R}, \xi_0, \cdots, \xi_{\varphi(m)-1}) \arrow[r, dashed, "\exists ! \bar{\sigma}"] & (\bar{S}, \eta_0, \cdots, \eta_{\varphi(m)-1}) \\
(R, f_1(x), \Phi_m(x)) \arrow[u, "\alpha"] \arrow[r, "\sigma"'] & (S, g_1(x), \Psi_m(x)) \arrow[u, "\beta"']
\end{tikzcd}$$

We explain the information of each vertex and each edge.

(1) $R = \mathbb{Z}$ is a Euclid domain, and $f_1(x)$ is the minimal polynomial of ξ_0 over R.

(2) $\bar{R} = R[\xi_0]$. We aim to reduce $\bar{R}$ to some field $\bar{S}$ modulo p.

(3) $\alpha : R \to \bar{R}$ is the inclusion map, which is a universal splitting map of $x^m - 1$.

(4) $S = \mathbf{GF}(p)$ is a field, where the quotient map $\sigma : R \to S$ sends the coefficients of $f_1(x), \Phi_m(x)$ to that of $g_1(x), \Psi_m(x)$. As $p \nmid m$, for some $n \geq 1$, $p^n \equiv 1 (\mathrm{mod}\ m)$.

(5) $\bar{S} = \mathbf{GF}(p^n)$ is a field, where $p^n \equiv 1(\mathrm{mod}\ m)$, so there exists $\eta_0 \in \bar{S}^\times$ of order m.

(6) $\beta : S \to \bar{S}$ is the inclusion map, which splits $\Phi_m(x)$ into some $\eta_0, \cdots, \eta_{\varphi(m)-1} \in \bar{S}^\times$ of order m. As $g_1(x) \mid \Psi_m(x)$, we may replace η_0 by a root of $g_1(x)$.

(7) As η_0 satisfies the minimal polynomial $f_1(x)$ of ξ_0 over R, σ has a unique lift $\bar{\sigma} : \bar{R} \to \bar{S}$ under α, β sending ξ_0 to η_0, so we may reduce $\bar{R}$ to $\bar{S}$ modulo p.

Assume to the contrary that $\Phi_m(x) = f_1(x)f_p(x)$, where $f_p(\xi_0^p) = \bar{0}$.
Reduce $\bar{R}$ to $\bar{S}$ modulo p, and we obtain $g_p(\eta_0)^p = g_p(\eta_0^p) = \bar{0}$, i.e., $g_p(\eta_0) = \bar{0}$.
This implies a contradiction where $p \nmid m$, $x^m - 1 \in S[x]$ is separable,
$g_1(x)g_p(x) = \Phi_m(x) \mid x^m - 1$, and $g_1(\eta_0) = g_p(\eta_0) = \bar{0}$. Hence, $f_1(\xi_0^p) = \bar{0}$. □

Remark: As a consequence, **Deck**$(\mathbb{Q}[\zeta]/\mathbb{Q}) = (\mathbb{Z}/m\mathbb{Z})^\times$. Recall from number theory that it is cyclic iff $m = 1, 2, 4, p^k, 2p^k$, where p is an odd prime and $k \geq 1$.

Example 4.18. **Deck**$(\mathbb{Q}[\bar{\kappa}_0, \bar{\kappa}_1, \bar{\kappa}_2, \bar{\kappa}_3, \bar{\kappa}_4, \bar{\kappa}_5]/\mathbb{Q})$=$\langle(\bar{\kappa}_0, \bar{\kappa}_1, \bar{\kappa}_2, \bar{\kappa}_3, \bar{\kappa}_4, \bar{\kappa}_5)\rangle$,where:

$$\zeta = \mathrm{e}^{\frac{2\pi \mathrm{i}}{7}}$$
$$\bar{\kappa}_0, \bar{\kappa}_1, \bar{\kappa}_2, \bar{\kappa}_3, \bar{\kappa}_4, \bar{\kappa}_5 = \zeta, \zeta^3, \zeta^2, \zeta^6, \zeta^4, \zeta^5$$

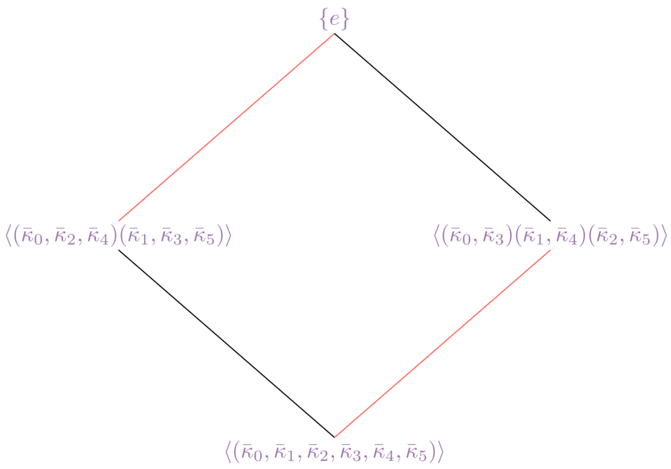
$\{e\}$
$\langle(\bar{\kappa}_0, \bar{\kappa}_2, \bar{\kappa}_4)(\bar{\kappa}_1, \bar{\kappa}_3, \bar{\kappa}_5)\rangle$
$\langle(\bar{\kappa}_0, \bar{\kappa}_3)(\bar{\kappa}_1, \bar{\kappa}_4)(\bar{\kappa}_2, \bar{\kappa}_5)\rangle$
$\langle(\bar{\kappa}_0, \bar{\kappa}_1, \bar{\kappa}_2, \bar{\kappa}_3, \bar{\kappa}_4, \bar{\kappa}_5)\rangle$

Figure 11: The Subgroup Lattice in **Example 4.18.**

Proposition 4.19. (**Simplified Dirichlet Theorem**)
For all $m \geq 0, n \geq 2$, there exist m distinct primes $p_k \equiv 1(\mathrm{mod}\ n)$.

Proof. We prove this statement by induction on m.
Basis Step: When $m = 0$, the statement is true.
Inductive Hypothesis: For all $s \geq 0$, when $m = s$, assume the statement.
Inductive Step: When $m = s + 1$, choose:

$$m - 1 \text{ distinct primes } p_k \equiv 1(\mathrm{mod}\ n)$$
$$\zeta = n \prod_{0 \leq k \leq m-2} p_k \geq 2$$
$$\text{prime divisor } q \text{ of } \Phi_n(\zeta) \geq 2$$

(1) As $n \geq 2$, the constant term of $\Phi_n(x)$ is 1, so q divides 1 plus some multiple of ζ, which implies q is distinct from the $m-1$ primes p_k, and $q \nmid n$.

(2) As $q \nmid n$, for some $l \geq 1$, $q^l \equiv 1(\text{mod } n)$, and the inclusion map $\sigma : \mathbf{GF}(q) \to \mathbf{GF}(q^l)$ splits $\Phi_n(x)$ into some $\zeta_0, \cdots, \zeta_{\varphi(n)-1} \in \mathbf{GF}(q^l)^\times$ of order n.

(3) As $q \mid \Phi_n(\zeta)$, ζ is one of $\zeta_0, \cdots, \zeta_{\varphi(n)-1}$, so $l = 1$ is enough,
and it follows from **Lagrange theorem** that $q \equiv 1(\text{mod } n)$.

□

Proposition 4.20. (**Kronecker-Weber Theorem**)
For all finite Abelian group G, for some $n \geq 1$, $G \leq \mathbf{Deck}(\mathbb{Q}[\mathrm{e}^{\frac{2\pi \mathrm{i}}{n}}]/\mathbb{Q})$.

Proof. According to **the classification theorem of finite Abelian groups**, for some unique $m \geq 0$, for some unique $d_0 \mid d_1 \mid \cdots \mid d_{m-2} \mid d_{m-1}$ greater than 1:

$$G \cong \frac{\mathbb{Z}}{d_0\mathbb{Z}} \oplus \frac{\mathbb{Z}}{d_1\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{d_{m-2}\mathbb{Z}} \oplus \frac{\mathbb{Z}}{d_{m-1}\mathbb{Z}}$$

According to **simplified Dirichlet theorem**, for some distinct primes $p_0, p_1, \cdots, p_{m-2}, p_{m-1}$:

$$p_0 \equiv 1(\text{mod } d_0), p_1 \equiv 1(\text{mod } d_1), \cdots, p_{m-2} \equiv 1(\text{mod } d_{m-2}), p_{m-1} \equiv 1(\text{mod } d_{m-1})$$

Hence, it suffices to choose $n = p_0 p_1 \cdots p_{m-2} p_{m-1} \geq 1$. □

4.5 Radicals

Definition 4.21. (**Kummer Homomorphism**)
Let $K, \bar{K}$ be fields, $p \neq \mathbf{Char}(K)$ be prime, and $\sigma : K \to \bar{K}$ be Galois.
If $\mathbf{Deck}(\sigma)$ is p-cyclic, then σ is p-Kummer.

Proposition 4.22. Let $K, \bar{K}$ be fields, $p \neq \mathbf{Char}(K)$ be prime, $\zeta \in K^\times$ be of order p, and $\sigma : K \to \bar{K}$ be Galois. TFAE:

(1) σ is p-Kummer.

(2) σ is a universal splitting map of some irreducible $x^p - k \in K[x]$.

Proof. We may divide our proof into two directions.
"if" direction:
Assume that σ is a universal splitting map of some irreducible $x^p - k \in K[x]$.
As $\zeta \in K^\times$ is of order p, σ splits the separable and irreducible $x^p - k$ into some $\bar{\kappa}, \cdots, \sigma(\zeta)^{p-1}\bar{\kappa} \in \bar{K}$ universally, so $\mathbf{Deck}(\sigma)$ of order p is generated by $(\bar{\kappa}, \cdots, \sigma(\zeta)^{p-1}\bar{\kappa})$.
"only if" direction:
Assume that $\mathbf{Deck}(\sigma)$ is generated by some $\bar{\tau} \in \mathbf{Deck}(\sigma)$ of order p.

As $\bar{\tau}^p - \bar{1} = \bar{0}$, and σ splits $x^p - 1$ into distinct $1, \cdots, \zeta^{p-1}$, $\bar{\tau}$ is diagonalizable.
As the fixed point set of $\bar{\tau}$ has K-dimension 1, and $\zeta \in K^\times$ is of prime order p, each root ζ^k of $x^p - 1$ is an eigenvalue of $\bar{\tau}$.
For all eigenvector $\bar{\kappa}$ of $\bar{\tau}$ with $(\bar{\tau} - \bar{1})(\bar{\kappa}) \neq \bar{0}$, $K[\bar{\kappa}] = \bar{K}$.
As $\bar{\tau}(\bar{\kappa}^p) = \bar{\kappa}^p$, for some $k \in K$, $\sigma(k) = \bar{\kappa}^p$.
Hence, σ is a universal splitting map of the irreducible polynomial $x^p - k \in K[x]$. □

Definition 4.23. (**Artin-Schreier Homomorphism**)
Let $K, \bar{K}$ be fields, $p = \mathbf{Char}(K)$ be prime, and $\sigma : K \to \bar{K}$ be Galois.
If $\mathbf{Deck}(\sigma)$ is p-cyclic, then σ is p-Artin-Schreier.

Proposition 4.24. Let $K, \bar{K}$ be fields, $p = \mathbf{Char}(K)$ be prime, and $\sigma : K \to \bar{K}$ be Galois. TFAE:

(1) σ is p-Artin-Schreier.

(2) σ is a universal splitting map of some irreducible $x^p - x - k \in K[x]$.

Proof. We may divide our proof into two directions.
"if" direction:
Assume that σ is a universal splitting map of some irreducible $x^p - x - k \in K[x]$.
As $1 \in K$ is of order p, σ splits the separable and irreducible $x^p - x - k$ into some $\bar{\kappa}, \cdots, \bar{\kappa} - \bar{1} \in \bar{K}$ universally, so $\mathbf{Deck}(\sigma)$ of order p is generated by $(\bar{\kappa}, \cdots, \bar{\kappa} - \bar{1})$.
"only if" direction:
Assume that $\mathbf{Deck}(\sigma)$ is generated by some $\bar{\tau} \in \mathbf{Deck}(\sigma)$ of order p.
As $(\bar{\tau} - \bar{1})^p = \bar{0}$, and the fixed point set of $\bar{\tau}$ has K-dimension 1,
the Jordan normal form of $\bar{\tau}$ has a unique Jordan block with eigenvalue 1.
For all generalized eigenvector $\bar{\kappa}$ of $\bar{\tau}$ with $(\bar{\tau} - \bar{1})^{p-1}(\bar{\kappa}) \neq \bar{0}$, $K[\bar{\kappa}] = \bar{K}$.
As $\bar{\tau}(\bar{\kappa}^p - \bar{\kappa}) = \bar{\kappa}^p - \bar{\kappa}$, for some $k \in K$, $\sigma(k) = \bar{\kappa}^p - \bar{\kappa}$.
Hence, σ is a universal splitting map of the irreducible polynomial $x^p - x - k \in K[x]$. □

Example 4.25. (**Galois's Great Theorem**)
Let $K, \bar{K}$ be fields with $K \leq \bar{K}$, where the inclusion map $\sigma : K \to \bar{K}$ is Galois with $G = \mathbf{Deck}(\sigma)$, and $p_0, p_1, \cdots, p_{m-2}, p_{m-1}$ be primes, where for each p_n, either $p_n = \mathbf{Char}(K)$, or there exists $\zeta_n \in K^\times$ of order p_n. TFAE:

(1) There exists a sequence $G = G_0 \geq G_1 \geq \cdots \geq G_{m-2} \geq G_{m-1} = \{e\}$ of subgroups of G, such that for all inclusion group homomorphism $G_{n+1} \to G_n$, for some prime p_n, G_n/G_{n+1} is p_n-cyclic.

(2) There exists a sequence $K = K_0 \leq K_1 \leq \cdots \leq K_{m-2} \leq K_{m-1} = \bar{K}$ of subfields of $\bar{K}$, such that for all inclusion field homomorphism $K_n \to K_{n+1}$, for some prime p_n, K_{n+1}/k_n is p_n-Kummer or p_n-Artin-Schreier.

References

[1] H. Ren, “Template for math notes,” 2021.

[2] Wikipedia contributors, “Resultant — Wikipedia, the free encyclopedia,” 2025, [Online; accessed 26-July-2025]. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Resultant&oldid=1293973970

[3] C. C.-A. Cheng, J. H. McKay, and S. S.-S. Wang, “Resultants of cyclotomic polynomials,” *Proceedings of the American Mathematical Society*, vol. 123, no. 4, pp. 1053–1059, Apr. 1995, communicated by William Adams. [Online]. Available: https://www.ams.org/journals/proc/1995-123-04/S0002-9939-1995-1242077-8/S0002-9939-1995-1242077-8.pdf

[4] R. E. Borcherds, “Galois theory lecture,” YouTube Video, 2020. [Online]. Available: https://www.youtube.com/watch?v=ccc4EYeytYo