Algebra I

Minerva

2020-1st

Contents

Chapter 1

Group theory

1.1 Motivation and basic notion

Question: Is there exists a root-formula for $f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_0 = 0$

- $n = 2$:
$$x = \frac{-a_1 \pm \sqrt{a_1^2 - 4a_2}}{2}$$
- $n = 3$: Let $y = x - \frac{a_1}{3} \rightsquigarrow y^3 + py + q = 0$. Let $y = u + v$, then
$$u^3 + v^3 + q + (u + v)(3uv + p) = 0$$
Let $3uv + p = 0$, then
$$\begin{cases} 3uv = -p \\ u^3 + v^3 = -q \end{cases} \rightsquigarrow u^3 = \frac{-q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$
- $n = 4$: Let $y = x - \frac{a_1}{4} \rightsquigarrow y^4 + ay^2 + by + c = 0$.
$$\left(y^2 + \left(\frac{a}{2} + t\right)\right)^2 = 2ty^2 - by - c + \left(\frac{a}{2} + t\right)^2$$
We want RHS is a square of y, which means
$$b^2 - 4 \cdot 2t \cdot \left(-c + \left(\frac{a}{2} + t\right)^2\right) = 0$$
and it had been by $n = 3$. So we can reduce to case of $n = 2$.
- $n = 5$:
  - Abel (1824): $\exists\ f(x) = x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5$ has no root-formula
  - Galois (1811 1832): Assume that $f(x) = 0$ has roots $\alpha_1, \alpha_2, ..., \alpha_n$
    Let $F = \mathbb{Q}(a_1, ..., a_n)$ and $K = F(\alpha_1, ..., \alpha_n)$

Theorem 1.1.1. (Main Goal)
$f(x)$ has a root-formula $\iff$ $G = \mathrm{Aut}(K/F)$ is solvable

Example 1.1.1. $f(x) = x^4 - 5x^2 + 6 = 0 \rightsquigarrow x = \pm\sqrt{2}, \pm\sqrt{3}, F = \mathbb{Q}, K = \mathbb{Q}(\pm\sqrt{2}, \pm\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
If $\sigma \in \mathrm{Aut}(K/F) \implies \sigma(\sqrt{2})^2 = \sigma(\left(\sqrt{2}\right)^2) = 2 \implies \sigma(\sqrt{2}) = \pm\sqrt{2}$
Similarly, $\sigma(\sqrt{3}) = \pm\sqrt{3}$

$$\mathrm{Aut}(K/F) = \left\{ \begin{pmatrix} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{pmatrix}, \begin{pmatrix} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{pmatrix}, \begin{pmatrix} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{pmatrix}, \begin{pmatrix} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{pmatrix} \right\}$$

We find that $\sigma \circ \sigma = \mathrm{id}$ have particular structure.

Definition 1.1.1 (Group)**.** Let G be a set

- A map $\begin{matrix} G \times G & \to & G \\ (x, y) & \mapsto & x \cdot y \end{matrix}$ is called a **law of composition**
- The law of composition is a **associative** if $(xy)z = x(yz)$ $\forall x, y, z \in G$
  Then we call G is **semigroup**
- G is called a **monoid** if G is a **semigroup** and $\exists e \in G$ s.t. $xe = ex = x$ $\forall x \in G$
- G is a **group** if G is a monoid and $\forall x \in G$ $\exists$ y s.t. $xy = yx = e$

Property 1.1.1.

- e is unique: If $\exists$ another e' s.t. $xe' = e'x = x$ $\forall x \in G$, then $e = ee' = e'$
- $\forall x$ the y is unique. If $\exists$ another y', then $y = ye = yxy' = ey' = y'$

Example 1.1.2.
$(\mathbb{Z}, +, 0)$ is a group, but $(\mathbb{Z}, \times, 1)$ is not a group $(2^{-1} \notin \mathbb{Z})$
$(\mathbb{Q} \setminus \{0\}, \times, 0)$ is a group. Moreover, it is a **subgroup** of $(\mathbb{R} \setminus \{0\}, \times, 0)$

Definition 1.1.2. Let S be a nonempty set.

- A permutation of S is a $1-1$ and onto map from S to S
- $\mathrm{Perm}(S)$ is the set of all permutation of $S \rightsquigarrow (\mathrm{Perm}(S), \circ, \mathrm{id})$ forms a group.
- $S = \{1, 2, ..., n\}$, then $S_n := \mathrm{Perm}(S)$ (the symmetric group of degree n)

Definition 1.1.3 (morphism)**.** Let G, G' be groups and $f : G \to G'$ be a map

- f is called a group **homomorphism** if $\forall x, y \in G$ $f(xy) = f(x)f(y)$
- f is called a group **monomorphism** if f is $1-1$ and homo. $(f : G \hookrightarrow G')$

- f is called a group **epimorphsim** if f is onto and homo. ($f : G \twoheadrightarrow G'$)
- f is called a group **isomorphism** if f is bijective and homo. ($f : G \xrightarrow{\sim} G'$ or $G \simeq G'$)

Theorem 1.1.2. (Cayley) Every group can be regarded as (**isomorphism**) a subgroup of permutation group

Proof: For given $x \in G$, we can define a map $\sigma_x : \begin{array}{ccc} G & \to & G \\ z & \mapsto & xz \end{array}$

- σ_x is a permutation of G :
  - $1-1$: if $xz_1 = xz_2 \rightsquigarrow z_1 = x^{-1}xz_1 = x^{-1}xz_2 = z_2$
  - onto: $\forall y \in G$, $\sigma_x(x^{-1}y) = y$
- $f : \begin{array}{ccc} G & \to & \mathrm{Perm}(G) \\ x & \mapsto & \sigma_x \end{array}$
  - $\sigma_{xy}(z) = xy(z) = \sigma_x(yz) = (\sigma_x \circ \sigma_y)(z)\ \forall z \in G \implies \sigma_{xy} = \sigma_x \circ \sigma_y$
  - $f(G)$ is a subgroup of $\mathrm{Perm}(G)$
    - $\mathrm{id} = \sigma_e$
    - $f(x)f(y) = f(xy) \in f(G)$
    - $f(x)f(x^{-1}) = f(e) = f(x^{-1})f(x)$
  - f is $1-1$: if $\sigma_x = \sigma_y$ i.e. $xz = yz\ \forall z \in G$. In particular, $x = xe = ye = y$

  Hence, $G \simeq f(G) \leq \mathrm{Perm}(G)$ □

Example 1.1.3. $f : G \xrightarrow{\sim} G' \implies f^{-1} : G' \to G$ is a group homo.
$f(x) = x', f(y) = y' \implies f(xy) = x'y' \implies f^{-1}(x'y') = xy = f^{-1}(x)f^{-1}(y)$

Definition 1.1.4. G is called **abelian** if $\forall\ x, y \in G,\ xy = yx$

1.2 Symmetric group and Dihedral groups

Recall: $S_n = \{f : \{1, 2, ..., n\} \to \{1, 2, ..., n\} | f \text{ is } 1-1 \text{ and onto}\}$

Definition 1.2.1 (**Cyclic notation**). $\sigma \in S_n$. If $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{pmatrix}$, then we write $\sigma = (14)(235)$ and (14) is called 2-cycle, (235) is called 3-cycle.
$\implies$ Any permutation can be written as a product of disjoint cycle

Example 1.2.1. In $S_7, \sigma = (123)(456), \tau = (1356)(247)$
$\implies \sigma\tau = (1)(234736) = (234736), \sigma^{-1} = (132)(465)$

Definition 1.2.2 (transposition). 2-cycle is called **transposition**
$\implies$ Any permutation is a product of 2-cycles

Property 1.2.1. For $\sigma \in S_n$, the number of transposition appearing in any product for σ is unique in modulo 2.

Proof: Let $S = \{e_1, e_2, ..., e_n\}$ be the set of column vectors of I_n

$\forall\ \sigma \in S_n$, define $I_\sigma = [e_{\sigma(1)}\ e_{\sigma(2)}\ \cdots\ e_{\sigma(n)}] = \sum_{i=1}^{n} E_{\sigma(i)i}$

Claim: $I_\sigma I_\tau = I_{\sigma\tau}$

$$I_\sigma I_\tau = \left(\sum_{i=1}^{n} E_{\sigma(i)i}\right)\left(\sum_{j=1}^{n} E_{\tau(j)j}\right) = \sum_{i=1}^{n}\sum_{j=1}^{n} E_{\sigma(i)i}E_{\tau(j)j} = \sum_{j=1}^{n} E_{\sigma(\tau(j))j} = I_{\sigma\tau}$$

Note: If σ is transposition, then $\det(I_\sigma) = -\det(I_n) = -1$.
Hence, if $\sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_r = \tau_1' \circ \tau_2' \circ \cdots \circ \tau_s'$ with τ_i, τ_j' : 2-cycle
Then $(-1)^r = \det(I_{\tau_1} I_{\tau_2} \cdots I_{\tau_r}) = \det(I_\sigma) = \det(I_{\tau_1'} I_{\tau_2'} \cdots I_{\tau_s'}) = (-1)^s$
$\implies r \equiv s \pmod 2$ □

Definition 1.2.3. $\sigma \in S_n$, $\begin{cases}\det(I_\sigma) = 1 \rightsquigarrow \sigma \text{ is even} \\ \det(I_\sigma) = -1 \rightsquigarrow \sigma \text{ is odd}\end{cases}$
$\implies A_n := \{\sigma \in S_n | \sigma \text{ is even}\}$ is a subgroup of S_n

Property 1.2.2. $\forall n \geq 2,\ |A_n| = \frac{|S_n|}{2}$

Proof: Construct

$$\begin{array}{ccc} A_n & \longleftrightarrow & S_n \setminus A_n \\ \sigma & \longrightarrow & (12)\sigma \\ (12)\tau & \longleftarrow & \tau \end{array}$$

then $|A_n| = |S \setminus A_n|$ □

Property 1.2.3. (Useful Lemma) $\sigma(i_1\ i_2\ \cdots\ i_m)\sigma^{-1} = (\sigma(i_1)\ \sigma(i_2)\ \cdots\ \sigma(i_m))$

Proof: Let $i \in \{1, 2, ..., n\}$

- $i = \sigma(i_t)$: LHS$(i) = \sigma(i_{t+1})$ =RHS(i)
- $i \notin \{\sigma(i_1), ..., \sigma(i_m)\} \implies \sigma^{-1}(i) \notin \{i_1, ..., i_m\} \implies$ LHS$(i) = i =$ RHS(i)

□

Definition 1.2.4. A group G is said to be generated by $x_1, x_2, ..., x_n$ denoted by $G = \langle x_1, x_2, ..., x_n\rangle$ if $x \in G$ then $\exists j_i \in \{1, 2, ..., n\}$ and $m_i \in \{1, -1\}$ s.t. $x = \prod_{i=1}^{r} x_{j_i}^{m_i}$

Property 1.2.4.

(1) $S_n = \langle (12), (13), ..., (1n)\rangle$
$(a\ b) = (1\ b)(1\ a)(1\ b)^{-1}$

(2) $S_n = \langle (1\ 2), (2\ 3), ..., (n-1\ n)\rangle$
$(1\ a) = (a-1\ a)(a-2\ a-1)\cdots(2\ 3)(1\ 2)(2\ 3)\cdots(a-1\ a-2)(a-1\ a)$

(3) $S_n = \langle (1\ 2), (1\ 2\ \cdots\ n-1\ n) \rangle$

$(a-1\ a) = (1\ 2\ \cdots\ n-1\ n)^{a-2}(1\ 2)(1\ 2\ \cdots\ n-1\ n)^{-(a-2)}$

Definition 1.2.5. A subgroup H of S_n is **transitive** if for $i, j \in \{1, 2, ..., n\}, \exists\ \sigma \in H$ s.t. $\sigma(i) = j$

Property 1.2.5. Let H be a transitive subgroup of S_n containing a 2-cycle and an $(n-1)$-cycle. Then $H = S_n$

Proof: We may assume $\sigma = (1\ 2\ \cdots\ n-1), (i\ j) \in H$.

Let $\tau \in H$ s.t. $\tau(j) = n$. Then $\tau(i\ j)\tau = (k\ n)$ for some $1 \le k \le n-1$

$(k+1\ n) = \sigma(k\ n)\sigma^{-1} \in H$ and $(k-1\ n) = \sigma^{-1}(k\ n)\sigma \in H$

$\implies \langle (1\ n), (2\ n), ..., (n-1\ n) \rangle \subseteq H \implies S_n = H$ □

Definition 1.2.6. The **Dihedral group** D_{2n} is the group of symmetric of a regular n-gon.

It contain rotation, which rotate $\frac{2\pi}{n}$ counterclockwise and denoted by σ.

Fixed a reflection axis, let this reflection be τ. We can check let $\tau\sigma = \sigma^{-1}\tau$

In general,

$$D_{2n} = \langle \sigma, \tau | \sigma^n = \tau^2 = 1, \tau\sigma = \sigma^{-1}\tau \rangle = \{\sigma^i \tau^j | 0 \le i \le n-1, 0 \le j \le 1\}$$

Hence, $|D_{2n}| = 2n$

Definition 1.2.7. The period of x is defined to be the smallest natural number m s.t. $x^m = e$

1.3 Coset and quotient group

Definition 1.3.1. Let $f : G \to G'$ be a group homomorphism, define **kernel** of f is $\ker f := \{x \in G | f(x) = e'\}$ is a subgroup of G

Property 1.3.1. $\ker f = \{e\} \iff f$ is injective

$$\begin{aligned} f \text{ is } 1-1 &\iff \text{“}f(x) = f(y) \iff x = y\text{”} \\ &\iff \text{“}f(xy^{-1}) = e' \iff xy^{-1} = e\text{”} \iff \ker f = \{e\} \end{aligned}$$

In general, $f : G \to G'$ define $F_{x'} = f^{-1}(x') := \{x \in G | f(x) = x'\}$ is the preimage of x'. Obviously, $\overline{G} = \{F_{x'} | x' \in \operatorname{Im} f\}$ forms a partition of G and $\overline{G}$ inherits a group structure from $\operatorname{Im} f$:

$$F_{x'} F_{y'} = F_{x'y'}$$

To analyze the intrinsic property of $\overline{G}$ ($H = \ker f$)

- $F_{x'} = xH$ for any $x \in G$ with $f(x) = x'$

- $F_{x'}F_{y'} = F_{x'y'} \implies xHyH = xyH$

We conclude that if $H = \ker f$ for $f; G \to G'$ then $G/H = \{xH | x \in G\}$ forms a group under $xHyH$ and $G/H \simeq \operatorname{Im} f$ (1st isom.thm.)

Definition 1.3.2. Let G be a group and H be a subgroup of G

- For $x \in G, xH$ is called **left coset** of H and x is called **representative**
- For $x \in G$ we call x **congruent** to y modulo H, written $x \equiv y \pmod H$ if $x^{-1}y \in H$

  $\forall y \in xH$, say $y = xh \implies yH = xhH \subseteq xH$ and $x = yh^{-1} \implies xH = yh^{-1}H \subseteq yH$. Thus, $xH = yH$

Property 1.3.2. $\{xH | x \in G\}$ forms a partition of G
If $z \in (xH \cap yH) \implies xH = zH = yH$

Theorem 1.3.1. (Lagrange) Let G be a finite group and $H \leq G$. Then $|H|\big||G|$.

Proof: Claim: $|H| = |xH| \ \forall x \in G$. $\begin{pmatrix} \phi : & H & \to & xH \\ & h & \mapsto & xh \end{pmatrix}$ is a bijection

We have $G = \bigcup_{i=1}^{r} x_i H$ with $\{x_1 H, ..., x_r H\}$: distinct left coset of H. Then

$$|G| = \sum_{i=1}^{r} |x_i H| = \sum_{i=1}^{r} |H| = r|H| \implies |H|\big||G|$$

□

Remark 1.3.1. The converse of Lagrange theorem is false
No subgroup of A_4 has order 6. (Note: $|A_4| = \frac{4!}{2} = 12$)
If $H \leq A_4$ with $|H| = 6$, say $A_4 = H \cup xH$ with $x \notin H$.
$z \in xH$: say $z = xh \rightsquigarrow z^2 = xhxh$. If $z^2 \in xH \rightsquigarrow hxh \in H \rightsquigarrow x \in H (\to\leftarrow)$. Hence, $z^2 \in H \implies \forall z \in A_4 \, z^2 \in H$. But $(i\ j\ k) = (i\ k\ j)^2 \in H \rightsquigarrow 8 \leq |H| (\to\leftarrow)$

Remark 1.3.2. $\{\text{left coset of } H\} \iff \{\text{right coset of } H\}$

Example 1.3.1. In $S_3, H = \langle (1\ 2) \rangle \rightsquigarrow (1\ 2\ 3)H = (1\ 3)H$ but $H(1\ 2\ 3)H \neq H(1\ 2)$
Since $(1\ 2\ 3)^{-1}(1\ 3) = (1\ 2) \in H$ and $(1\ 2\ 3)(1\ 3)^{-1} = (2\ 3) \notin H$

Definition 1.3.3. Let $H \leq G$. The **index** of H in G is defined to be the number of distinct left (right) cosets, denoted by $(G : H)$.
By Lagrange theorem, $(G : H) = \frac{|G|}{|H|}$

Ques. Is $\{zH | x \in G\}$ made into a group?
We need "$xHyH = xyH$" $\forall\, x, y \in G$. In particular, $xHx^{-1}H = H \rightsquigarrow xHx^{-1} \subseteq H \ \forall\ x \in G$. Since $|xHx^{-1}| = |H| \implies xHx^{-1} = H \rightsquigarrow xH = Hx \ \forall\ x \in G$

$$\implies xHyH = xyHH = xyH$$

Definition 1.3.4.

- Let $H \leq G$, H is said to be **normal** ($H \lhd G$) if $xHx^{-1} = H$
- If $H \lhd G$, then $G/H := \{xH | x \in G\}$ is called the **quotient group** of G by H.

Property 1.3.3. If $H \leq G$ with $(G : H) = 2$, then $H \lhd G$.
$\forall x \notin H, G = H \cup xH = H \cup Hx \implies xH = Hx$ and $\forall x \in H, xH = Hx$

Definition 1.3.5. We say f from G to G is **automorphism** if f is isomorphism.
$\mathrm{Aut}(G) := \{f : G \to G | f \text{ is automorphism}\}$

Example 1.3.2. $\forall n \geq 2, A_n \lhd S_n$

$\forall x \in G$, define $r_x : \begin{array}{ccc} G & \to & G \\ y & \mapsto & xyx^{-1} \end{array}$ (we say xyx^{-1} is a conjugate of y)

- r_x is $1-1$: $xy_1x^{-1} = xy_2x^{-1} \rightsquigarrow y_1 = y_2$
- r_x is onto: $r_x(x^{-1}yx) = y$
- r_x is auto.: $r_x(yz) = xyzx^{-1} = xyx^{-1}xzx^{-1} = r_x(y)r_x(z)$

Definition 1.3.6. $\mathrm{Inn}(G) := \{r_x | x \in G\} \leq \mathrm{Aut}(G)$

Property 1.3.4. $f : \begin{array}{ccc} G & \to & \mathrm{Inn}(G) \\ x & \mapsto & r_x \end{array}$ is a group homo. and $\ker f = Z_G := \{x \in G | xy = yx \ \forall \ y \in G\}$ is call **center** of G, then $G/Z_G \simeq \mathrm{Inn}(G)$ (by 1st isom.thm.)

Proof:

- $f(xy)(z) = xyz(xy)^{-1} = x(yzy^{-1})x^{-1} = f(x)f(y)(z) \ \forall \ z \in G \rightsquigarrow f(xy) = f(x)f(y)$
- $x \in \ker f \iff r_x = \mathrm{id}_G \iff xzx^{-1} = z \ \forall \ z \in G \iff x \in Z_G$

□

Definition 1.3.7 (exact sequence).
- $G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3 \xrightarrow{f_3} \cdots \xrightarrow{f_{n-2}} G_{n-1} \xrightarrow{f_{n-1}} G_n$ is exact if $\mathrm{Im}\, f_i = \ker f_{i+1}$
- $0 \longrightarrow G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3 \longrightarrow 0$ is exact if $\mathrm{Im}\, f_1 = \ker f_2, f_1 : 1-1, f_2 :$ onto

Definition 1.3.8.

- $j : G \hookrightarrow G'$ is called **inclusion map** if $j(x) = x \ \forall \ x \in G$
- $\varphi : G \twoheadrightarrow G/H$ is called **canonical map** if $\varphi(x) = xH \ \forall \ x \in G$

Theorem 1.3.2. (1st 1som.thm.) $G/\ker f \simeq \operatorname{Im} f$

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker f & \xhookrightarrow{j} & G & \xrightarrow{f} & \operatorname{Im} f & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle \mathrm{id}} & & \uparrow{\scriptstyle \mathrm{id}} & & \uparrow{\scriptstyle s}\wr & & \\ 0 & \longrightarrow & \ker f & \xhookrightarrow{j} & G & \xrightarrow{\varphi} & G/\ker f & \longrightarrow & 0 \end{array} \qquad \begin{array}{l} \text{is exact} \\ \\ \text{is exact} \end{array}$$

Proof: $\forall x' \in \operatorname{Im} f, \exists\, x \in G$ s.t. $f(x) = x'$, then define $s(x \ker f) = x'$

- s is well defined: if $x\ker f = y\ker f \rightsquigarrow x^{-1}y \in \ker f \implies f(x) = f(y)$
- s is homo.: $s([x\ker f][y\ker f]) = s(xy\ker f) = f(xy) = f(x)f(y) = s(x\ker f)s(y\ker f)$
- s is $1-1$: $s(x\ker f) = e \iff f(x) = e \iff x \in \ker f \iff x\ker f = \ker f$
- s is onto: $\forall x' \in \operatorname{Im} f, \exists\, x \in G$ s.t. $f(x) = x' \implies s(x\ker f) = x'$

Hence, $G/\ker f \simeq \operatorname{Im} f$ □

1.4 Isomorphism theorem

Theorem 1.4.1. (factor theorem) Let $f : G \to G'$ with $H = \ker f$ and $N \lhd G$ with $N \leq H$, then there exists unique monomorphsim f_* s.t diagram commute.

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ \downarrow{\scriptstyle \varphi} & \nearrow_{\exists! f_*} & \\ G/N & & \end{array}$$

Proof: Define $f_* : G/N \to G'$ by $f_*(x) = f(x)$

- well defined: $xN = yN \rightsquigarrow x^{-1}y \in N \leq \ker f \implies f(x) = f(y)$
- Note $G/N \xrightarrow{f_*} G'$ with $\ker f_* = H/N$. By 1st isom.thm,

$$(G/N)/(H/N) \simeq \operatorname{Im} f_* = \operatorname{Im} f \simeq G/H$$

□

Theorem 1.4.2. (3rd isom.thm.) Let $H, K \lhd G$ with $K \leq H$. Then

$$G/H \simeq (G/K)/(H/K)$$

Proof: Consider canonical map $\varphi : G \to G/H$, then $\ker f = H$ and $K \leq \ker f$. By factor theorem, we have

$$(G/K)/(H/K) \simeq G/H$$

□

Note: The property of being normal depends on an embedding of H, not on H itself.

Definition 1.4.1. The **normalizer** of H in G is defined to be $H \leq N(H) := \{x \in G | xHx^{-1} = H\} \leq G$. Which is the biggest subgroup of G that let H be normal in.

Property 1.4.1. By def, $H \lhd N(H)$ and "$H \leq K \leq N(H) \implies N \lhd K$"

Definition 1.4.2. Let $H, K \leq G, HK := \{hk | h \in H, k \in K\}$

- In general, HK is not a subgroup

  eg. In S_3, $H = \langle (1\ 2) \rangle, K = \langle (2\ 3) \rangle \implies HK = \{(1), (1\ 2), (2\ 3), (1\ 2\ 3)\}$.

  Since $4 = |H| \not| |G| = 6$, by Lagrange thm, HK is not the group.

- $HK \leq G \iff HK = KH$

  Proof:

  ($\Rightarrow$): $K, H \leq HK \rightsquigarrow KH \subseteq HK$. $\forall hk \in HK\ \exists h'k' \in HK$ s.t. $(hk)(h'k') = e \implies hk = k'^{-1}h'^{-1} \in KH$

  ($\Leftarrow$): $\forall h_1k_1, h_2k_2 \in HK, (h_1k_1)(h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1} \in HKH = HHK = HK$ □

- $H \lhd G, K \lhd G \implies \forall x \in K \leq G, xHx^{-1} = H \implies \forall x \in K, xH = Hx \implies KH = HK \implies HK \leq G$

- $K \leq N(H) \implies HK \leq N(H) \leq G$ (Since $H \lhd N(H)$)

- $H \leq Z_G, k \leq G \implies HK = KH \implies HK \leq G$

Theorem 1.4.3. (2nd isom. thm.) $H, K \leq G$ with $H \leq N(K)$, then

$$HK/K \simeq H/(H \cap K)$$

Proof:

- First we check $K \lhd HK$: $\begin{cases} H \leq N(K) \\ K \lhd N(K) \end{cases} \implies HK \leq N(K) \implies K \lhd NK$

- Define $f : \begin{array}{ccc} H & \to & HK/K \\ h & \mapsto & hK \end{array}$, which is a group homo. by def.

  - f is onto: $\forall hkK \in Hk/K, f(h) = hK = hkK$
  - $h \in \ker f \iff hK = K \iff h \in H \cap K$

  By 1st iso.thm. $HK/K \simeq H/(H \cap K)$

□

Let $f : G \to G'$ be a group homo. and $H' \leq G'$, then

- $f^{-1}(H') \leq G$: $x, y \in f^{-1}(H)$ say $f(x) = x', f(y) = y' \rightsquigarrow x'^{-1}y \in H' \implies x^{-1}y \in f^{-1}(H')$
- $H' \lhd G' \implies f^{-1}(H') \lhd G$: Consider $G \xrightarrow{f} G' \xrightarrow{\varphi} G'/H'$, then $f^{-1}(H') = \ker(\varphi \circ f) \lhd G$

  Also we get $G/H \hookrightarrow G'/H'$ (where $H = f^{-1}(H')$)

  If f is epimorphism, then $G/H \simeq G'/H'$

Property 1.4.2. If $K \lhd G$ and canonical map $\varphi : G \to G/K$, then

$$\begin{array}{ccc} \{H \leq G | K \leq H\} & \longleftrightarrow & \{H' \leq G/K\} \\ H & \longmapsto & H/K \\ \varphi^{-1}(H') & \longmapsfrom & H' \end{array}$$

and consider those two exact sequence (let $H := \varphi^{-1}(H')$)

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \varphi^{-1}(H') & \hookrightarrow & G & \longrightarrow & G/H & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \varphi} & & & & \\ 0 & \longrightarrow & H' & \hookrightarrow & G/K & \longrightarrow & G/H & \longrightarrow & 0 \end{array}$$

Use 1st iso.thm. on the one below, we get

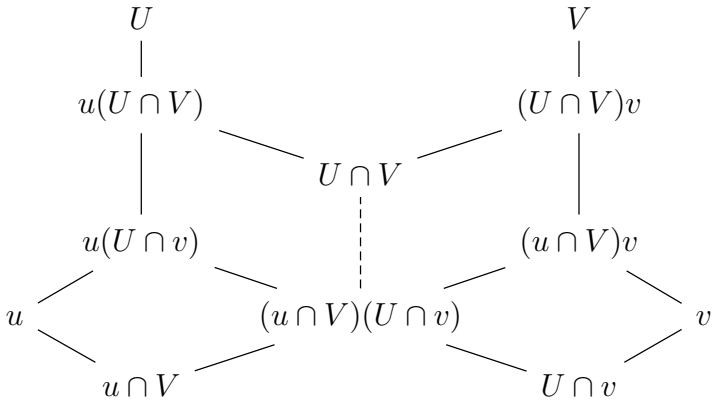
$$G/H \simeq (G/K)/(H/K)$$

which is 3rd iso.thm.

Theorem 1.4.4. (Butterfly lemma) Let $U, V \leq G$ and $u \lhd U, v \lhd V$, then

$$u(U \cap V)/u(U \cap v) \simeq (U \cap V)v/(u \cap V)v$$

Proof:



- $(u(U \cap V)) \cap ((U \cap V)v) = ((U \cap V)u) \cap ((U \cap V)v) = (U \cap V)(u \cap v) = U \cap V$

  Since $u \lhd U, u(U \cap V) = (U \cap V)u$

- $(u(U\cap v))\cap((u\cap V)v)=(u\cap V)(U\cap v)$:
  If $u_1U_1=V_1v_1$ for $u_1\in u, U_1\in(U\cap v), v_1\in v, V_1\in(u\cap V)$, then
  $$U\supseteq u\ni V_1^{-1}u_1=v_1U_1^{-1}\in v\subseteq V\implies u_1\in V, v_1\in U$$
- Let $H=U\cap V\leq U, K=u(U\cap v)\leq U$, then
  - $H\leq N(K)$: $\forall x\in H,\ x(u(U\cap v))x^{-1}=xux^{-1}(x(u(U\cap v))x^{-1})$
    Since $u\lhd U$, $xux^{-1}=u$. $x(U\cap v)x^{-1}=(xUx^{-1})\cap(xvx^{-1})\subseteq U\cap V$
    Hence, $x(u(U\cap v)x^{-1})\subseteq u(U\cap V)$
  - $HK=(U\cap V)u(U\cap v)=u(U\cap V)(U\cap v)=K$
  - $H\cap K=(U\cap V)\cap(u(U\cap v))=(u\cap V)(U\cap v)$

  By 2nd isomorphism theorem, $HK/K\simeq H/(H\cap K)\implies$
  $$u(U\cap v)/u(U\cap v)\simeq(U\cap V)/(u\cap V)(U\cap v)\simeq(u\cap V)v/(u\cap V)v$$
  (last iso. is by symmetry) □

Definition 1.4.3. If $G=\langle a\rangle$, then we call G is **cyclic**.
Denoted C_n be the cyclic group with order n.

Property 1.4.3. If G is cyclic, then $G\simeq\mathbb{Z}$ or $G\simeq Z/n\mathbb{Z}$
Let $f:\begin{array}{ccc}\mathbb{Z}&\to&G\\ n&\mapsto&a^n\end{array}$ is epimorphism.
If $\forall m\in\mathbb{Z}, a^m\neq e\implies\ker f=0\implies G\simeq\mathbb{Z}$
If period of a is n, then $\ker f=n\mathbb{Z}\implies G\simeq\mathbb{Z}/n\mathbb{Z}$

1.5 Solvable groups

Ques: How to simply a group G?
Strategy: If $G=\{e\}$, then done!
If $G\neq\{e\}$, then we check whether G has a nontrivial proper normal subgroup.
If no, then done! Then we call G is **simple**
Otherwise, find $G_1\lhd G$ as large as possible s.t. G/G_1 is simple.
(If $N\lhd G/G_1\implies\exists G_1\lhd N'\lhd G$ s.t. $N=N'/G_1$.)
If G_1 is simple, then done! Otherwise, $\exists\ G_2\lhd G_1$ s.t. G_1/G_2 is simple. $\cdots$
If $|G|<\infty$, $\exists\ \{e\}=G_n\lhd G_{n-1}\lhd\cdots\lhd G_1\lhd G:=G_0$ s.t. G_i/G_{i+1} is simple.
(We can't insert any normal subgroup into it.)
It is called a **composition series** of G with n (the **length** of G) and G_i/G_{i+1} is called **factor**.

Example 1.5.1. $G=\mathbb{Z}/12\mathbb{Z}=\{\overline{0},\overline{1},...,\overline{11}\}\rightsquigarrow|G|=12$
$G_1=\langle\overline{2}\rangle\rightsquigarrow|G_1|=6\rightsquigarrow|G/G_1|=2\rightsquigarrow G/G_1\simeq C_2$: simple
$G_2=\langle\overline{4}\rangle\rightsquigarrow|G_2|=3\rightsquigarrow|G_1/G_2|=2\rightsquigarrow G_1/G_2\simeq C_2$: simple
$G_3=\langle\overline{0}\rangle\rightsquigarrow G_2/G_3\simeq C_3$: simple

$G_3 \lhd G_2 \lhd G_1 \lhd G \rightsquigarrow$ length $= 3$, factors: C_2, C_2, C_3
$G_1' = \langle \overline{3} \rangle \rightsquigarrow |G_1'| = 4 \rightsquigarrow |G/G_1'| = 3 \rightsquigarrow G/G_1' \simeq C_3$: simple
$G_2' = \langle \overline{6} \rangle \rightsquigarrow |G_2'| = 2 \rightsquigarrow |G_1'/G_2'| = 2 \rightsquigarrow G_1'/G_2' \simeq C_2$: simple
$G_3' = \langle \overline{0} \rangle \rightsquigarrow G_2'/G_3' \simeq C_3$: simple
$G_3' \lhd G_2' \lhd G_1' \lhd G \rightsquigarrow$ length $= 3$, factors: C_3, C_2, C_2

We find that two composition series of $G = \mathbb{Z}/12\mathbb{Z}$ have same length and same factors up to permutation. In fact, it will hold for general cases!

Theorem 1.5.1. (Jorden-Hölder theorem) If G has composition series, then two composition series are **equivalent**" (def : have same length and the same factors up to permutation)

But before proof Jorden-Hölder theorem, we see this theorem first.

Theorem 1.5.2. (Schreier theorem) Any two **normal series** (def : series not required have simple factors) have equivalent **refinemant** (def : insert a finite number of normal subgroups into a normal series).

Proof: Given $\begin{cases} \{e\} = H_r \lhd H_{r-1} \lhd \cdots \lhd H_1 \lhd H_0 = G \\ \{e\} = K_r \lhd K_{s-1} \lhd \cdots \lhd K_1 \lhd K_0 = G \end{cases}$
We defined $H_{ij} = H_{i+1}(H_i \cap K_j)$ and $K_{ji} = (H_i \cap K_j)K_{j+1}$.
Apply butterfly lemma on $H_{i+1} \lhd H_i, K_{j+1} \lhd K_j$ we have

$$\begin{aligned} H_{ij}/H_{i(j+1)} &= H_{i+1}(H_i \cap K_j)/H_{i+1}(H_i \cap K_{j+1}) \\ &\simeq (H_i \cap K_j)K_{j+1}/(H_{i+1} \cap K_j)K_{j+1} = K_{ji}/K_{j(i+1)} \end{aligned}$$

then we have

$$\begin{aligned} \{e\} = H_r =& H_{(r-1)s} \lhd H_{(r-1)(s-1)} \lhd \cdots \lhd H_{(r-1)0} \\ =& H_{r-1} = H_{(r-2)s} \lhd \cdots \lhd H_{(r-2)0} \\ =& H_{r-2} = H_{(r-3)s} \lhd \cdots \lhd H_{10} \\ =& H_1 = H_{0s} \lhd \cdots \lhd H_{01} \lhd H_{00} = G \\ \{e\} = K_s =& K_{(s-1)r} \lhd K_{(s-1)(r-1)} \lhd \cdots \lhd K_{(s-1)0} \\ =& K_{s-1} = K_{(s-2)r} \lhd \cdots \lhd K_{(s-2)0} \\ =& K_{s-2} = K_{(s-3)r} \lhd \cdots \lhd K_{10} \\ =& K_1 = K_{0r} \lhd \cdots \lhd K_{01} \lhd K_{00} = G \end{aligned}$$

Both of sizes $= rs$, also $H_{ij}/H_{i(j+1)} \simeq K_{ji}/K_{j(i+1)}$.
Note that if $H_{ij} = H_{i(j+1)}$ then $K_{ji} = K_{j(i+1)}$, we can omit H_{ij}, K_{ji} at same time. Consequently, they are equivalent. □

Back to the proof of Jorden-Hölder theorem. Let (I) and (II) be two of composition series. By Schreier theorem, they have equivalent $(\widetilde{\text{I}}), (\widetilde{\text{II}})$. But (I),(II) are

already composition series, we can't insert any subgroup. Thus, (I)= $(\widetilde{\text{I}})$, (II)= $(\widetilde{\text{II}})$. So (I),(II) are equivalent.

Definition 1.5.1. G is solvable if $\exists\ \{e\} = G_m \lhd G_{m-1} \lhd \cdots \lhd G_1 \lhd G_0 = G$ with G_i/G_{i+1}: abelian

Property 1.5.1. Let G be finite and abelian. Then G admits a normal series with cyclic factors.

Proof: By induction in $|G|$. $|G| = 1 \rightsquigarrow G = \{e\}$.
Let $|G| > 1$. Then pick $e \neq x \in G$ and consider $G/\langle x\rangle$.
Since $|\langle x\rangle| > 1$, $|G/\langle x\rangle| < |G|$. By induction hypothesis

$$\{e\} = G'_{m-1} \lhd \cdots \lhd G'_1 \lhd G'_0 = G/\langle x\rangle \text{ with } G'_i/G'_{i+1} \text{ is cyclic}$$

Write $G'_i = G_i/\langle x\rangle$ and in particular, $G_{m-1} = \langle x\rangle$.
By 3rd iso.thm, $G_i/G_{i+1} \simeq G'_i/G'_{i+1}$ is cyclic $\forall i = 0, 1, ..., m-2$. Then

$$G_m := \{e\} \lhd \langle x\rangle = G_{m-1} \lhd \cdots \lhd G_1 \lhd G_0 = G \text{ with } G_i/G_{i+1} \text{ is cyclic}$$

□

Property 1.5.2. G is solvable and $|G| < \infty \implies$ exists a normal series with cyclic factors.

Proof: Write $\{e\} = G_n \lhd \cdots \lhd G_1 \lhd G_0 = G$
Since G_i/G_{i+1} is abelian $\rightsquigarrow \{e\} = \overline{G_\ell} \lhd \cdots \lhd \overline{G_0} = G_i/G_{i+1}$ with cyclic factor and embed in $G_{i+1} \lhd G_i$ and get a normal series with cyclic factors. □

Property 1.5.3. Let $H \lhd G$. G is solvable $\iff$ H is solvable and G/H is solvable

Proof:
($\Leftarrow$) Let $\begin{cases}\{e\} = H_m \lhd H_{m-1} \lhd \cdots \lhd H_1 \lhd H_0 = H \text{ with } H_i/H_{i+1} \text{ abelian}\\ \{\overline{e}\} = \overline{G_\ell} \lhd \overline{G_{\ell-1}} \lhd \cdots \lhd \overline{G_1} \lhd \overline{G_0} = G/H \text{ with } \overline{G_i}/\overline{G_{i+1}} \text{ abelian}\end{cases}$
Write $\overline{G_i} = G_i/H \rightsquigarrow G_i/G_{i+1} \simeq \overline{G_i}/\overline{G_{i+1}}$ is abelian. Hence,

$$\{e\} = H_m \lhd \cdots \lhd H_1 \lhd H_0 = H = G_\ell \lhd \cdots \lhd G_1 \lhd G_0 = G$$

($\Rightarrow$) Write $\{e\} = G_m \lhd G_{m-1} \lhd \cdots \lhd G_1 \lhd G_0 = G$ with G_i/G_{i+1}: abelian. Consider

- Let $H_i = G_i \cap H \rightsquigarrow H_i \lhd H_{i-1}$ and H_{i-1}/H_i is abelian

$$H_{i-1} \hookrightarrow G_{i-1} \xrightarrow{can.} G_{i-1}/G_i \quad \text{and} \quad \ker f = G_i \cap H = H_i$$

So $H_i/H_{i-1} \simeq G_{i-1}/G_i$ is abelian.

- Let $\varphi : G \twoheadrightarrow G/H \rightsquigarrow \varphi(G_m) \lhd \varphi(G_{m-1}) \lhd \cdots \lhd \varphi(G_1) \lhd \varphi(G_0) = G/H$
  (Since $\varphi(x)\varphi(G_i)\varphi(x)^{-1} = \varphi(xG_ix^{-1}) = \varphi(G_i)\ \forall\ x \in G_{i-1}$)

$$G_{i-1} \xhookrightarrow{\varphi} \varphi(G_{i-1}) \xrightarrow{can} \varphi(G_{i-1})/\varphi(G_i) \quad \rightsquigarrow G_i \subseteq \ker g$$
$$\text{(composite } G_{i-1} \to \varphi(G_{i-1})/\varphi(G_i) \text{ labelled } g\text{)}$$

  By factor theorem, $G_{i-1}/G_i \overset{\exists}{\twoheadrightarrow} \varphi(G_{i-1})/\varphi(G_i)$.
  By 1st iso.thm, $\varphi(G_{i-1})/\varphi(G_i)$ is a quotient group of an abelian which is abelian.

□

Remark 1.5.1. The classification of finite simple groups is given as follows

- $\mathbb{Z}/p\mathbb{Z}$ which p: prime
- A_n for $n \geq 5$
  - S_3 is solvable
  $$\{0\} \lhd A_3 \lhd S_3$$
  - S_4 is solvable
  $$\{0\} \lhd \langle(12)(34)\rangle \lhd V_4 \lhd A_4 \lhd S_4$$
  where $V_4 = \{(1), (12)(34), (13)(24), (14)(23)\}$
- simple group of Lie type
- 26 sporadic simple group

Example 1.5.2. $\mathbb{Z}/p\mathbb{Z}$ is a field and defined $(\mathbb{Z}/n\mathbb{Z})^\times := \{\overline{k} | \gcd(k, n) = 1\}$

1.6 Cyclic group

Recall: $G = \langle a \rangle$

- a has infinite period $\rightsquigarrow G \simeq \mathbb{Z}$
- a has period $n \rightsquigarrow G \simeq \mathbb{Z}/n\mathbb{Z}$

Definition 1.6.1. The **order** of G is defined to be $|G|$ and $\forall a \in G$ the **order** of a is defined to be $|\langle a \rangle|$ and denoted $o(a)$.

Property 1.6.1. Let $G = \langle a \rangle$ and $o(a) = n$. Then for $1 \leq r \leq n$, $o(a^r) = \frac{n}{\gcd(r,n)}$.
Write $d = \gcd(r, n)$ and $r = dr', n = dn'$

- $(a^r)^{n'} = a^{dn'r'} = e \rightsquigarrow o(a^r) \big| n'$

- $e = (a^r)^{o(a^r)} = a^{ro(a^r)} \rightsquigarrow n \big| ro\,(a^r) \rightsquigarrow n' = \frac{n}{d} \big| o\,(a^r)$

  Hence, $o\,(a^r) = n$

Property 1.6.2. Any subgroup of a cyclic group is cyclic
Let $G = \langle a \rangle$ and $H \leq G$. If $H = \{e\}$ then done!
Otherwise, $\exists\ d = \min\{m \in \mathbb{N} | a^m \in H\}$ (Note $a^\ell \in H \iff a^{-\ell} \in H$)
Claim: $H = \{a^d\}$
($\supseteq$): Ok!
($\subseteq$): If $a^n \in H$ with $n \in \mathbb{N}$, write $n = dx + y$ with $x \in \mathbb{N}$ and $0 \leq y < d$.
Since $a^y = a^n \cdot \left(a^d\right)^{-x} \in H \rightsquigarrow\ y = 0$ or $y \geq d \rightsquigarrow y = 0$

Property 1.6.3. Let $G = \langle a \rangle$ with $o(a) = n$. Then $d|n \iff \exists! H \leq G$ s.t. $|H| = d$
($\Leftarrow$) By Lagrange theorem.
($\Rightarrow$) Write $n = dn' \implies o\left(a^{n'}\right) = \frac{n}{\gcd(n,n')} = d$. Let $H = \langle a^{n'} \rangle \rightsquigarrow |H| = d$
If exists another H' with $|H'| = d$ say $H = \langle a^m \rangle$ then $o\,(a^m) = d$
Then $d \gcd(n, d) = n = dn' \rightsquigarrow n' | m \rightsquigarrow \langle a^m \rangle \subseteq \langle a^{n'} \rangle$.
Combine with $|H| = |H'| \implies H = H'$

Definition 1.6.2 (direct product)**.** Let $G_1, G_2, ..., G_\ell$ be groups.

$$G_1 \times \cdots \times G_\ell := \{(x_1, x_2, ..., x_\ell) | x_i \in G_i\}$$

is called the **direct product** of $G_1, G_2, ..., G_\ell$ which is a group under

$$(x_1, x_2, ..., x_n)(y_1, y_2, ..., y_n) = (x_1 y_1, x_2 y_2, ..., x_n y_n)$$

Example 1.6.1. $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \simeq \mathbb{Z}/pq\mathbb{Z}$ with $\gcd(p, q) = 1$
Claim: $m := o(\overline{1}, \overline{1}) = pq$

- $pq(\overline{1}, \overline{1}) = (\overline{pq}, \overline{pq}) = (\overline{0}, \overline{0}) \rightsquigarrow m | pq$
- $(\overline{0}, \overline{0}) = m(\overline{1}, \overline{1}) = (\overline{m}, \overline{m}) \rightsquigarrow p, q | m \rightsquigarrow pq | m$

  Since $|\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}| = pq = |\langle(\overline{1}, \overline{1})\rangle| \implies \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \simeq \langle(\overline{1}, \overline{1})\rangle \simeq \mathbb{Z}/pq\mathbb{Z}$

Property 1.6.4. G is abelian and $o(a) = p, o(b) = q$ with $\gcd(p, q) = 1 \implies o(ab) = pq$

Definition 1.6.3. The **exponent** of a finite abelian group G is defined to be $\exp G = \min\{m \in \mathbb{N} | x^m = e\ \forall\ x \in G\}$

Note: $\forall\ x \in G,\ \langle x \rangle \leq G \rightsquigarrow o(x) = |\langle x \rangle| \big| |G| \rightsquigarrow x^{|G|} = e$

Property 1.6.5. Let G be a finite abelian group. Then G is cyclic $\iff \exp G = |G|$

Proof:

($\Rightarrow$) $G = \langle a \rangle$. Then for a, $|G|$ is the smallest positive integer n s.t. $a^n = e \rightsquigarrow \exp G = |G|$

($\Leftarrow$) **Claim**: If a is a element in G has max order, then $\exp G = o(a)$

pf. If $\exists b \in G$ s.t. $o(b) \nmid o(a)$, then $\begin{cases} o(a) = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} \\ o(b) = p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n} \end{cases}$ with $\alpha_i, \beta_i \geq 0$.

Since $o(b) \nmid o(a)$, there exists i s.t. $\beta_i > \alpha_i$ (Say $\alpha_1 > \beta_1$).

Let $a' = a^{p_1^{\alpha_1}}, b' = b^{p_2^{\beta_2} p_3^{\beta_3} \cdots p_n^{\beta_n}}$, then $o(a') = p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ and $o(b') = p_1^{\beta_1}$ are coprime. Thus, $o(a'b') = p_1^{\beta_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_n^{\alpha_n} > o(a)$ ($\rightarrow\leftarrow$). $\square$

Hence, $o(a) = \exp(G) = |G| \rightsquigarrow G = \langle a \rangle$ is cyclic. $\square$

Theorem 1.6.1. Let F be a finite field, then $F^\times$ is cyclic group.

Proof: We only need to prove that $\exp(F^\times) = |F^\times|$

Let $n = \exp(F^\times) < \infty$, then $x^n = 1 \ \forall x \in F^\times$

(Fact: $x^n - 1 = 0$ has at most n roots)

It $n < |F^\times|$, then $\exists\ \alpha \in F^\times$ s.t. $a^n - 1 \neq 0$ ($\rightarrow\leftarrow$) $\rightsquigarrow n = |F^\times|$ $\square$

Remark 1.6.1. For any positive integer $m, n, r > 1$, there exists a finite group G with $a, b \in G$ s.t. $o(a) = m, o(b) = n, o(ab) = r$
(You can come back and see it again after learn Field theory.)

Proof: Pick a prime p s.t. $p \nmid 2mnr$. Then $\gcd(p, 2mnr) = 1 \rightsquigarrow \overline{p} \in (\mathbb{Z}/2mnr\mathbb{Z})^\times$

Let $o(\overline{p}) = s$ i.e. $\overline{p}^s = \overline{1}$ in $(\mathbb{Z}/2mnr\mathbb{Z})^\times \rightsquigarrow 2mnr | p^s - 1$. (Denote $p^s = q$)

Note: $|F| < \infty \Rightarrow\ F = p,\ \mathbb{Z}/p\mathbb{Z} \subseteq F$. Let $\dim_{\mathbb{Z}/p\mathbb{Z}} F = n \rightsquigarrow F \simeq (\mathbb{Z}/p\mathbb{Z})^n \Rightarrow |F| = p^n$)

Since $\exists\ |\mathbb{F}_q| = q$ and $\mathbb{F}_q^\times$ is cyclic with $2mnr | q - 1 \rightsquigarrow \exists\ u, v, w \in \mathbb{F}^\times$ s.t. $o(u) = 2m, o(v) = 2m, o(w) = 2r$. Since $o(u), o(v), o(w) > 2 \rightsquigarrow u \neq u^{-1}, v \neq v^{-1}, w \neq w^{-1}$.

Let $a = \begin{pmatrix} u & 1 \\ 0 & u^{-1} \end{pmatrix}$, $b = \begin{pmatrix} v & 0 \\ t & v^{-1} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_q)$. Also, $ab = \begin{pmatrix} uv + t & v^{-1} \\ u^{-1}t & u^{-1}v^{-1} \end{pmatrix}$

$ch_a(x) = (x-u)(x-u^{-1}) \rightsquigarrow a \sim \begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix} \rightsquigarrow o(a) = 2m$. Similarly, $o(b) = 2n$.

$ch_{ab}(x) = x^2 - (u^{-1}v^{-1} + uv + t)x + 1$. Choose $t = w + w^{-1} - (u^{-1}v^{-1} + uv)$.

Then $ab \simeq \begin{pmatrix} w & 0 \\ 0 & w^{-1} \end{pmatrix} \rightsquigarrow o(ab) = 2r$ $\square$

Finally, in $\mathrm{SL}_2(\mathbb{F}_q)$, $-I$ is the unique element of order 2.

$\Longrightarrow\ o(\overline{a}) = m, o\left(\overline{b}\right) = n, o\left(\overline{ab}\right) = r$ in $\mathrm{SL}_2(\mathbb{F}_q)/\langle I \rangle$

1.7 Group action

Definition 1.7.1 (Group action)**.** 1. An **action** of G on S ($G \curvearrowright S$) is a group homo. $\pi : G \to \mathrm{Perm}(S)$

2. An **action** of G on S is a map $\begin{array}{ccc} G \times S & \to & S \\ (x, s) & \mapsto & xs \end{array}$

- $es = s \ \forall \ s \in S$
- $(xy)s = x(ys) \ \forall \ x, t \in G, s \in S$

Note: Two definition are equivalent:
$1 \Rightarrow 2 : \forall \ x \in G, s \in S$, define $xs = \pi(x)(s)$

- $es = \pi(e)(s) = \mathrm{id}(s) = s$
- $(xy)(s) = \pi(xy)(s) = (\pi(x)\pi(y))(s) = \pi(x)(\pi(y)(s)) = x(ys)$

$2 \Rightarrow 1 :$ Define $\pi(x)(s) = xs \ \forall \ x \in G, s \in S$

- $\pi(x)$ is permutation:
  - $\pi(x)$ is $1-1$: $xs_1 = xs_2 \rightsquigarrow s_1 = x^e s_1 = x^{-1}(xs_1) = x^{-1}(xs_2) = es_2 = s_2$
  - $\pi(x)$ is onto: $\pi(x^{-1}s) = x(x^{-1}s) = (xx^{-1})s = s$
- π is group homo.
  - $\pi(xy)(s) = (xy)(s) = x(ys) = \pi(x)(\pi(y)(s)) \rightsquigarrow \pi(xy) = \pi(x)\pi(y)$

Property 1.7.1. $\ker \pi = \{x \in G | xs = s \ \forall s \in S\}$ is the group og G fixing S

$$\Longrightarrow \begin{array}{ccc} G/\ker \pi \times S & \to & S \\ (\overline{x}, s) & \mapsto & xs \end{array} \rightsquigarrow G/\ker f \hookrightarrow \mathrm{Perm}\, S$$

Definition 1.7.2 (faithful)**.** $G \curvearrowright S$ and is **faithful** if $\pi : G \hookleftarrow \mathrm{Perm}\, S$

Definition 1.7.3 (orbit)**.** Let $G \curvearrowright S$ and $s \in S$. The **orbit** of s is the subset $Gs := \{xs | x \in G\} \subseteq S$

Property 1.7.2. The set consisting of orbits forms a partition of S.

Proof: Define an equivalence relation on S by

$$s \sim t \iff t = xs \text{ for some } x \in G$$

- $s \sim s$, since $s = es$
- $s \sim t$, say $t = xs \rightsquigarrow s = x^{-1}t \rightsquigarrow t \sim s$
- $s \sim t, t \sim u$, say $t = xs, u = yt \rightsquigarrow u = yt = y(xs) = (yx)s \rightsquigarrow s \sim u$

Also, the equivalence of s is the G-orbit of s.
Note.

- $Gs = Gt \iff s \sim t \iff \exists \ x \in G$ s.t. $t = xs$
- $|Gs| = 1 \iff Gs = \{s\} \iff G_s = G$

where G_s is **isotropy group** of s in G is defined by $\{x \in G | xs = s\}$

□

Theorem 1.7.1. Let $G \curvearrowright S$ and $s \in S$. Then $|Gs| = (G : G_s)$.
In particular, if G is finite, then $|G| = |Gs| \cdot |G_s|$

Proof: Define $\varphi : \begin{array}{ccc} \{\text{left cosets of } G_s\} & \to & Gs \\ xG_s & \mapsto & xs \end{array}$

- well defined & 1−1: $xs = ys \iff (y^{-1}x)s = s \iff y^{-1}x \in G_s \iff xG_s = yG_s$
- onto: $\forall x \in G\ \varphi(xG_s) = xs$

□

Example 1.7.1. Basis example

- Action by left multiplication
  - $\begin{array}{ccc} G \times G & \to & G \\ (x, y) & \mapsto & xy \end{array}$
    - $G \xhookrightarrow{\text{Cayley thm.}} \operatorname{Perm} G$
    - $\forall x, y \in G,\ y = (yx^{-1})x \rightsquigarrow$ there is only one orbit
  - Let $H \leq G$ and $S = \{\text{left cosets of } H\}$.
    $\begin{array}{ccc} G \times S & \to & S \\ (x, yH) & \mapsto & xyH \end{array}$
    - $\varphi : G \to \operatorname{Perm} S$
    - $\ker\varphi = \{x \in G | xyH = yH\ \forall y \in G\} = \{x \in G | y^{-1}xy \in H\ \forall y \in G\} = \bigcap_{y \in G} yHy^{-1} \subseteq H$
    - $\ker\varphi$ is the largest normal subgroups of G obtain in H:
      If $N \lhd G, N \leq H \rightsquigarrow \forall x \in G, N = xNx^{-1} \subseteq xHx^{-1} \rightsquigarrow N \leq \ker\varphi$
- Action by conjugation
  - $\begin{array}{ccc} G \times G & \to & G \\ (x, y) & \mapsto & xyx^{-1} \end{array}$
    - $\varphi : G \to \operatorname{Inn} G$ with $\ker\varphi = Z_G$
    - $y \in G \begin{cases} Gy = \{xyx^{-1} | x \in G\} =: \operatorname{conj}_G(y) \\ G_y = \{x | xyx^{-1} = y\} = Z_y : \text{the } \textbf{centralizer} \text{ of } y \text{ in } G \end{cases}$
    - $|\operatorname{conj}_G(x)| = (G : Z_x)$
  - $H \lhd G$, $\begin{array}{ccc} G \times H & \to & H \\ (x, h) & \mapsto & xhx^{-1} \end{array}$
    - $\varphi : G \to \operatorname{Aut}(H)$
    - $\ker\varphi = \{x \in G | xhx^{-1} = h\ \forall h \in H\} = Z_H$: the **centralizer** of H in G
    - $G/H \hookrightarrow \operatorname{Aut}(H)$

- $H \leq G$, $\begin{array}{ccc} N(H) \times H & \to & H \\ (x,h) & \mapsto & xhx^{-1} \end{array}$
  - $N(H)/H \hookrightarrow \mathrm{Aut}(H)$
- $H \leq G, S = \{\text{conjuates of } H\}$. $\begin{array}{ccc} G \times S & \to & S \\ (x, yHy^{-1}) & \mapsto & xyH(xy)^{-1} \end{array}$
  - $G \curvearrowright S$ transitively (i.e. $yHy^{-1} = (yx^{-1})(xHx^{-1})(yx^{-1})^{-1}$)
  - $G_H = \{x \in G | xHx^{-1} = H\} = N(H)$
  - $|GH| = (G : G_H) = (G : N(H))$

Property 1.7.3. If p is a prime and $H \leq S_p$ with $|H| = p$, then

$$N(H)/H = N(H)/Z_H \simeq \mathrm{Aut}(H)$$

Proof:

- $\mathrm{Aut}\,(\mathbb{Z}/p\mathbb{Z}) = \{f_k | 1 \leq k \leq p-1\}$, where $\begin{array}{rccc} f_k : & \mathbb{Z}/p\mathbb{Z} & \to & \mathbb{Z}/p\mathbb{Z} \\ & \overline{1} & \mapsto & \overline{k} \end{array}$

  $f_{k_1} \circ f_{k_2}(\overline{1}) = f_{k_1}(\overline{k_2}) = \overline{k_1 k_2} = f_{k_1 k_2}(\overline{1}) \implies \mathrm{Aut}\,(\mathbb{Z}/p\mathbb{Z}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times \simeq C_{p-1}$
- We know that
$$|N(H)| = \frac{|S_p|}{|\text{conjugates of } H|}$$

  Assume $\tau := (1\ 2\ \cdots\ p) \in H \rightsquigarrow H = \langle \tau \rangle$ contain $(p-1)$ p-cycles.

  Also, $H' = \alpha H \alpha^{-1} = \langle (\alpha(1)\ \alpha(2)\ \cdots\ \alpha(p)) \rangle$ contain $(p-1)$ p-cycles.

  By Lagrange thm, $|H \cap H'||H| = p \implies |H \cap H'| = 1$ or $p \implies H = H'$ or $H \cap H' = \{\mathrm{id}\}$

  In S_p, there are $p!/p$ p-cycles. Let m be the number of conjugates of H

  $\rightsquigarrow m = \frac{(p-1)!}{p-1} = (p-2)!$. Hence, $|N(H)| = p(p-1)$

  We have $Z_H = Z_\tau$, then we have
$$|Z_\tau| = \frac{S_p}{|\text{conjugate of } \tau|} = \frac{p!}{\frac{p!}{p}} = p$$

  Since $H \leq Z_\tau$ and $|H| = p = |Z_\tau| \implies H = Z_H$
- By $|N(H)/Z_H| = p - 1 = |\,\mathrm{Aut}(H)|$ and $N(H)/Z_H \hookrightarrow \mathrm{Aut}(H) \implies N(H)/Z_H \simeq \mathrm{Aut}(H)$

□

Remark 1.7.1. If we define group action by $\begin{array}{ccc} S \times G & \to & G \\ (s,x) & \mapsto & sx \end{array}$

- $se = s\ \forall s \in S$
- $s(xy) = (sx)y\ \forall x, y \in G, s \in S$

Example 1.7.2.

- $\begin{array}{ccc} G \times G & \to & G \\ (s,x) & \mapsto & x^{-1}sx \end{array}$

  (If we define as $(s,x) \mapsto xsx^{-1} \rightsquigarrow (sx)y = yxsx^{-1}y^{-1} \neq (sx)y$ which is not a group action)

- Let $H \leq G$ and $K \leq G$, consider $\begin{array}{ccc} (H \times K) \times G & \mapsto & G \\ ((h,k),x) & \mapsto & hxk^{-1} \end{array}$

Definition 1.7.4 (G-set, G-map)**.** Let S_1 and S_2 be **G-sets** i.e. $\exists G \curvearrowright S_1, G \curvearrowright S_2$

A **G-map** $f : S_1 \to S_2$ is a map preserving G-action i.e. $\forall x \in G, f(xs) = xf(s)\ \forall s \in S_1$

Example 1.7.3. Let S be a G-set and $\mathcal{R} = \{\text{real value function on } S\}$, $\forall x \in G, f \in \mathcal{R}$, define $(xf)(s) = f(x^{-1}s)$ is a G-map

1.8 Simpleness of A_n

Theorem 1.8.1. A_5 is simple:

- The cycle structure table of S_5:

cycle type	number	order	parity
id	1	1	even
(12)	$\binom{5}{2} = 10$	2	odd
(123)	$\binom{5}{3} \times 2 = 20$	3	even
(1234)	$\frac{P_4^5}{4} = 30$	4	odd
(12345)	$\frac{5!}{5} = 24$	5	even
(12)(34)	$\binom{5}{2} \times \binom{3}{2} * \frac{1}{2} = 15$	2	even
(12)(345)	$\binom{5}{3} \times 2 = 20$	6	odd

  Note: two elements of S_5 are conjugate in $S_5 \iff$ they have same cycle type

- For A_5:

  - 3-cycle: say $\alpha = (123)$

$$20 = |\text{conj}_{S_5}(\alpha)| = \frac{|S_5|}{|Z_\alpha^{(S_5)}|} \rightsquigarrow |Z_\alpha^{(S_5)}| = 6$$

    and thus $Z_\alpha^{(S_5)} = \{\text{id}, \alpha, \alpha^2, \alpha(45), \alpha^2(45)\}$
    $\rightsquigarrow Z_\alpha^{(A_5)} = \{\text{id}, \alpha, \alpha^2\} \rightsquigarrow |\text{conj}_{A_5}(\alpha)| = \frac{|A_5|}{3} = 20.$
    Hence, *all* 3-cycle in A_5 are conjugate.

- $2-2$-cycle: say $\alpha = (12)(34)$

$$15 = |\text{conj}_{S_5}(\alpha)| = \frac{|S_5|}{|Z_\alpha^{(S_5)}|} \rightsquigarrow |Z_\alpha^{(S_5)}| = 8$$

and thus $Z_\alpha^{(S_5)} = \{\text{id}, \alpha, (12), (34), (13)(24), (14)(23), (1324), (1423)\}$
$\rightsquigarrow Z_\alpha^{(A_5)} = \{\text{id}, \alpha, (13)(24), (14)(23)\} \rightsquigarrow |\text{conj}_{A_5}(\alpha)| = \frac{|A_5|}{4} = 15.$
Hence, *all* $2-2$-cycle in A_5 are conjugate.

- 5-cycle: say $\alpha = (12345)$

$$20 = |\text{conj}_{S_5}(\alpha)| = \frac{|S_5|}{|Z_\alpha^{(S_5)}|} \rightsquigarrow |Z_\alpha^{(S_5)}| = 5$$

and thus $Z_\alpha^{(S_5)} = \{\text{id}, \alpha, \alpha^2, \alpha^3, \alpha^4\}$
$\rightsquigarrow Z_\alpha^{(A_5)} = Z_\alpha^{(S_5)} \rightsquigarrow |\text{conj}_{A_5}(\alpha)| = \frac{|A_5|}{5} = 12$
Hence, there are two conjugacy class of 5-cycle in A_5, each of then have 12 elements. (i.e. $(12354) = (45)(12345)(45)^{-1}$)

- A_5 is simple:

If $\{e\} \neq H \lhd A_5$, i.e. $\forall x \in A_5,\ xHx^{-1} = H$, then we find that H must be a union of some conjugacy class of A_5. But no sum off union of $1, 20, 15, 12, 12$ (include 1) get a proper divisor of 60 $(\rightarrow\leftarrow) \rightsquigarrow A_5$ is simple

We will prove A_n (≥ 5) is simple in Homework 8 with different way, since this method is too complicated.

1.9 Class formula

Definition 1.9.1. Let $G \curvearrowright S$, denote $S^G := \{s \in S | gs = s\ \forall g \in G\}$ is the fix part of S by G.

Observation: Let $G \curvearrowright S$ and $|G|, |S| < \infty$, then

- $s \in S^G \iff |Gs| = 1,\ s \notin S^G \rightsquigarrow G_s \neq G \rightsquigarrow |Gs| = (G : G_s) > 1$
- Assume that $\{Gs_1, Gs_2, ..., Gs_n\}$ is the set of different orbit in S. After rearrangement, assume that $s_1, s_2, ..., s_r \in S,\ s_{r+1}, ..., s_n \notin S^G$. Then

$$\left(\bigcup_{i=1}^{r} Gs_i\right) \cup \left(\bigcup_{i=r+1}^{n} Gs_i\right) = S \implies |S| = |S^G| + \sum_{i=r+1}^{n} (G : G_{s_i})$$

Theorem 1.9.1. (Class formula) Let G be a finite group. Then $G = Z_G$ or $\exists x_1, x_2, ..., x_m \in G \setminus Z_G$ s.t. $|G| = |Z_G| + \sum_{i=1}^{m} (G : Z_{x_i})$

Proof: Consider $\begin{matrix} G\times G & \to & G \\ (x,y) & \mapsto & xyx^{-1}\end{matrix}$.

Then $G^G=\{y\in G|xyx^{-1}=y\ \forall x\in G\}=Z_G$ and $G_y=\{x\in G|xyx^{-1}=y\}=Z_y$. By the above observation, $|G|=|Z_G|+\sum_{i=1}^{m}(G:Z_{x_i})$ for some $x_i\notin Z_G$ □

Property 1.9.1. Let $|G|=p^n$ (then we called G is a p-**group**) for some p and $n\in\mathbb{N}$. Then $Z_G\neq\{0\}$

By class formula, $|G|=|Z_G|+\sum_{i=1}^{n}(G:Z_{x_i})$

$(G:Z_{x_i})>1$ and $|G|=p^n\rightsquigarrow p|(G:Z_{x_i})\rightsquigarrow p||Z_G|$, which means $|Z_G|\neq\{0\}$

Property 1.9.2. If $|G|=p^2$, then G is abelian.

We know $|Z_G|=p$ or p^2.

- $|Z_G|=p^2\implies Z_G=G$, which means G is abelian
- $|Z_G|=p\rightsquigarrow(G:Z_G)=p\rightsquigarrow Z_G\lhd G$ and $G/Z_G\simeq C_p\rightsquigarrow G=\bigcup_{i=0}^{p-1}x^iZ_G$

For $z_1,z_2\in G$, we can write $z_1=x^{i_1}a_1, z_2=x^{i_2}a_2$ with $a_1,a_2\in Z_G$

$\implies z_1z_2=(x^{i_1}a_1)(x^{i_2}a_2)=x^{i_1+i_2}a_1a_2=x^{i_2+i_1}a_2a_1=z_2z_1$, since $a_1,a_2\in Z_G$. i.e. G is abelian $\implies |Z_G|=p^2$ $(\to\leftarrow)$

Property 1.9.3. If $|G|=p^n$, then G is solvable.

Claim: $\forall 0\le k\le n,\exists G_k\lhd G$ s.t. $|G_k|=p^k$ and $G_i\lhd G_{i+1}\ \forall i=0,1,...,(n-1)$

pf : By induction on n, $n=1\rightsquigarrow|G|=p$ is OK! Let $n>1$.

By Prop.1.9.1 $Z_G\neq\{e\}\rightsquigarrow\exists\ e\neq a\in Z_G$ say $o(a)=p^k\implies o\left(a^{p^{k-1}}\right)=p$

So we may let $a\in Z_G$ with $o(a)=p$

By induction hypothesis, $\forall 0\le k\le n-1\ \exists\ \overline{G_k}\lhd G/\langle a\rangle$ s.t. $|\overline{G_k}|=p^k$ and $\overline{G_i}\lhd\overline{G_{i+1}}\ \forall i=0,1,...,(n-2)$

By 3rd iso.thm, write $\overline{G_k}=G_{k+1}/\langle a\rangle$ with $G_{k+1}\lhd G$ and $G_0=\{0\}$. Then $|G_i|=p^i$ and $G_i\lhd G_{i+1}\ \forall i=0,1,...,n-1$

Theorem 1.9.2. (Cauchy theorem) If $p\big||G|$ with p is prime, then $\exists a\in G$ s.t. $o(a)=p$

Proof:

- G is abelian: By induction on $|G|$, $|G|=p\rightsquigarrow G\simeq C_p$ done!

Let $|G|>p$, $e\neq a\in G$ and define $H:=\langle a\rangle$

  - $p|o(a)\rightsquigarrow o\left(a^{\frac{|H|}{p}}\right)=p$
  - $p\not|o(a)\rightsquigarrow p\big||G/H|<|G|$. By induction hypothesis, $\exists\ xH\in G/H$ s.t. $o(xH)=p$. $(xH)^{o(x)}=x^{o(x)}H=H\rightsquigarrow p|o(x)\implies o\left(x^{\frac{o(x)}{p}}\right)=p$

- G is non-abelian:

- $p \big| |Z_G|$: Since Z_G is abelian, $\exists a \in Z_G \leq G$ s.t. $o(a) = p$
- $p \not| |Z_G| : |G| = |Z_G| + \sum_{i=1}^{n} (G : Z_{x_i}) \rightsquigarrow \exists\ i$ s.t. $p \not| (G : Z_{x_i}) \rightsquigarrow p \big| |Z_{x_i}| < |G|$
  By induction hypothesis, $\exists a \in Z_{x_i} \leq G$ s.t. $o(a) = p$

□

Property 1.9.4. Let G be a p-group. If $G \curvearrowright S$, then $|S| \equiv |S^G| \pmod{p}$
$|S| = |S^G| + \sum_{i=1}^{n} (G : Z_{x_i})$, since $x_i \notin S^G \rightsquigarrow (G : Z_{x_i}) > 1$ and thus $p|(G : Z_{x_i})$
$\rightsquigarrow |S| \equiv |S^G| \pmod{p}$

Remark 1.9.1. Let $H \lhd G, K \leq G$ and $G = HK$

$$(h_1k_1)(h_2k_2) = h_1(k_1h_2k_1^{-1})_{\in H}k_1k_2 = (h_1h_2')(k_1k_2)$$

and we define $k_1h_2k^{-1} =: \varphi_{k_1}(h_2)$ and write

$$G = HK \simeq H \rtimes_{\varphi} K$$

1.10 Sylow theorems

Definition 1.10.1. Let $|G| = p^{\alpha}\gamma$ with $p \not| \gamma$ and $\alpha \geq 1$

- A subgroup of order p^{α} is called a **p-Sylow subgroup** of G
- $\mathrm{Syl}_p(G)$ is defined be the set of p-Sylow subgroups of G
- $n_p = |\mathrm{Syl}_p(G)|$

First, we re-prove Cauchy theorem by more artificial group action.

Theorem 1.10.1. (Cauchy theorem) If $p \big| |G|$, then $\exists a \in G$ s.t. $o(a) = p$

Proof: Let $S = \{(a_1, a_2, ..., a_p) \in G^p | a_1a_2 \cdots a_p = e\}$

Consider
$$\begin{array}{ccc} \mathbb{Z}/p\mathbb{Z} \times S & \to & S \\ \big(\overline{k}, (a_1, a_2, ..., a_p)\big) & \mapsto & (a_{k+1}, a_{k+2}, ..., a_p, a_1, ..., a_k) \end{array}$$

(well defined: $(a_1 \cdots a_k)(a_{k+1} \cdots a_p) = e \rightsquigarrow (a_{k+1} \cdots a_p)(a_1 \cdots a_k) = e$)
By the formula, $|S^{\mathbb{Z}/p\mathbb{Z}}| \equiv |S| = |G|^{p-1} = 0 \pmod{p}$.
$(a_1, a_2, ..., a_p) \in S^{\mathbb{Z}/p\mathbb{Z}} \iff a_1 = a_2 = \cdots = a_p = a \iff a^p = e$
Since $(e, e, ..., e) \in S^{\mathbb{Z}/p\mathbb{Z}} \rightsquigarrow |S^{\mathbb{Z}/p\mathbb{Z}}| \neq 0$, pick $(a, a, ..., a) \in S^{\mathbb{Z}/p\mathbb{Z}}$ with $a \neq e$
Then $o(a) = p$. □

Theorem 1.10.2. (Sylow theorem)

(1) $n_p \geq 1$

(2) Let H be a p-subgroup of G. Then $\exists P \in \mathrm{Syl}_p(G)$ s.t. $H \leq P$

(3) All p-Sylow subgroups are conjugate

(4) $n_p \equiv 1 \pmod{p}, n_p \big| |G| \implies n_p | \gamma$

Proof:

(1) By induction on $|G|$, $|G| = p$ done! Let $|G| > p$

- $\exists H \lneq G$ with $p \nmid (G:H) \rightsquigarrow p^\alpha \big| |H| \xrightarrow{\text{by induction}} \exists P \leq H$ s.t. $|P| = p^\alpha \rightsquigarrow P \in \mathrm{Syl}_p(G)$
- $\forall H \lneq G, p|(G:H)$. By class formula, $p|(G:Z_{x_i}) \rightsquigarrow p||Z_G|$
  By Cauchy theorem, $\exists a \in Z_G$ s.t. $o(a) = p$. Since $|G/\langle a\rangle| = p^{\alpha=1}\gamma < |G|$, by induction hypothesis, $\exists P/\langle a\rangle \leq G/\langle a\rangle$ s.t. $|P/\langle a\rangle| = p^{\alpha-1} \rightsquigarrow |P| = p^\alpha \rightsquigarrow P \in \mathrm{Syl}_p(G)$

(2) **Claim**: $H \leq N(P)$ for some $P \in \mathrm{Syl}_p(G) \implies H \leq P$

$pf.$ $\begin{cases} H \leq N(P) \\ P \lhd N(P) \end{cases} \implies HP \leq N(P) \leq G$ and $HP/P \simeq H/(H \cap P)$

If $(H : H \cap P) \neq 1$. Since $(H : H \cap P)$ is power of $p, |HP| = p^{\alpha+\beta}$ $(\rightarrow\leftarrow)$

Hence, $(H : H \cap P) = 1 \rightsquigarrow H \cap P = H \rightsquigarrow H \leq P$ □

Let $P \in \mathrm{Syl}_p(G)$ and $S = \{\text{conjugate of } P\} \subseteq \mathrm{Syl}_p(G)$

(Recall that $|S| = (G : N(P))$. $P \leq N(P) \rightsquigarrow p^\alpha | N(P) \rightsquigarrow p \nmid |S|$)

Consider $\begin{matrix} H \times S & \to & S \\ (x, P) & \mapsto & xPx^{-1} \end{matrix}$ and we have $0 \neq |S| \equiv |S^H| \pmod p \rightsquigarrow |S^H| \neq 0$.

Pick $Q \in S^H$, by def, $hQh^{-1} = Q$ $\forall h \in H \implies H \leq N(Q) \implies H \leq Q$

(3) If $P, P' \in \mathrm{Syl}_p(G)$, then apply the same agreement at (2) by $H = P' \rightsquigarrow \exists\, Q \in S^{P'}$ s.t. $P' \leq Q$. Since $|P'| = |Q| = p^\alpha$, $P' = Q = xPx^{-1}$ for some $x \in G$.

(4) As above, let $H \in \mathrm{Syl}_p(G)$. Again $Q \in S^H \implies H \leq N(Q) \implies H \leq Q \implies Q = H$ (Since $|Q| = |H|$) i.e. $S^H = \{H\}$.

$n_p = |S| \equiv |S^H| \pmod p$. Again again, $n_p = (G : N(P)) \implies n_p || G|$

□

Corollary 1.10.1. If $n_p = 1$, let $P \in \mathrm{Syl}_p(G)$. Then $P \lhd G$.
$\forall x \in G, xPx^{-1} \in \mathrm{Syl}_p(G) \rightsquigarrow xPx^{-1} = P \rightsquigarrow P \lhd G$.

Property 1.10.1. Let $|G| = pq$ with p, q are primes with $p < q$ and $q \not\equiv 1 \pmod p$. Then G is cyclic.

Proof: By Sylow theorem, $\begin{cases} n_p = 1 + ph | q \implies n_p = 1 \implies \exists! H \in \mathrm{Syl}_p(G) \text{ s.t. } H \lhd G \\ n_q = 1 + qk | p \implies n_q = 1 \implies \exists! K \in \mathrm{Syl}_q(G) \text{ s.t. } K \lhd G \end{cases}$

- $|H \cap K| \big| |H|, |K| \xrightarrow{\gcd|H|,|K|=1} |H \cap K| = 1 \rightsquigarrow H \cap K = \{e\}$
- $\forall h \in H, k \in K$, $\begin{cases} K \lhd G \implies hkh^{-1} \in K \rightsquigarrow hkh^{-1}k^{-1} \in K \\ H \lhd G \implies khk^{-1} \in H \rightsquigarrow hkh^{-1}k^{-1} \in H \end{cases}$

$$\implies hkh^{-1}k^{-1} \in H \cap K = \{e\} \implies hk = kh$$

- $|G| = |H||K|$ and $G \simeq H \times K \simeq C_p \times C_q \simeq C_{pq}$

□

Example 1.10.1. Classify group

- By Sylow theorem:

  $|G| = 45 \implies G$ is abelian ($G \simeq \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ or $(\mathbb{Z}/3\mathbb{Z})^2 \times \mathbb{Z}/5\mathbb{Z}$)

  pf : By Sylow theorem, $n_3 = n_5 = 1$, which means $\exists!\ H \in \mathrm{Syl}_3(G), K \in \mathrm{Syl}_5(G)$ s.t. $H \lhd G, K \lhd G$. Similarly, $G \simeq H \times K \simeq C_9 \times C_5 \simeq C_{45}$.

- Consider commutator of G and using n_p to calculate $|G|$:

  $|G| = 255 \implies G$ is abelian ($G \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z}$)

  pf : By Sylow theorem, $n_{17} = 1 \implies \exists!\ H \in \mathrm{Syl}_{17}(G)$ s.t. $H \lhd G$

  We find that $|G/H| = 15 \rightsquigarrow G$ is abelian $\rightsquigarrow [G : G] \leq H \implies |[G : G]|\big|17$

  Also, $n_3 = 1$ or 85, $n_5 = 1$ or 51.

  If $n_3 = 85$ and $n_5 = 51$, then every 3-Sylow subgroup would require 2 elements and every 5-Sylow subgroup would require 4 elements. Then, G have at least $85 \cdot 2 + 51 \cdot 51 = 374$ ($\rightarrow\leftarrow$). That means at least one of 3-Sylow subgroup or 5-Sylow subgroup is normal.

  Case.1 $\exists!\ K \in \mathrm{Syl}_3(G)$ with $K \lhd G$, $|G/K| = 85 \rightsquigarrow G/K$ is abelian $\rightsquigarrow [G : G] \leq K \implies |[G : G]|\big|3 \implies [G, G] = \{e\} \implies G$ is abelian.

  Case.2 Similarly.

- Consider $N(H)H \hookrightarrow \mathrm{Aut}(H)$:

  $|G| = 1463 \implies G$ is abelian ($G \simeq \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/19\mathbb{Z}$)

  pf : By Sylow theorem, $n_7 = 1$, which means $\exists!\ H \in \mathrm{Syl}_7(G)$ with $H \lhd G$. $|G/H| = 11 \times 19 \implies G/H$ is cyclic $\implies \exists K/H \lhd G/H$ s.t. $|K/H| = 19$ and $K \lhd G \rightsquigarrow |K| = 133$

  Recall: $\begin{matrix} G \times K & \to & K \\ (x, k) & \mapsto & xkx^{-1} \end{matrix} \rightsquigarrow f : G \to \mathrm{Aut}(K) \rightsquigarrow G/Z_K \simeq \mathrm{Im}\, f \leq \mathrm{Aut}(K)$

  So $\begin{cases} |\mathrm{Im}\, f|\big||G| = 7 \times 11 \times 19 \\ |\mathrm{Im}\, f|\big||\mathrm{Aut}(K)| = \phi(133) \end{cases} \implies |\mathrm{Im}\, f| = 1 \implies G = Z_K \implies K \leq Z_G$

  Now, for $P \in \mathrm{Syl}_{11}(G)$, $G = KP$ with $K \in Z_G$ and P is abelian $\implies G$ is abelian.

- Use kernel to find a non-trivial normal proper subgroup

  No group G of order 36 is simple.

  pf: Let $H \in \mathrm{Syl}_3(G)$ and $S = \{\text{left cosets of } H\}$

  Consider $\begin{matrix} G \times S & \to & S \\ (x, aH) & \mapsto & (xa)H \end{matrix} \rightsquigarrow f : G \to S_4$

  Since $|G| = 36 > |S_4|$, which means $\ker f \neq \{e\}$ and $\ker f \in H \rightsquigarrow \ker f \neq G$

  $\implies \ker f \lhd G$

1.11 Semidirect product

Recall: $\begin{cases} H \lhd G, K \lhd G \\ H \cap K = \{0\} \end{cases} \implies HK \simeq H \times K$

In general, $\begin{cases} H \lhd G, K \leq G \\ H \cap K = \{e\} \end{cases} \implies HK \leq G$ and $HK \longleftrightarrow \{(h,k) | h \in H, k \in K\}$

$(1-1$: $h_1k_1 = h_2k_2 \rightsquigarrow h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K = \{e\} \rightsquigarrow h_1 = h_2, k_1 = k_2)$
and $(h_1k_1)(h_2k_2) = h_1(k_1h_2k_1^{-1})k_1k_2 \in HK$

Definition 1.11.1 (**Semidirect product**)**.** For two groups H, K and a group homo. $\varphi : K \to \mathrm{Aut}(H)$. Define

$$H \rtimes_\varphi K = \{(h,k) | h \in H, k \in K\}$$

with operation

$$(h_1, k_1)(h_2, k_2) = (h_1\varphi(k_1)(h_2), k_1k_2)$$

Now, we see some property of semidirect product:

- identity $= (e, e)$:
  $(e,e)(h,k) = (e\varphi(e)(h), ek) = (\mathrm{id}(h), k) = (h,k)$
  $(h,k)(e,e) = (h\varphi(k)(e), ke) = (h,k)$
- $(h,k)^{-1} = (\varphi(k^{-1})(h^{-1}), k^{-1})$:
  $(\varphi(k^{-1})(h^{-1}), k^{-1})(h,k) = (\varphi(k^{-1})(h^{-1})\varphi(k^{-1})(h), e) = (\varphi(k^{-1})(e), e) = (e,e)$
  $(h,k)(\varphi(k^{-1})(h^{-1}), k^{-1}) = (h\varphi(k)(\varphi(k^{-1})(h^{-1})), e) = (h\,\mathrm{id}(h^{-1}), e) = (e,e)$
- associativity:

$$\begin{aligned} ((h_1,k_1)(h_2,k_2))(h_3,k_3) &= (h_1\varphi(k_1)(h_2), k_1k_2)(h_3,k_3) \\ &= (h_1\varphi(k_1)(h_2)\varphi(k_1k_2)(h_3), k_1, k_2k_3) \\ &= (h_1,k_1)(h_2\varphi(k_2)(h_3), k_2k_3) = (h_1,k_1)((h_2,k_2)(h_3,k_3)) \end{aligned}$$

- $\begin{matrix} H & \simeq & H \times \{e\} \\ h & \mapsto & (h,e) \end{matrix}$: $(h_1,e)(h_2,e) = (h_1\varphi(e)(h_2), e) = (h_1h_2, e)$
  It clear that, $K \simeq \{e\} \times K \implies H \cap K = \{e\}$
- $\varphi(k)(h) = khk^{-1}$ under the above identification: $\forall (h,e) \in H \times \{e\}, (e,k) \in \{e\} \times K$
  $(e,k)(h,e)(e,k)^{-1} = (\varphi(k)(h), k)(e, k^{-1}) = (\varphi(k)(h), e)$
- $H \lhd (H \rtimes K)$: $\forall (h,k) \in (H \rtimes K), (h', e) \in H$
  $(h,k)(h',e)(h,k)^{-1} = (h\varphi(k)(h'), k)(\varphi(k^{-1})(h^{-1}), k^{-1}) = (h\varphi(k)(h')h^{-1}, e) \in H$

Example 1.11.1. Classify groups of order 30

Claim: If $|G| = 30$, then both $P \in \mathrm{Syl}_3(G), Q \in \mathrm{Syl}_5(G)$ are normal.

pf. By Sylow theorem, $n_3 = 1$ or 6, $n_5 = 1$ or 6. If $n_3 = 10$ and $n_5 = 6$, then $|G|$ has at least $n_3(3-1) + n_5(5-1) = 44 > 30$ distinct elements ($\to\leftarrow$).

Hence, one of P, Q normal in $G \implies PQ \leq G$. Since $(G : PQ) = 2 \rightsquigarrow PQ \lhd G$ and $PQ \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

Now, $\forall x \in G,\ xPx^{-1} \leq xPQx^{-1} = PQ \implies xPx^{-1} \in \mathrm{Syl}_3(PQ) = \{P\}$. Hence, $P \lhd G$. Similarly, $Q \lhd G$. □

Let $H = PQ, K \in \mathrm{Syl}_2(G)$. Then $H \cap K = \{e\}$ and $G = HK$
$\rightsquigarrow G = H \rtimes_\varphi K$ for some $\varphi : K \to \mathrm{Aut}(H) \simeq \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z})$
Write $H = \langle a \rangle \times \langle b \rangle$ and $K = \langle c \rangle$. If $\varphi : c \to \rho \rightsquigarrow o(\rho) | 2$
Then there is only those possible ρ:

$$\rho_1 : \begin{cases} a \mapsto a \\ b \mapsto b \end{cases} \qquad \rho_2 : \begin{cases} a \mapsto a^{-1} \\ b \mapsto b \end{cases} \qquad \rho_3 : \begin{cases} a \mapsto a \\ b \mapsto b^{-1} \end{cases} \qquad \rho_4 : \begin{cases} a \mapsto a^{-1} \\ b \mapsto b^{-1} \end{cases}$$

- $\varphi(c) = \rho_1$: $G \simeq H \times K \simeq \mathbb{Z}/15\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}/30\mathbb{Z}$
- $\varphi(c) = \rho_2$: $\begin{cases} \varphi_2(c)(a) = a^{-1} \implies cac^{-1} = a^{-1} \\ \varphi_2(c)(b) = b \implies cbc^{-1} = b \end{cases}$

$$\implies G \simeq \langle a, b, c | a^3 = b^5 = c^2, ab = ba, cac^{-1} = a^{-1}, cbc^{-1} = b \rangle = \mathbb{Z}/5\mathbb{Z} \times D_6$$

- $\varphi(c) = \rho_3$: Similar to ρ_2, $G \simeq \mathbb{Z}/3\mathbb{Z} \times D_{10}$
- $\varphi(c) = \rho_4$: $\begin{cases} \varphi_4(c)(a) = a^{-1} \implies cac^{-1} = a^{-1} \\ \varphi_4(c)(b) = b^{-1} \implies cbc^{-1} = b^{-1} \end{cases}$

$$\implies G \simeq \langle a, b, c | a^3 = b^5 = c^2, ab = ba, cac^{-1} = a^{-1}, cbc^{-1} = b^{-1} \rangle = D_{30}$$

Property 1.11.1. Classify groups of order p^3 with p being an odd prime

- G is abelian: $G \simeq \mathbb{Z}/p^3\mathbb{Z}, \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}, (\mathbb{Z}/p\mathbb{Z})^3$
- G is non-abelian: If $|Z_G| = p^2$, then G/Z_G is cyclic $\rightsquigarrow G$ is abelian.

  $\implies |Z_G| = p$ and $|G/Z_G| = p^2$, then G/Z_G is abelian $\implies e \neq [G : G] \leq Z_G \rightsquigarrow [G : G] = Z_G$ and $G/Z_G \simeq (\mathbb{Z}/p\mathbb{Z})^2 \rightsquigarrow \forall x \in G, x^p \in Z_G$ $((xZ_G)^p = Z_G)$

  $\forall x, y \in G$ define $[y, x] = y^{-1}x^{-1}yx$

  Claim: $f : \begin{array}{ccc} G & \to & G \\ x & \mapsto & x^p \end{array}$ is a group homo. (i.e. $x^p y^p = (xy)^p$)

  pf. Note that $[y, x] \in Z_G,\ [y, x]^p = e\ \forall x \in G$ and $xy[y, x] = yx$

  which means we can change xy to yx by multiple $[yx]$. In fact, we can exchange $\frac{p(p-1)}{2}$ times let $x^p y^p$ to $(xy)^p$, thus

$$(xy)^p = x^p y^p [y, x]^{\frac{p(p-1)}{2}} = x^p y^p$$

□

- G contains an element of order p^2, say $o(a) = p^2$, let $H = \langle a \rangle$
  Since $(G : H) = p$ is the smallest prime dividing $|G|$, $H \lhd G$
  Also $e \neq a^p \in Z_G$, $\begin{cases} \ker f \neq G \\ \operatorname{Im} f = Z_G \end{cases} \implies |G/\ker f| = |Z_G| = p \implies \begin{cases} |\ker f| = p^2 \\ \forall x \in \ker f, o(x) = p \end{cases}$
  $\implies E := \ker f \simeq (\mathbb{Z}/p\mathbb{Z})^2$. It is clear that $H \cap E = \langle a^p \rangle$. Pick $b \in E \setminus H$ and $K := \langle b \rangle \rightsquigarrow o(b) = p, K \cap H = \{e\}$.
  So $G \simeq H \rtimes_\varphi K$ for some $\varphi : K \to \operatorname{Aut}(H) \simeq \operatorname{Aut}(\mathbb{Z}/p^2\mathbb{Z}) \simeq (\mathbb{Z}/p^2\mathbb{Z})^\times$
  Claim: $(\mathbb{Z}/p^2\mathbb{Z})^\times$ is cyclic.
  pf. $|(\mathbb{Z}/p^2\mathbb{Z})^\times| = p(p-1)$. We know $(1+p)^p \equiv 1 \pmod{p^2}, (1+p) \not\equiv 1 \pmod{p^2}$
  $\rightsquigarrow \langle \overline{1+p} \rangle$ is a cyclic p-Sylow subgroup of $(\mathbb{Z}/p^2\mathbb{Z})^\times$ (and is unique).
  Consider $g : \underset{\overline{k}}{(\mathbb{Z}/p^2\mathbb{Z})^\times} \underset{\mapsto}{\to} \underset{\overline{k}}{(\mathbb{Z}/p\mathbb{Z})^\times}$

  $$\rightsquigarrow |\ker g| = p \rightsquigarrow \ker g = \langle \overline{1+p} \rangle \rightsquigarrow \left(\mathbb{Z}/p^2\mathbb{Z}\right)^\times / \langle 1+p \rangle \simeq (\mathbb{Z}/p\mathbb{Z})^\times \simeq C_{p-1}$$

  Since $(\mathbb{Z}/p^2\mathbb{Z})^\times$ is abelian, we have $(\mathbb{Z}/p^2\mathbb{Z})^\times = C_{p-1} \times C_p \simeq C_{p(p-1)}$ is cyclic. □
  Since $\operatorname{Aut}(H) \simeq \mathbb{Z}/p(p-1)\mathbb{Z}$, $\langle 1+p \rangle$ is unique subgroup of $\mathbb{Z}/p(p-1)\mathbb{Z}$ in order p.
  $\rightsquigarrow \varphi(b) = \langle \overline{1+p} \rangle$ i.e. $\varphi(b)(a) = a^{1+p} \rightsquigarrow bab^{-1} = a^{1+p}$

  $$\implies G \simeq \langle a, b | a^{p^2} = b^p = e, bab^{-1} = a^{1+p} \rangle$$

- $\forall x \in G,\ o(x) = p$
  Since G is a p-group, $\exists H \leq G$ s.t. $|H| = p^2$ $\begin{cases} H \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} =: \langle a \rangle \times \langle b \rangle \\ H \lhd G \end{cases}$
  and we can regard $\langle a \rangle \times \langle b \rangle$ as a vector space over $\mathbb{Z}/p\mathbb{Z}$. Let $c \in G \setminus H$ and $K := \langle c \rangle \rightsquigarrow K \cap H = \{e\}$.
  So $G \simeq H \rtimes_\varphi K$ for some $\varphi : K \to \operatorname{Aut}(H) \simeq \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ and $|\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})| = (p^2-1)(p^2-p)$
  Since $o\left(\begin{pmatrix} \overline{1} & \overline{0} \\ \overline{1} & \overline{1} \end{pmatrix}\right) = p$, we define $\rho = \begin{cases} a \mapsto ab \\ b \mapsto b \end{cases}$
  $\varphi(c) = \rho \rightsquigarrow \varphi(c)(a) = ab, \varphi(c)(b) = b$

  $$\implies G \simeq \langle a, b, c | a^p = b^p = c^p = e, ab = ba, cac^{-1} = ab, cbc^{-1} = b \rangle$$

1.12 Fundamental theorem of finite abelian group

Definition 1.12.1. If $P \big| |G|$ for a prime p, then

$$G(p) := \{x \in G | o(x) = p^\ell \text{ for some } \ell \geq 0\}$$

Note: In general, $G(p) \not\leq G$. (e.g. $|S_5(3)| = 1 + 20 = 21 \not| 120$)

Property 1.12.1. If G is abelian, then $G(p) \leq G$

Proof: For $x, y \in G(p)$, say $o(x) = p^\alpha, o(y) = p^\beta$, then
$(x^{-1}y)^{p^{\alpha+\beta}} = (x^\alpha)^{-p^\beta}\left(y^\beta\right)^{p^\alpha} = e \implies o(x^{-1}y)\big|p^{\alpha+\beta} \implies x^{-1}y \in G(p)$ □

Theorem 1.12.1. Let G be abelian with $|G| = p_1^{n_1}p_2^{n_2}\cdots p_k^{n_k}$ for $p_1 < p_2 < \cdots < p_k$ are primes. Then

- for $\ell < k$ $(G(p_1)G(p_2)\cdots G(p_\ell)) \cap G_{\ell+1} = \{e\}$
- $G = G(p_1)G(p_2)\cdots G(p_k)$

Proof:

- $|G(p_i)| = p_i^{m_i}$ with $m_i \leq n_i$: If $\exists p_j \neq p_i$ s.t. $p_j\big||G(p_i)|$
  By Cauchy theorem, $\exists a \in G(p_i)$ s.t. $o(a) = q$ $(\rightarrow\leftarrow)$
- for $\ell < k$, $|G(p_1)G(p_2)\cdots G(p_\ell)| = p_1^{m_1}p_2^{m_2}\cdots p_\ell^{m_\ell}$: By induction on ℓ,
  $\ell = 2$: $G(p_1) \cap G(p_2) = \{e\}$, then
  $$|G(p_1)G(p_2)| = \frac{|G(p_1)||G(p_2)|}{|G(p_1) \cap G(p_2)|} = p_1^{m_1}p_2^{m_2}$$
  For $\ell > 2$. Since $\gcd\left(|G(p_1)\cdots G(p_{ell-1})|, |G(p_\ell)|\right) = 1$
  $\implies |G(p_1)\cdots G(p_\ell)| = p_1^{m_1}\cdots p_k^{n_k}$
- for $\ell < k$, $G(p_1)G(p_2)\cdots G(p_\ell) \cap G(p_{\ell+1}) = \{e\}$: By gcd = 1
- $G = G(p_1)G(p_2)\cdots G(p_k)$: $(\supseteq)$: OK
  $(\subseteq)$: $\forall x \in G$, $o(x) = p_1^{b_1}\cdots p_k^{b_k}$ with $b_i \leq n_i$ $\forall i$. Let $a_i = \frac{o(x)}{p_i^{b_i}} \rightsquigarrow \gcd(a_1, ..., a_k) = 1$.
  By Bézout's lemma, $\exists r_i \in \mathbb{Z}$ s.t. $r_1a_1 + \cdots + r_ka_k = 1$
  Write $x = x^1 = x^{r_1a_1}x^{r_2a_2}\cdots x^{r_ka_k}$ and $(x^{r_ia_i})^{p_i^{b_i}} = \left(x^{o(x)}\right)^{r_i} = e \rightsquigarrow x^{r_ia_i} \in G(p_i)$

□

Lemma 1.12.1. If $G = N_1N_2\cdots N_k$ for $N_i \lhd G$ and $(N_1N_2\cdots N_{j-1}) \cap N_j = \{e\}$ with $j \geq 2$, then $G \simeq N_1 \times N_2 \times \cdots \times N_k$

Proof: For $i < j$, $N_i \cap N_j \leq (N_1N_2\cdots N_{j-1}) \cap N_j = \{e\} \implies N_i \cap N_j = \{e\}$
Recall $\begin{cases} N_i, N_j \lhd G \\ N_i \cap N_j = \{e\} \end{cases} \rightsquigarrow \forall x \in N_i, y \in N_j\ xy = yx$
We define $f: \begin{array}{ccc} G & \rightarrow & N_1 \times N_2 \times \cdots \times N_k \\ h_1h_2\cdots h_k = x & \mapsto & (h_1, h_2, ..., h_k) \end{array}$ is isomorphism. □

Corollary 1.12.1. If G is abelian with $|G| = p_1^{n_1}p_2^{n_2}\cdots p_k^{n_k}$ for $p_1 > p_2 > \cdots$ are primes, then
$$G \simeq G(p_1) \times G(p_2) \times \cdots \times G(p_k)$$

Theorem 1.12.2. If G is abelian with $|G| = p^n$, then

$$G \simeq \mathbb{Z}/p^{\alpha_1} \times \mathbb{Z}/p^{\alpha_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{\alpha_t}\mathbb{Z} \text{ with } \alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_t$$

Proof: Since $|G| < \infty$, we can choose $x_1 \in G$ of max order $p_1^{\alpha_1} \leq p_1^n$ in G
Then $H_1 := \langle x_1 \rangle \lhd G$ and $|G/H_1| = p^{n-\alpha_1}$
If $n = \alpha_1$, then $G \simeq H = \langle x_1 \rangle \simeq \mathbb{Z}/p^n\mathbb{Z}$
Otherwise, for some $y \in H$, $o(yH_1)$ is max in G/H_1
$\because (H_1y)^{o(y)} = H_1 \therefore p^{\alpha_2} | o(y) \leq p^{\alpha_2} \implies p^{\alpha_2} \leq p^{\alpha_1}$
If $o(y) = p^{\alpha_2}$, let $H_2 = \langle y \rangle$. If $y^\ell \in H_1 \cap H_2 \rightsquigarrow (H_1y)^\ell = H_1 \rightsquigarrow p^{\alpha_2} | \ell \rightsquigarrow y^\ell = e$
$\implies H_1 \cap H_2 = \{e\} \implies H_1H_2 = H_1 \oplus H_2$
By def, $y^{p^{\alpha_2}} \in H_1 = \langle x_1 \rangle$, say $y^{p^{\alpha_2}} = x_1^k$. Write $k = qp^{\alpha_2} + r$ with $0 \leq r < p^{\alpha_2}$
If $r > 0$, then $x_2 := x_1^{-q}y$.
$\because o(x_2) = p^s \leq p^{\alpha_1} \therefore e = x_2^{p^{\alpha_1}} = \left(x_1^{-qp^{\alpha_2}} y^{p^{\alpha_2}}\right)^{p^{\alpha_1-\alpha_2}} = x_1^{rp^{\alpha_1-\alpha_2}} \rightsquigarrow p^{\alpha_1} | rp^{\alpha_1-\alpha_2}$
$\rightsquigarrow p^{\alpha_2} | r \rightsquigarrow r = 0$
Now, $\begin{cases} x_2^{p^{\alpha_2}} = x_1^{-qp^{\alpha_2}} y^{p^{\alpha_2}} = x_1^r = e \rightsquigarrow o(x_2) | p^{\alpha_2} \\ H_1x_2 = H_1y, o(H_1y) = p^{\alpha_2} \rightsquigarrow p^{\alpha_2} | o(x_2) \end{cases} \implies o(x_2) = p^{\alpha_2}.$
Let $H_2 = \langle x_2 \rangle \rightsquigarrow H_1H_2 \simeq H_1 \oplus H_2 \simeq \mathbb{Z}/p^{\alpha_1}\mathbb{Z} \oplus \mathbb{Z}/p^{\alpha_2}\mathbb{Z}$
If $G = H_1H_2$, then done!
Otherwise, $H_2' = H_1H_2$ and $z \in G$ s.t. $o(H_2'z) = p^{\alpha_3}$ is max in G/H_2'
$(H_2'z)^{o(H_1z)} = H_2(H_1z)^{o(H_1z)} = H_2H_1 = H_2' \rightsquigarrow p^{\alpha_3} | o(H_1z) \leq p^{\alpha_2} \rightsquigarrow p^{\alpha_3} \leq p^{\alpha_2}$
By def, $z^{p^{\alpha_3}} = x_1^{k_1}x_2^{k_2}$

- $k_1 = 0, k_2 = 0$:
  $\begin{cases} z^{p^{\alpha_2}} = e \rightsquigarrow o(z) | p^{\alpha_3} \\ o(H_2'z) = p^{\alpha_3} \rightsquigarrow p^{\alpha_3} | o(z) \end{cases} \implies o(z) = p^{\alpha_3}$. Let $H_3 = \langle z \rangle$
  If $z^\ell \in H_2' \cap H_3 \rightsquigarrow (H_2'z)^\ell = H_2' \rightsquigarrow p^{\alpha_3} | \ell \rightsquigarrow z^\ell = e \implies H_2' \cap H_3 = \{e\}$
  So $H_2'H_3 \simeq H_2 \oplus H_3 \simeq H_1 \oplus H_2 \oplus H_3$
- $k_1 > 0, k_2 = 0$:
  Write $k_1 = q'p^{\alpha_3} + r'$ with $0 \leq r' < p^{\alpha_3}$. Set $x_3 = x_1^{-q'}z$ $(H_2'x_3 = H_2'z)$
  $\rightsquigarrow e = x_3^{p^{\alpha_1}} = \left(x_1^{-q'p^{\alpha_3}} z^{p^{\alpha_3}}\right)^{p^{\alpha_1-\alpha_3}} = x_1^{r'p^{\alpha_1-\alpha_3}} \rightsquigarrow p^{\alpha_1} | r'p^{\alpha_1-\alpha_3} \rightsquigarrow r' = 0$
  $\begin{cases} x_3^{p^{\alpha_3}} = x_1^{-k_1} z^{p^{\alpha_3}} = e \rightsquigarrow o(x_3) | p^{\alpha_3} \\ (H_2'z)^{o(z)} = H_2', o(H_2'z) = p^{\alpha_3} \rightsquigarrow p^{\alpha_3} | o(z) \end{cases} \implies o(z) = p^{\alpha_3}.$
  Let $H_3 = \langle x_3 \rangle$, then $H_1H_2H_3 \simeq H_1 \oplus H_2 \oplus H_3$
- $k_2 > 0$:
  Write $k_2 = q''p^{\alpha_3} + r''$ with $0 \leq r'' < p^{\alpha_3}$. Set $x_3' = x_2^{-q''}z$ $H_2'x_3' = H_2'z$
  $H_1 = (H_1x_3')^{p^{\alpha_2}} = \left(H_1(x_2^{-q''p^{\alpha_3}} z^{p^{\alpha_3}})\right)^{p^{\alpha_2-\alpha_3}} = \left(H_1(x_1^k x_2^{k_2-q''p^{\alpha_3}})\right)^{p^{\alpha_2-\alpha_3}} = (H_1x_2)^{r''p^{\alpha_1-\alpha_3}}$
  $\rightsquigarrow p^{\alpha_2} | r''p^{\alpha_2-\alpha_3} \rightsquigarrow r'' = 0 \rightsquigarrow (x_3')^{p^{\alpha_3}} = x_2^{-q''p^{\alpha_3}} z^{p^{\alpha_3}} = x_1^k$

By case2, $\exists x_3 \in G$ s.t. $\begin{cases} o(x_3) = p^{\alpha_3} \\ H_2' x_3 = H_2' x_3' \end{cases}$ $\rightsquigarrow$done!

Since $|G| < \infty$, after a finite numbers of steps, we can get that

$$G \simeq H_1 H_2 \cdots H_t \simeq \mathbb{Z}/p^{\alpha_1}\mathbb{Z} \oplus \mathbb{Z}/p^{\alpha_2}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{\alpha_t}\mathbb{Z}$$

□

Theorem 1.12.3. Let G be abelian with $|G| = p^n$. If

$$\begin{aligned} G &\simeq \mathbb{Z}/p^{\alpha_1}\mathbb{Z} \oplus \mathbb{Z}/p^{\alpha_2}\mathbb{Z} \cdots \mathbb{Z}/p^{\alpha_t}\mathbb{Z} := A \\ &\simeq \mathbb{Z}/p^{\beta_1}\mathbb{Z} \oplus \mathbb{Z}/p^{\beta_2}\mathbb{Z} \cdots \mathbb{Z}/p^{\beta_s} := B \end{aligned}$$

Then, $t = s$ and $\alpha_i = \beta_i$

Proof: By induction on n, $n = 1$ $G \simeq \mathbb{Z}/p\mathbb{Z}$ Ok.
For $n > 1$, let $G_p = \{x \in G | o(x) = p\} \leq G$ (since G is abelian)
If $G_p = G$, then $A_p = A, B_p = B \rightsquigarrow t = s = n$ and $\alpha_i = \beta_i = 1$ $\forall i$
Otherwise, $G_p \lneq G \rightsquigarrow A_p \lneq A, B_p \lneq B$
Say $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_a > \alpha_{a+1} = \alpha_{a+2} = \cdots = \alpha_t = 1$
For each $\mathbb{Z}/p^{\alpha_i}\mathbb{Z}$, $\exists! \langle \overline{x_i} \rangle \leq \mathbb{Z}^{\alpha_i}\mathbb{Z}$ with $|\langle \overline{x_i} \rangle| = p$
This say that $G_p \simeq A_p \simeq \langle \overline{x_1} \rangle \oplus \cdots \oplus \langle \overline{x_t} \rangle \rightsquigarrow G/G_p \simeq A/A_p \simeq \bigoplus_{i=1}^{t} \mathbb{Z}/p^{\alpha_i - 1}\mathbb{Z}$
Similarly, $G/G_p \simeq \bigoplus_{i=1}^{s} \mathbb{Z}/p^{\beta_i - 1}\mathbb{Z}$. Since $|G/G_p| < |G|$, by induction hypothesis, $a = b$ and $\alpha_i - 1 = \beta_i - 1$ $\forall i \leq a = b$
Also, $G_p \simeq A_p \simeq B_p \rightsquigarrow s = t \implies \alpha_i = \beta_i = 1$ $\forall a < i \leq s$ □

Chapter 2

Ring theory

2.1 Basis properties

Definition 2.1.1 (Ring)**.** A **ring** is a triple $(R, +, \cdot)$ for R is a nonempty set with two functions $+, \cdot : R \times R \to R$ and $0, 1 \in R$ s.t.

(1) $(R, +, 0)$ is a abelian group (We call $+$ as addition)

(2) $(R, \cdot, 1)$ is a monoid (We call $\cdot$ as multiplication)

(3) **Distributive law**: $\begin{cases} x \cdot (y+z) = x \cdot y + x \cdot z \\ (y+z) \cdot x = y \cdot x + z \cdot x \end{cases} \quad \forall x, y, z \in R$

Fact:

- $0 \cdot x = x \cdot 0 = 0$:

  $0 \cdot x = (0+0) \cdot x = 0 \cdot x + 0 \cdot x \implies 0 \cdot x = 0$

  $x \cdot x = x \cdot (0+0) = x \cdot 0 + x \cdot 0 \implies x \cdot 0 = 0$

- $x(-y) = (-x)y = -(xy) : x(-y) + xy = x((-y) + y) = x \cdot 0 = 0$

- $(-x)(-y) = xy : (-x)(-y) = -x(-y) = -(-xy) = xy$

- If all axiom for a ring except commutativity of addition are assumed, then comm. follow:

  $-(x+y) = -y - x = (-1)y + (-1)(x) = (-1)(y+x) = -(y+x) \rightsquigarrow x + y = y + x$

Definition 2.1.2. Let R be a ring

- $u \in R$ is called a **unit** if $\exists u^{-1}$ s.t. $u \cdot u^{-1} = u^{-1} \cdot u = 1$

- $R^\times := \{\text{all units in} R\} \implies (R^\times, \cdot, 1)$ forms a group

- R is called a **division ring** if $0 \neq 1$ and $\forall 0 \neq x \in R$, x is a unit

- R is called a **commutative ring** if $\forall x, y \in R,\ xy = yx$

- R is called a **field** if R is a commutative divsion ring

Example 2.1.1.

- $\overline{2}$ is not a unit in $\mathbb{Z}/6\mathbb{Z}$ but is a unit in $\mathbb{Z}/9\mathbb{Z}$
- $\mathbb{Z}\left[\sqrt{2}\right] = \left\{a_0 + a_1\left(\sqrt{2}\right) + \cdots + a_n\left(\sqrt{2}\right)^n | a_i \in \mathbb{Z}\right\} = \{a + b\sqrt{2} | a, b \in \mathbb{Z}\}$ is a ring and $(2 + \sqrt{2})$ is not a unit but $(1 + \sqrt{2})$ is.

Definition 2.1.3. Let R be a ring

- For $x \in \mathbb{R}$, if $\exists y \neq 0$ s.t. $xy = 0$, then x is called a **left zero divisor**
- For $x \in \mathbb{R}$, x is called a **zero divisor** if it is a left zero divisor or right zero divisor
- R is called a **domain** if R has no non-zero divisor
- R is **integral domain** (**entire ring**) if R is domain + commutative

  Fact:
- R : domain $\implies$ if $x \neq 0$ $\begin{cases} xy = xz \rightsquigarrow x(y - z) = 0 \rightsquigarrow y = z \\ yx = zx \rightsquigarrow y = z \end{cases}$
- division $\implies$ domain : If $x \neq 0$, $xy = 0 \rightsquigarrow 0 = x^{-1}xy = y$
- finite domain $\implies$ division : Let $R = \{0, x_1, ..., x_n\}$. For $0 \neq x \in \mathbb{R}$, $|\{0, xx_1, ..., xx_n\}| = n + 1 \implies \{0, xx_1, ..., xx_n\} = R \rightsquigarrow \exists i$ s.t. $xx_i = 1$
- $\mathbb{Z}/n\mathbb{Z}$ is an integral domain $\iff$ $\mathbb{Z}/n\mathbb{Z}$ is a field $\iff$ n is a prime number

Definition 2.1.4 (**characteristic**). Let R be a ring. If $n = 1+1+\cdots 1(n \text{ times}) \neq 0$, then $R = 0$.

Otherwise, $R := \min\{n \in \mathbb{N} | n \cdot 1 = 0\}$

Property 2.1.1. Let R be a domain

- $R = 0$ or p is a prime : Assume $R = k\ell$ with $k, \ell > 1$
  $\rightsquigarrow 0 = (1 \cdot k)(1 \cdot \ell) \rightsquigarrow$ one of $1 \cdot k, 1 \cdot \ell$ is zero $(\rightarrow\leftarrow)$
- Let R be an integral domain with $R = p$, then

$$x^p + y^p = (x + y)^p \quad \forall\ x, y \in R$$

Observation of quotient: Let R be a ring and I be an additive subgroup of R.

By def, $I \lhd R$ and $(R/I, \cdot, 0 + I)$ forms a group.

But we want $(R/I, \cdot, 0 + I)$ is a ring, which means

$$(x_1 + I)(x_2 + I) = x_1x_2 + x_1I + Ix_2 + I^2 \ \forall\ x_1, x_2 \in R$$

So we request $x_1I, Ix_2 \subseteq I$.

Now, we can define ideal (like normal subgroup correspond to quotient) in ring.

Definition 2.1.5 (ideal)**.** Let I be an additive subgroup of R

- If $xa \in I \ \forall x \in R, a \in I$, then we call I is a **left ideal** of R. Similarly, we can define **right ideal**. If I is left ideal and right ideal, then we call I is an **ideal**.
- $\{0\}$ is called the **trivial ideal** of R
- Let $a_1, a_2, ..., a_n \in R$

$$I = \langle a_1, a_2, ..., a_n \rangle := \{x_1a_1 + x_2a_2 + \cdots + x_na_n | x_i \in R\}$$

  is called the left ideal generated by $a_1, a_2, ..., a_n$.

- If $I = \langle a \rangle$, then I is called a principal ideal.

Fact:

- If I is an ideal, then $(R/I, +, \cdot)$ is a ring
- If I is an ideal and a unit $u \in I$, then $I = R : \forall\ x \in R,\ x = (xu^{-1})u \in R$
- Let R be a commutative ring. Then

$$R \text{ is a field } \iff \text{ the only ideal of } R \text{ are } \{0\} \text{ and } R$$

pf. ($\Rightarrow$) If $\{0\} \neq I \subseteq I \rightsquigarrow \exists 0 \neq x \in I$ and thus a unit $x \in I \rightsquigarrow I = R$
($\Leftarrow$) $\forall 0 \neq x \in I \rightsquigarrow \langle x \rangle \neq \{0\}$ is an ideal. Then $\langle x \rangle = R \rightsquigarrow \exists y \in R$ s.t. $yx = 1 \rightsquigarrow y = x^{-1}$

Definition 2.1.6. Let R be a commutative ring and I be a proper ideal of R

1. I is said to be **maximal ideal** if $\forall J$ is an ideal of R, "$I \subsetneq J \implies J = R$"
2. I is called a prime ideal if $xy \in I$ ($xy \equiv 0 \pmod{I}$) $\implies x \in I$ or $y \in I$
3. R is **local ring** if $\exists!$ maximal ideal

Fact:

1. I is maximal $\iff$ R/I is a field
   pf. ($\Rightarrow$) $\forall\ \overline{0} \neq \overline{x} \in R/I$, $\langle x \rangle + I \supsetneq I \rightsquigarrow \langle x \rangle + I = R \ni 1$.
   Say $1 = xy + a \in I \rightsquigarrow \overline{x}^{-1} = \overline{y}$
   ($\Leftarrow$) For $J \supsetneq I$, let $x \in J \setminus I$ i.e. $\overline{x} \neq \overline{0}$ in $R/I \rightsquigarrow \exists \overline{y} \in R/I$ s.t. $\overline{yx} = \overline{1}$
   $\rightsquigarrow yx - 1 \in I \subsetneq J$. Since $yx \in J \implies 1 \in J \implies J = R$
2. I is prime $\iff$ R/I is an integral domain
   pf. ($\Rightarrow$) If $\overline{x} \neq \overline{0}$ and $\overline{xy} = \overline{0} \rightsquigarrow xy \in I \rightsquigarrow y \in I \rightsquigarrow \overline{y} = \overline{0}$
   ($\Leftarrow$) If $xy \in I$ and $x \notin I \rightsquigarrow \overline{xy} = \overline{0} \rightsquigarrow \overline{y} = \overline{0} \rightsquigarrow y \in I$

Corollary 2.1.1. R is maximal $\implies$ R is prime

Definition 2.1.7 (sum and product of ideals)**.** If I_1, I_2 are ideal in R, then define

$$I_1 + I_2 := \{a + b | a \in I_1, b \in I_2\}$$
$$I_1 I_2 := \{a_1 b_1 + a_2 b_2 + \cdots + a_n b_n | a_i \in I_1, b_i \in I_2\}$$

Theorem 2.1.1. (ring isomorphism theorem)

- (1st) $f : R \to R'$ is ring homomorphism, then $\operatorname{Im} f \simeq R/\ker f$
- (2nd) S is a subring of R and I is an ideal in R, then $(S + I)/I \simeq S/(S \cap I)$
- (3rd) I, J are ideal in R with $J \subseteq I$, then $R/I \simeq (R/J)/(I/J)$

  We will prove it in Homework 12, it just similar to the proof of group iso.thm.

Theorem 2.1.2. (Chinese Remainder theorem) Let R be a commutative ring and $I_1, I_2, ..., I_n$ be an ideals od R. Then

$$\begin{array}{rccc} f: & R & \mapsto & R/I_1 \times R/I_2 \times \cdots \times R/I_n \\ & x & \mapsto & (\overline{x}, \overline{x}, ..., \overline{x}) \end{array}$$

is a ring homo. And

(1) if I_i, I_j are **coprime** (i.e. $I_i + I_j = R$) $\forall\ i \neq j$, then $I_1 I_2 \cdots I_n = I_1 \cap I_2 \cap \cdots \cap I_n$

(2) f is surjective $\iff$ I_i, I_j are coprime $\forall\ i \neq j$

(3) I_i, I_j coprime $\forall\ i \neq j$ $\implies$ $R/(I_1 \cap I_2 \cap \cdots \cap I_n) \simeq R/I_1 \times R/I_2 \times \cdots \times R/I_n$

Proof: It is clear that f is ring homomorphism.

(1) By induction on n. $n = 2$:

$I_1 I_2 \subseteq I_1 R = I_1, I_1 I_2 \subseteq R I_2 = I_2 \implies I_1 I_2 \subseteq I_1 \cap I_2$

$I_1 \cap I_2 = R(I_1 \cap I_2) = (I_1 + I_2)(I_1 \cap I_2) \subseteq I_1 I_2 + I_2 I_1 = I_1 I_2 \rightsquigarrow I_1 \cap I_2 = I_1 I_2$

For $n > 2 : \forall i \neq n,\ I_i + I_n = R \rightsquigarrow \exists x_i \in I_i, y_i \in I_n$ s.t. $x_i + y_i = 1$, then

$I_1 I_2 \cdots I_{n-1} \ni x_1 x_2 \cdots x_{n-1} = (1 - y_1)(1 - y_2) \cdots (1 - y_{n-1}) = 1 + y \in I_n$

$\rightsquigarrow I_1 I_2 \cdots I_{n-1} + I_n = R$. Hence,

$$(I_1 I_2 \cdots I_{n-1}) I_n = (I_1 I_2 \cdots I_{n-1}) \cap I_n = I_1 \cap I_2 \cap \cdots \cap I_n$$

(2) For convenience, we only write the case of I_1, I_2

$(\Rightarrow)$ $\exists a \in R$ s.t. $f(a) = (\overline{1}, \overline{0}, \overline{0}, ..., \overline{0}) \rightsquigarrow a - 1 \in I_1, a \in I_2$

$\implies 1 = (1 - a) + a \in I_1 + I_2 \rightsquigarrow I_1 + I_2 = R$

$(\Leftarrow)$ If we can choose $a_i \in R$ s.t. $f(a_i) = (\overline{0}, ..., \overline{0}, \overline{1} \in R/I_i, \overline{0}, ..., \overline{0})$, then f is surjective. $\because R_1 + I_i = R \therefore \exists x_i \in R_1, y_i \in I_i$ s.t. $x_i + y_i = 1$.

Take $a = y_2 \cdots y_n \in I_i\ \forall i \neq 1$. In the other hands, $a = (1 - x_2) \cdots (1 - x_n) = 1 + x \rightsquigarrow a - 1 \in R_1 \rightsquigarrow f(a) = (\overline{1}, \overline{0}, ..., \overline{0})$

(3) By 1st ring isomorphism theorem.

□

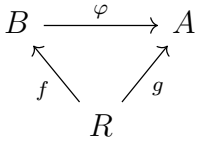
2.2 Universal property and localization

Give me some time to know how to write it down
Goal: Let R be a commutative ring and S be a multiplicatively closed set with $0, 1 \in S$. To construct R_S s.t. the elements of S are invertible in R_S

Definition 2.2.1. Suppose that there is a ring B and a ring homo. $f : R \to B$ s.t.

(1) $f(x)$ is a unit of B $\forall x \in S$

(2) if $g : R \to A$ is another ring homo. s.t. $g(x)$ is a unit in A $\forall x \in S$, then $\exists!$ ring homo. $\varphi : B \to A$ s.t diagram commute.



Give me some time to know it more

2.3 ED,PID and UFD

In this section, R be an integral domain

Definition 2.3.1 (divide)**.**
- Let $a, b \in R$ with $b \neq 0$. We say $b|a$ if $\exists x \in R$ s.t. $a = bx$
- We say a, b are **associates** (write $a \sim b$) if $a|b$ and $b|a$ i.e. $a = bu$ with u is unit
- $d = \gcd(a, b)$ if $d|a, d|b$ and "$c|a, c|b \implies d|c$"
  (Note: gcd is unique up to associates)

Definition 2.3.2 (GCD domain)**.** If R is a ring such that every two elements in R have greatest common divisor (gcd), then R is called a **GCD domain**

Definition 2.3.3 (norm,ED)**.**
- Any function $N : R \to \mathbb{N}$ with $N(0) = 0$ is called a **norm** on R
- N is called positive if $N(a) > 0$ $\forall a \neq 0$
- R is called a **Euclidean domain** if $\exists$ a norm N on R s.t.
  $\forall a, b \in R, \exists\ q, r \in R$ s.t. $a = qb + r$ with $r = 0$ or $N(r) > N(b)$

Example 2.3.1. $\mathbb{Z}, F[x], F$ are ED

Property 2.3.1. (Euclidean Algorithm) Let R be a ED. For $0 \neq a, b \in R$
$a = q_1 b + r_1, b = q_2 r_1 + r_2, r_1 = q_3 r_2 + r_3, ..., r_{k-1} = q_{k+1} r_k + r_{k+1}$ with $r_{k+1} = 0$
Then $\gcd(a, b) = r_k$

Proof: Let $A(x) = \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix}$ is invertible and rewrite the equation

$$\begin{pmatrix} a & b \end{pmatrix} = \begin{pmatrix} b & r_1 \end{pmatrix} \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} b & r_1 \end{pmatrix} = \begin{pmatrix} r_1 & r_2 \end{pmatrix} \begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix}, \cdots, \begin{pmatrix} r_{k-1} & r_k \end{pmatrix} = \begin{pmatrix} r_k & 0 \end{pmatrix} \begin{pmatrix} q_{k+1} & 1 \\ 1 & 0 \end{pmatrix}$$

$\begin{pmatrix} a & b \end{pmatrix} = \begin{pmatrix} r_k & 0 \end{pmatrix} A(q_{k+1}) A(q_k) \cdots A(q_1) \rightsquigarrow r_k | a, b$
$\begin{pmatrix} r_k & 0 \end{pmatrix} = \begin{pmatrix} a & b \end{pmatrix} A(q_1)^{-1} A(q_2)^{-1} \cdots A(q_{k+1})^{-1} \rightsquigarrow r_k = ta + sb$
$\rightsquigarrow$ "$c|a, b \implies r_k|a, b$" $\implies r_k = \gcd(a, b)$ □

Definition 2.3.4 (PID)**.** R is called a **principal ideal domain** if for all ideal I in R is principal.

Property 2.3.2. $\langle a, b \rangle = \langle d \rangle \implies d = \gcd(a, b)$

1. $a \in \langle d \rangle \rightsquigarrow d|a, b \in \langle d \rangle \rightsquigarrow d|b$
2. $d \in \langle a, b \rangle \rightsquigarrow d = sa + tb \rightsquigarrow$ "$c|a, b \implies d|c$"

Corollary 2.3.1. ED, PID $\implies$ GCD domian

Theorem 2.3.1. ED $\implies$ PID

Proof: If $I = \langle 0 \rangle$, then done!
Let $I \neq \langle 0 \rangle$ and $n = \min\{N(a) | a \in R\}$ with $N(d) = n$
Claim: $I = \langle d \rangle$
($\supseteq$) OK!
($\supseteq$) $\forall 0 \neq a$, let $a = qd + r$. If $r \neq 0$, then $N(r) < N(d)$ ($\rightarrow\leftarrow$)
Hence, $r = 0$. i.e. $a \in \langle d \rangle$ □

Definition 2.3.5. Let $p \in R$ is non-zer0 and not a unit

- p is called a prime if "$p|ab \implies p|a$ or $p|b$"
- p is said to be irreducible if $p|ab \implies a \in R^\times$ or $b \in R^\times$

Fact: prime $\implies$ irreducible
pf. If $p = ab \rightsquigarrow p|a$ or $p|b$, say $a = pc \implies 1 = cb$ i.e. $b \in R^\times$

Example 2.3.2. irreducible $\not\implies$ prime
$A_{-5} := \{a + b\sqrt{-5} | a, b \in \mathbb{Z}\}$. We find that $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$
Define $N(a + b\sqrt{-5}) = (a + b\sqrt{-5})\overline{(a + b\sqrt{-5})} = a^2 + 5b^2$
$\implies N(\alpha\beta) = N(\alpha)N(\beta)$ and u is unit $\iff N(u) = 1$

- $1+\sqrt{-5}$ is irr. : If $1+\sqrt{-5}=\alpha\beta$
  $\implies 6=N\left(1+\sqrt{-5}\right)=N(\alpha)N(\beta) \implies$ one of $N(\alpha), N(\beta)=1$
- $1+\sqrt{-5} \nmid 2, 3$: Since $6 \nmid 4, 9$

Definition 2.3.6 (UFD)**.** R is called a **unique factorization domain** if

- $\forall a \in R \setminus (\{0\} \cup R^\times), \exists u$ is unit, p_i is irr. s.t. $a = up_1p_2\cdots p_r$
- If $a = up_1p_2\cdots p_r = wq_1q_2\cdots q_s$ with $u, w \in R^\times$ and p_i, q_j are irr, then $r = s$ and $p_i \sim q_i$ $\forall i$

Lemma 2.3.1. Let R be a PID and $p \in R \setminus (\{0\} \cup R^\times)$ TFAE

(1) p is irreducible element

(2) $\langle p\rangle$ is a maximal ideal

(3) $\langle p\rangle$ is a prime ideal

(4) p is prime element

Thus, in PID prime element $\iff$ irreducible element. Moreover, we will prove that in UFD prime element $\iff$ irreducible element in Homework 14.

Proof: We only need proof (1) $\Rightarrow$ (2)

Let $\langle p\rangle \subseteq N \subseteq R$ and $N = \langle b\rangle$, say $p = bc \implies \begin{cases} b \in R^\times \rightsquigarrow N = R \\ c \in R^\times \rightsquigarrow N = \langle b\rangle \end{cases}$ □

Theorem 2.3.2. PID $\implies$ UFD

Proof:

- Existance: Let $a \in R \setminus (\{0\} \cup R^\times)$

  Claim: a has at least one irreducible factor

  pf. If a is irr, then done!

  Otherwise, $a = a_1b_1$ with $a_1, b_1 \in R \setminus (\{0\} \cup R^\times)$. If a_1 is irr, then done!

  Otherwise, $a_1 = a_2b_2$ with $a_2, b_2 \in R \setminus (\{0\} \cup R^\times)$. If a_2 is irr, then done! $\cdots$

  Then $\exists\, a_n$ is irr, otherwise $\langle a_1\rangle \subsetneq \langle a_2\rangle \subsetneq \cdots$ and let $I = \bigcup_{i=1}^{\infty} \langle a_i\rangle$ which is an ideal, say $I = \langle d\rangle \rightsquigarrow d \in \langle a_i\rangle$ for some i

  $\implies I = \langle d\rangle \subseteq \langle a_i\rangle \implies \langle a_i\rangle = \langle a_{i+1}\rangle$ $(\rightarrow\leftarrow)$ □

  Now, if a is irr, then done!

  Otherwise, $a = p_1a_1$ with p_1 is irr. and $a_1 \in R \setminus (\{0\} \cup R^\times)$. If a_1 is irr, then done!

  Otherwise, $a_1 = p_2a_2$ with p_2 is irr. and $a_2 \in R \setminus (\{0\} \cup R^\times) \cdots$

  Then $\exists\, a_n$ is irr. (By same reason in claim)

- Uniqueness: Let $= up_1p_2\cdots p_n = vq_1q_2\cdots q_m$, u, v is unit and p_i, q_j is irr.

  By induction on n, $n = 1 \rightsquigarrow p_1|q_1q_2\cdots q_m \rightsquigarrow p_1|q_i$ for some i, say $p_1|q_1$ and $q_1 = p_1w$, where $w \in R^\times$

  For $n > 1$, by same reason, say $q_1 = p_1w$ and thus $up_2\cdots p_n = vwq_2\cdots q_m$. By induction hypothesis, $n-1 = m-1$ and $p_i \sim q_i$

□

2.4 Irreducibility

In this section, $P \in$ Spec$R$ if P is prime ideal, $P \in$ Max R if P is maximal ideal.

Property 2.4.1. Let P be a prime ideal in R and $f(x)$ be a monic poly. of deg ≥ 0 in $R[x]$. If $f(x)$ is irr. in $R/P[x]$, then $f(x)$ is irr. in $R[x]$.

Proof: If $f(x) = g(x)h(x)$ with $\deg g, \deg h > 0$ in $R[x]$
Consider $\overline{f}(x) = \overline{g}(x)\overline{h}(x)$ in $R/P[x]$
$\because \begin{cases} f \text{ is monic} \\ 1 \notin P \end{cases}$ $\therefore \deg \overline{f} = \deg f = \deg g + \deg h \geq \deg \overline{g} + \deg \overline{h} = \deg \overline{f}$
$\implies \overline{g}(x), \overline{h}(x)$ is not unit in $Z/P[x]$ □

Theorem 2.4.1. (Eisenstein's criterion) Let $P \in$ Spec$R$ and $f(x) = a_nx^n + \cdots + a_1x + a_0$ be primitive in $R[x]$. Assume that $a_n \notin P, a_{n-1}, ..., a_0 \in P$, but $a_0 \notin P^2$. Then $f(x)$ is irr. in $R[x]$.

Proof: If not, say $f(x) = g(x)h(x)$ with $\deg g, \deg h > 0$
Consider $a_nx^n = \overline{f}(x) = \overline{g}(x)\overline{h}(x)$. If $\begin{cases} \overline{g}(x) = \overline{b_r}x^r + \cdots + \overline{b_i}x^i \\ \overline{h}(x) = \overline{c_{n-r}}x^{n-r} + \cdots + \overline{c_j}x^j \end{cases}$
$\implies \overline{b_i}\overline{c_j} = 0 \rightsquigarrow$ one of $\overline{b_i}, \overline{c_j} = \overline{0}$ and thus $\overline{g}(x) = \overline{b_r}x^r, \overline{h}(x) = \overline{c_{n-r}}x^{n-r}$
Write $\begin{cases} g(x) = b_rx^r + \cdots + b_0 \\ h(x) = b_{n-r}x^{n-r} + \cdots + c_0 \end{cases}$ $\rightsquigarrow b_0, c_0 \in P \rightsquigarrow a_0 = b_0c_0 \in P^2$ $(\rightarrow\leftarrow)$ □

2.5 Gauss lemmas and Gauss prime

2.5.1 Gauss lemma

Goal: R : UFD $\implies$ $R[x]$: UFD ($\rightsquigarrow R[x_1, x_2, ..., x_n]$: UFD)

Theorem 2.5.1. UFD $\implies$ GCD domain

Proof: Write $\begin{cases} a = up_1^{\alpha_i}\cdots p_n^{\alpha_n} \\ b = vp_1^{\beta_i}\cdots p_n^{\beta_n} \end{cases} \implies \gcd(a, b) = p_1^{\gamma_i}\cdots p_n^{\gamma_n}$, where $\gamma_i = \min(\alpha_i, \beta_i)$

□

Definition 2.5.1. Let R be a UFD,

- $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ is **primitive** if $\gcd(a_n, a_{n-1}, ..., a_0) = 1$
- the **content** of $f = \mathrm{cont}(f) = \gcd(a_0, a_1, ..., a_n)$ up to association

Theorem 2.5.2. (Gauss lemma 1.) Let R be a UFD and $f(x), g(x) \in R[x]$. Then

$$\mathrm{cont}(fg) = \mathrm{cont}(f)\,\mathrm{cont}(g)$$

Proof:

1. f, g primitive $\implies$ fg primitive:
   If not, suppose $\mathrm{cont}(fg) = c \in R \setminus (\{0\} \cup R^\times)$
   Take a prime factor $p|c$. Let $f(x) = \sum_{i=0}^{n} a_i x^i$ and $a_{-1} = 0, a_i = 0\ \forall i > n$
   We let r be the smallest non-negative integer such that $p \nmid a_r$
   Similarly, we define $g(x) = \sum_{i=0}^{m} b_i x^i$ and $b_{-1} = 0, b_i = 0\ \forall i > m$ and $p \nmid b_s$
   Then the coefficient of $f(x)g(x)$ is
   $$p| \sum_{i=0}^{r+s} a_i b_{r+s-i} = \sum_{i=0}^{r-1} a_i b_{r+s-i} + a_r b_s + \sum_{i=r+1}^{r+s} a_i b_{r+s-i} \implies p|a_r b_s$$
   which means $p|a_r$ or $p|b_s$ $(\rightarrow\leftarrow)$
2. $\mathrm{cont}(fg) = \mathrm{cont}(f)\,\mathrm{cont}(g)$: Write $f(x) = \mathrm{cont}(f) f_1(x), g(x) = \mathrm{cont}(g) g_1(x)$
   with f_1, g_1 are primitive. Then $\mathrm{cont}(fg) = \mathrm{cont}(f)\,\mathrm{cont}(g)\,\mathrm{cont}(f_1 g_1) = \mathrm{cont}(f)\,\mathrm{cont}(g)$

□

Theorem 2.5.3. (Gauss lemma 2.) Let R be a UFD and $F = R_S$ where $S = R\backslash\{0\}$ (we call F is the **field of fraction** of R). For $f(x) \in R[x]$, if $f(x) = A(x)B(x)$ with $A(x), B(x) \in F[x] \setminus F$, then f is reducible in $R[x]$.

Specifically, there exists $r, s \in F$ s.t $rA(x) = a(x) \in R[x], sB(x) = b(x) \in R[x]$ and $f(x) = a(x)b(x)$

Proof: We write $A(x) = \frac{\ell_1}{t_1} a_1(x), B(x) = \frac{\ell_2}{t_2} b_1(x)$ with $a_1(x), b_1(x)$: primitive and $\ell_i, t_i \in R$ with $\gcd(\ell_i, t_i) = 1\ \forall\ i = 1, 2 \implies t_1 t_2 f(x) = \ell_1 \ell_2 a_1(x) b_1(x)$
$\implies t_1 t_2\,\mathrm{cont}(f) = \ell_1 \ell_2 u$ with $u \in R^\times$. Hence,

$$f(x) = \frac{u^{-1} t_1 t_2\,\mathrm{cont}(f)}{t_1 t_2} a_1(x) b_1(x) = \left(u^{-1}\,\mathrm{cont}(f) a_1(x)\right) b_1(x) = a(x)b(x)$$

where $a(x) = (u^{-1}\,\mathrm{cont}(f) a_1(x) \in R[x]$ and $b(x) = b_1(x) \in R[x]$. □

Theorem 2.5.4. (Gauss lemma 3.) If $f(x)$ is primitive of $\deg f > 0$ in $R[x]$, then $f(x)$ is irreducible in $F[x] \iff f(x)$ is irreducible in $R[x]$

Proof: ($\Leftarrow$) by Gauss lemma 2.

($\Rightarrow$) If $f(x) = g(x)h(x)$ with $\deg g, \deg h > 0$ in $R[x]$, then $f(x) = g(x)h(x)$ in $F[x]$ and $g(x), h(x)$ are still not unit in $F[x]$. □

Theorem 2.5.5. $R : \text{UFD} \implies R[x] : \text{UFD}$

Proof: Let F be the field of fraction for R. For $f(x) \in R[x] \setminus (R[x]^\times \cup \{0\})$, write $f(x) = \text{cont}(f)f_1(x)$, $f_1(x)$: primitive. We may assume $\deg f > 0$ (constant has been done in R)

- $\text{cont}(f) \in R$ which is a UFD, it can be uniquely factorization
- $f_1(x)$ has a factorization:

  $f_1(x) \in R[x] \subseteq F[x]$: ED$\rightsquigarrow$ UFD, thus we can factor $f_1(x)$ in $F[x]$, say $f_1(x) = p_1(x)p_2(x)\cdots p_r(x)$, where $p_i(x)$ is irreducible in $F[x]$.

  By lemma 2. $\exists\ r_i \in F$ s.t. $q_i := r_i p_i(x) \in R[x]\ \forall\ i$ and $f(x) = q_1(x)\cdots q_r(x)$

  (Note that $p_i(x)$ is primitive $\implies$ $q_i(x)$ is primitive)

  We have that $q_i(x) = r_i p_i(x)$ is also irreducible in $F[x]$. Therefore, $f_1(x) = q_1(x)\cdots q_r(x)$ is factorization
- factorization of $f_1(x)$ is unique:

  Assume that $f_1(x) = p_1(x)\cdots p_r(x) = q_1(x)\cdots q_s(x)$ with p_i, q_j : primitive and irreducible in $R[x]$.

  By uniqueness of factorization in $F[x]$, we know that $r = s$ and $p_i \sim q_i\ \forall\ i$ is associate in $F[x]$

  $p_i \sim q_i$ in $F[x] \implies p_i(x) = \frac{\ell_i}{t_i} q_i(x) \implies t_i p_i(x) = \ell_i q_i \rightsquigarrow t_i \sim q_i$ in $R[x] \implies \ell_i = u_i t_i \implies p_i(x) = u_i q_i(x) \implies p_i \sim q_i$ in $R[x]$

□

2.5.2 Ring of Gauss integer

Let $A_{-1} = \{a + b\sqrt{-1} | a, b \in \mathbb{Z}\}$ by $N(a + b\sqrt{-1}) = a^2 + b^2$, A_{-1} is ED $\implies$ A_{-1} is UFD (All unit in $A_{=1}$ are $\pm 1, \pm\sqrt{-1}$ since only them has norm of value 1)

Definition 2.5.2 (Gauss prime)**.** The prime elements of A_{-1} are called **Gauss prime**

Property 2.5.1. If α is Gauss prime, then $N(\alpha) = p$ or p^2 for some prime integer p.

Proof: Let $\alpha\overline{\alpha} = N(\alpha) = p_1 p_2 \cdot p_n \in \mathbb{Z} \implies \alpha | p_1 p_2 \cdots p_n \in \mathbb{Z}[\sqrt{-1}]$. Since α is prime, $\alpha | p_j$ for some $j \rightsquigarrow N(\alpha) | N(p_j) = p_j^2 \rightsquigarrow N(\alpha) = p_j$ or p_j^2 □

Note: If α is Gauss prime and $N(\alpha) = p^2 \implies \alpha | p^2 \rightsquigarrow \alpha | p$. Write $p = \alpha\beta \implies p^2 = N(p) = N(\alpha)N(\beta) \implies \beta$ is unit i.e. p is irreducible and then $\alpha \sim p$

Property 2.5.2. Let p be an prime integer. Then
p is Gauss prime $\iff x^2+1$ is irreducible in $(\mathbb{Z}/p\mathbb{Z})[x]$

Proof: Consider $\begin{array}{rccc}\phi: & \mathbb{Z}[x] & \to & \mathbb{Z}[\sqrt{-1}] \\ & x & \mapsto & \sqrt{-1}\end{array}$ which is a ring homomorphism.

Claim: $\ker\phi = \langle x^2+1\rangle$
pf. $f(x)\in\ker\phi \iff f(\sqrt{-1})=0 \iff f(\sqrt{-1})=f(-\sqrt{-1})=0$
$\iff (x^2+1)|f(x)$ □

By 1st iso.thm,

$$\mathbb{Z}[x]/\langle x^2+1\rangle \simeq \mathbb{Z}[\sqrt{-1}]$$

p is Gauss prime $\iff \langle p\rangle \in \mathbb{Z}[\sqrt{-1}]$ is maximal
$\iff \langle p, x^2+1\rangle/\langle x^2+1\rangle$ is maximal (Since $\langle p, x^2+1\rangle = \phi^{-1}(\langle p\rangle)$)
By 3rd iso.thm,

$$\left(\mathbb{Z}[x]/\langle x^2+1\rangle\right) / \left(\langle p, x^2+1\rangle/\langle x^2+1\rangle\right) \simeq \mathbb{Z}[x]/\langle p, x^2+1\rangle \simeq (\mathbb{Z}/p\mathbb{Z})[x]/\langle x^2+1\rangle$$

$$\begin{aligned}
&\langle p, x^2+1\rangle/\langle x^2+1\rangle \text{ is maximal ideal in } \mathbb{Z}[x]/\langle x^2+1\rangle \\
\iff &\left(\mathbb{Z}[x]/\langle x^2+1\rangle\right) / \left(\langle p, x^2+1\rangle/\langle x^2+1\rangle\right) \text{ is a field} \\
\iff &(\mathbb{Z}/p\mathbb{Z})[x]/\langle x^2+1\rangle \text{ is a field} \\
\iff &\langle x^2+1\rangle \text{ is maximal in } (\mathbb{Z}/p\mathbb{Z})[x] \text{ (is PID)} \\
\iff &x^2+1 \text{ is irreducible in } (\mathbb{Z}/p\mathbb{Z})[x]
\end{aligned}$$

□

Property 2.5.3. $p=\alpha\overline{\alpha} \iff p\equiv 1 \pmod 4$ or $p=2$.
(Thus p is Gauss prime $\iff p\equiv \pmod 4$)

Proof:

$$\begin{aligned}
&p \text{ is not a Gauss prime} \\
\iff &x^2+1 \text{ is reducible in } (\mathbb{Z}/p\mathbb{Z})[x] \\
\iff &x^2\equiv -1 \pmod p \text{ has an integer solution} \\
\iff &\exists a\in\mathbb{Z} \text{ s.t. } o(\overline{a})=4 \text{ in } \mathbb{Z}/p\mathbb{Z} \text{ or } p=2 \\
\iff &p\equiv 1 \pmod 4 \text{ or } p=2
\end{aligned}$$

For $\Leftarrow$ in the last arrow: $4\big|\,|(\mathbb{Z}/p\mathbb{Z})^\times|$. By Sylow theorem, there exists a subgroup of order 4, by $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic, we have the subgroup is cyclic. □

Theorem 2.5.6. Let $n=2^k p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}q_1^{b_1}q_2^{b_2}\cdots q_s^{b_s}$ with $a_i\equiv 1 \pmod 4, q_j\equiv 3 \pmod 4$. Then $n=A^2+B^2$ for some $A,B\in\mathbb{Z} \iff b_i\equiv 0 \pmod 2\ \forall i$

Moreover, if it have integer pair solution, then it have $4(a_1+1)(a_2+1)\cdots(a_r+1)$ pairs of solution.

Proof: ($\Rightarrow$) $n = N(A+B\sqrt{-1})$, factorize $A+B\sqrt{-1} = \alpha_1\alpha_2\cdots\alpha_k$ in $\mathbb{Z}[\sqrt{-1}]$ $\Longrightarrow$ $n = N(\alpha_1)N(\alpha_2)\cdots N(\alpha_k)$. Since $p_i = 2$ or $p_i \equiv 1 \pmod 4$ $\Longleftrightarrow$ $N(\alpha_i) = p_i, q_i \equiv 3 \pmod 4$ $\Longleftrightarrow$ $N(\alpha_i) = q_i^2$,. Thus, $b_i \equiv 0 \pmod 2$

($\Leftarrow$) $2 = (1+\sqrt{-1})(1-\sqrt{-1}), p_i = \alpha_i\overline{\alpha_i}$.

Let $A + B\sqrt{-1} = (1+\sqrt{-1})^k\alpha^{a_1}\cdots\alpha_r^{a_r}q_1^{b_1/2}\cdots q_s^{b_s/2}$ in $\mathbb{Z}[\sqrt{-1}]$

$\Longrightarrow$ $n = N(A+B\sqrt{-1}) = A^2 + B^2 - (*)$

Moreover, $N(\alpha) = N(\overline{\alpha})$, we can choose $\alpha_i^k\,(\overline{\alpha_i})^{a_i-k}$ replace α^{a_1} in $(*)$ and multiple a unit, so there have $4(a_1+1)\cdots(a_r+1)$ distinct pairs of solution. $\square$

Chapter 3

Field theory

3.1 Algebraic extensions

Definition 3.1.1.

- E/F is called an **extension of fields** if E is a field and F is a subfield of E and we can regard E as a vector space over F.
- E/F is **finite** if $[E:F] := \dim_F(E) < \infty$
- E/F is **algebraic** if $\forall \alpha \in E\ \exists a_n, a_{n-1}, ..., a_0 \in F$ are not all zero s.t.

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$$

- Given E/F and A is a subset of E, $F(A) :=$ the smallest subfield of E containing A and F, and it is clear that

$$F(A) = \left\{ \frac{P(\alpha_1, \alpha_2, ..., \alpha_n)}{Q(\alpha_1, \alpha_2, ..., \alpha_n)} \middle| \alpha_1, ..., \alpha_n \in A, \frac{P(x_1, ..., x_n)}{Q(x_1, ..., x_n)} \in F[x_1, x_2, ..., x_n] \right\}$$

- $E = F(\alpha)$ is called a **simple extension**
- Consider the **evaluation map** $\begin{array}{rccc} ev_\alpha : & F[x] & \to & F[\alpha] \\ & x & \mapsto & \alpha \end{array}$
  - α is **algebraic** over F if $\ker ev_\alpha \neq \{0\}$
  - α is **transcendental** over F if $\ker ev_\alpha = \{0\}$

Property 3.1.1. Given E/F and $\alpha \in E$, if α is alg/F, then $\exists!$ monic irr. poly. of minimal degree s.t. $m_{\alpha,F}(\alpha) = 0$ and "$\forall f \in F[x]$ with $f(\alpha) = 0 \implies m_{\alpha,F} | f$"

Proof: By def, $\ker ev_\alpha \neq \{0\}$ and since $F[x]$ is a PID $\implies \exists h(x) \in F[x]$ s.t. $\ker ev_\alpha = \langle h(x) \rangle$. Notice that $\langle h(x) \rangle = \langle g(x) \rangle \iff h(x) \sim g(x)$, then we pick $m_{\alpha,F}$ to be monic s.t. $\langle m_{\alpha,F} \rangle = \langle h(x) \rangle$ and thus it is unique.

Also, $f(\alpha) = 0 \rightsquigarrow f \in \ker ev_\alpha \rightsquigarrow m_{\alpha,F} | f$.

If $m_{\alpha,F} = f_1(x)f_2(x) \rightsquigarrow 0 = f_1(\alpha)f_2(\alpha) \rightsquigarrow f_1(\alpha) = 0$ or $f_2(\alpha) = 0$ (say $f_1(\alpha) = 0$) $\rightsquigarrow m_{\alpha,F} | f_1 \implies f_2$ is unit. $\square$

Remark 3.1.1.

- Define the **degree of** α **over** F is $\deg m_{\alpha,F}$
- Each root of $m_{\alpha,F}(x)$ in E has same min. poly. as α

Theorem 3.1.1. TFAE
(1) α is alg/F (2) $F[\alpha] = F(\alpha)$ (3) $[F(\alpha) : F] < \infty$

Proof:
(1) $\iff$ (2) :

- ($\Rightarrow$) By 1st iso.thm, $F[x]/\langle m_{\alpha,F}\rangle \simeq F[\alpha]$ is a field (since $m_{\alpha,F}$ is irr.)
  $\implies F(\alpha) \subseteq F[\alpha]$. By def, $F[\alpha] \subseteq F(\alpha) \implies F(\alpha) = F[\alpha]$
- $\alpha^{-1} \in F(\alpha) = F[\alpha]$, say $\alpha^{-1} = f(\alpha) \rightsquigarrow \alpha$ is a root of $xf(x) - 1 = 0$

(1) $\iff$ (2) :

- ($\Rightarrow$) Assume $\deg m_{\alpha,F} = n$
  Claim: $\{1, \alpha, ..., \alpha^{n-1}\}$ form a basis for $F(\alpha)$ over F
  pf. If $f(\alpha) := a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = 0 \rightsquigarrow f \in \ker ev_\alpha \rightsquigarrow a_0 = a_1 = \cdots = a_{n-1}$
  $\forall f(\alpha) \in F(\alpha) = F[\alpha]$, write $f(x) = g(x)m_{\alpha,F}(x) + r(x)$ with $\deg r < n$
  $\rightsquigarrow f(\alpha) = r(\alpha) \in \langle 1, \alpha, ..., \alpha^{n-1}\rangle$
- ($\Leftarrow$) Let $[F(\alpha) : F] = n$. Consider $\{1, \alpha, ..., \alpha^n\}$
  case1. $\exists \alpha^s = \alpha^t$ with $0 \le s < t \le n \impliedby x^t - x^s \in \ker ev_\alpha \rightsquigarrow \alpha$ is alg/F
  case2. $1, \alpha, ..., \alpha^n$ are distinct. $\because [F(\alpha) : F] = n \therefore \exists a_0, a_1, ..., a_n$ are not all zero s.t. $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0 \rightsquigarrow \alpha$ is alg/F

□

Example 3.1.1. Let $m_{\alpha,\mathbb{Q}} = x^3 - x^2 + x + 2$ and $\beta = 1 + 2\alpha - \alpha^2$. Find $m_{\beta,\mathbb{Q}}(x)$

Define $T : \begin{array}{ccc} \mathbb{Q}(\alpha) & \to & \mathbb{Q}(\alpha) \\ f(\alpha) & \mapsto & \beta f(\alpha) \end{array}$ and $\mathcal{B} = \{1, \alpha, \alpha^2\} \rightsquigarrow \begin{cases} T(1) = 1 + 2\alpha - \alpha^2 \\ T(\alpha) = 2 + 2\alpha + \alpha^2 \\ T(\alpha^2) = -2 + \alpha + 3\alpha^2 \end{cases}$

$\rightsquigarrow [T]_{\mathcal{B}} = \begin{pmatrix} 1 & 2 & -2 \\ 2 & 2 & 1 \\ -1 & 1 & 3 \end{pmatrix} \implies ch_T(x) = x^3 - 6x^2 + 4x + 17$ is irr. and monic

Notice that $0 = (ch_T(T))(1) = ch_T(\beta) \implies m_{\beta,\mathbb{Q}}(x) = x^3 - 6x^2 + 4x + 17$

Property 3.1.2. In homework 15 we will prove

1. If E/F and L/E are two field extensions, then

$$[L : F] = [L : E][E : F]$$

2. Let E/F be a field extension and A, B are two subsets of E, then
$$F(A \cup B) = F(A)(B)$$

and this two formula will be the key of calculate the degree of field extension.

Property 3.1.3. Given E/F, if $L = \{\alpha \in E | \alpha \text{ is alg}/F\}$, then L is a subfield of E.

Proof: For $\alpha, \beta \in L$. Observe that β is alg$/F \implies \beta$ is alg$/F(\alpha)$
Hence, $[F(\alpha, \beta) : F] = [F(\alpha)(\beta) : F(\alpha)][F(\alpha) : F] < \infty$
Since $\alpha \pm \beta, \alpha\beta, \frac{\alpha}{\beta}$ $(\beta \neq 0) \in F(\alpha, \beta) \rightsquigarrow F(\alpha \pm \beta), F(\alpha\beta), F(\frac{\alpha}{\beta}) \subseteq F(\alpha, \beta)$
$\rightsquigarrow [F(\alpha \pm \beta) : F].[F(\alpha\beta) : F], [F(\frac{\alpha}{\beta}) : F] < \infty \implies \alpha \pm \beta, \alpha\beta, \frac{\alpha}{\beta}$ is alg$/F$ □

Theorem 3.1.2. $[E : F] < \infty \iff E = F(\alpha_1, ..., \alpha_n)$ with α_i : alg$/F$ $\forall i$. In case, E/F is alg.

Proof: ($\Rightarrow$) Let $[E : F] = n$ and $E = F(\alpha_1) + F(\alpha_2) + \cdots F(\alpha_k) \subseteq F(\alpha_1, ..., \alpha_n) \subseteq E \rightsquigarrow E = F(\alpha_1, ..., \alpha_n)$. $\because [F(\alpha_i) : F] \leq [E : F] < \infty \implies \alpha_i$ is alg$/F$
($\Leftarrow$) Define $F_i = F(\alpha_1, ..., \alpha_i)$ and $F_0 = F$, then

$$[E : F] = \prod_{i=1}^{n} [F_i : F_{i-1}] = \prod_{i=1}^{n} [F_{i-1}(\alpha_i) : F_{i-1}] < \infty$$

□

Corollary 3.1.1. Given E/F and S is a subset of E, if $\forall \alpha \in S$ is alg$/F$. Then $F(S)/F$ is alg.
pf. Let $\beta \in F(S)$. Then $\exists x_1, ..., x_n \in S$ s.t. $\beta \in F(x_1, ..., x_n) \rightsquigarrow \beta$ is alg$/F$

Theorem 3.1.3. If E/L and L/F are alg. then E/F is alg.

Proof: $\forall \alpha \in E$, say $\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0$ for $a_i \in L \rightsquigarrow \alpha$ is alg$/F(a_1, a_2, ..., a_n$
Since $F(a_1, ..., a_n, \alpha) \subseteq L$ and
$[F(a_1, ..., a_n, \alpha) : F] = [F(\alpha_1, ..., \alpha_n)(\alpha) : F(\alpha_1, ..., \alpha_n)][F(\alpha_1, ..., \alpha_n) : F] < \infty \implies \alpha$ is alg$/F$ □

Example 3.1.2. Define $\overline{\mathbb{Q}} := \{\alpha \in \mathbb{R} | \alpha \text{ is alg}/\mathbb{Q}\}$ is called the **field of algebraic numbers**.

- $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty : [\overline{\mathbb{Q}}; \mathbb{Q}(\sqrt[n]{2})][\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] \geq n \ \forall \ n \in \mathbb{N}$
  since $m_{\sqrt[n]{2},\mathbb{Q}}(x) = x^n - 2$ (by Eisenstein's criterion it is irr.)
- $\overline{\mathbb{Q}} \neq \mathbb{R} : \mathbb{Q}$ is countable
  $\rightsquigarrow \{x^n + a_1x^{n-1} + \cdots + a_n | a_i \in \mathbb{Q}\}$ is countable
  $\rightsquigarrow V_n = \{\alpha \in \mathbb{R} | \alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0, a_i \in \mathbb{Q}\}$ is countable
  $\rightsquigarrow \overline{\mathbb{Q}} = \bigcup_{n=1}^{\infty} V_n$ is countable
  However, $\mathbb{R}$ is not countable, so $\overline{\mathbb{Q}} \neq \mathbb{R}$

3.2 Algebraic closure

Set-up: F, L : field, if $\sigma : F \to L$ is a non-trivial ring homo. Since kernel of σ is an ideal and not equal to $F \implies \ker\sigma = \{0\}$ i.e. σ is an injective homo. and $F\sigma(F) =: F^\sigma \subseteq L$. So we can regard F as a subfield of L.

- $f(x) = a_n x^n + \cdots + a_0 \in F[x]$, then define $f^\sigma(x) = a_n^\sigma x^n + \cdots + a_0^\sigma$, where $a_i^\sigma = \sigma(a_i)$, then
$$\begin{array}{ccc} F[x] & \longleftrightarrow & F^\sigma[x] \\ f(x) & \longleftrightarrow & f^\sigma(x) \end{array}$$
- E/F : an extension of field and $0 \neq \sigma : F \to L$. We want regard E as a subfield of L, which means
$$\begin{array}{ccc} F & \xrightarrow{\sigma} & L \\ \downarrow & \nearrow_{\tau} & \\ E & & \end{array}$$
commute and we will say $\tau : E \to L$ extends σ i.e. $\tau|_F = \sigma$
- If $\alpha \in E$ with $f(\alpha) = 0$ ($f(x) \in F[x]$), then $f^\sigma(\tau(\alpha)) = \tau(f(\alpha)) = 0$

Theorem 3.2.1. (Kronecker) Let $f(x)$ be a non constant poly. in $F[x]$. Then $\exists L/F$ s.t. L contains a roots of $f(x)$.

Proof: We factorize $f(x) = f_1(x)\cdots f_n(x)$ with f_i : irr. in $F[x]$
Since $f_1(\alpha) = 0 \rightsquigarrow f(\alpha) = 0$, we may assume that f is irr.
Also, since $F[x]$ is a PID and f is irr.$\rightsquigarrow L := F[x]/\langle f(x)\rangle$: field
Let $\begin{array}{rccc} \sigma : & F & \to & F[x]/\langle f(x)\rangle \\ & a & \mapsto & \overline{a} = a + \langle f(x)\rangle \end{array} \rightsquigarrow F \simeq F^\sigma \subseteq L$
Observe that $f^\sigma(\overline{x}) = f(x) + \langle f(x)\rangle = \overline{0}$ and we get a root. □

Definition 3.2.1.

- A field L is said to be **algebraically closed** if each non-constant polynomial $f(x) \in L[x]$ has a root in L.
- F^a is called an **algebraic closure** of F if F^a/F is alg. and $\forall f(x) \in F[x]$ splits completely over F^a i.e. $f(x) = a(x-\alpha_1)\cdots(x-\alpha_n)$ for some $a_i \in F^a$
(F^a/F is alg. $\implies$ F^a is "minimal" extension satisfy second condition)

Property 3.2.1. L is algebraic closed $\iff$ $L^a = L$

Proof: ($\Leftarrow$) Trivial
($\Rightarrow$) **Claim:** $\forall f(x) \in L[x]$ splits over L
pf. By induction on $\deg f = n$, $n = 1 \implies f(x) = ax + b$ has a root $\frac{-b}{a} \in L$
For $n > 1$, let $\alpha \in L$ be a root of $f(x)$. We have $f(x) = (x = \alpha)f_1(x)$ with $f_1(x) \in L[x]$ and $\deg f_1 = n - 1$
By induction hypothesis, $f_1(x) = a(x = \alpha_1)\cdots(x - \alpha_{n-1})$ with $\alpha_i \in L$
$\rightsquigarrow f(x) = a(x-\alpha)a(x = \alpha_1)\cdots(x-\alpha_{n-1})$ and done! □

Property 3.2.2. L^a is algebraic closed ($\rightsquigarrow (L^a)^a = L^a$)

Proof: Let $f(x) \in L^a[x]$ and $\alpha \in E/L^a$ (by Kronecker) be a root of $f(x) \rightsquigarrow \alpha$ is alg/$L^a \implies L^a(\alpha)/L^a$ is alg.
$\because L^a/L$ is alg. $\therefore L^a(\alpha)/L$ is alg. $\rightsquigarrow \alpha$ is alg/$L \rightsquigarrow \alpha \in L^a$ □

Property 3.2.3. Given E/F if E is algebraically closed , then $L = \{\alpha \in E | \alpha \text{ is alg}/F\}$ is an algebraic closure of F

Proof: $\forall f(x) \in F[x] \subseteq E[x] \rightsquigarrow f(x) = a(x-\alpha_1)\cdots(x-\alpha_n)$ with $\alpha_i \in E$
Which means α_i alg/F and thus $\alpha \in L$ □

Theorem 3.2.2. (Existence of algebraic closure) $\forall F$: field, F^a exists

Proof: Let $S = \{x_f | f \in F[x] \text{ with } \deg f \geq 1\}$ be a set of variables.
Consider the polynomial ring $F[S]$ and $I = \langle f(x_f) | \deg f \geq 1\rangle \subseteq F[S]$
Claim: $I \neq F[S]$

pf. Assume not, i.e. $1 \in F[S]$, say $1 = \sum_{i=1}^{n} g_i \cdot f_i(x_{f_i})$ with $g_i \in F[S]$. Write $x_i := x_{f_i}$ and assume $g_i \in F[x_1, x_2, ..., x_n, x_{n+1}, ..., x_m]$
By Kronecker thm, $\exists\ \alpha_i$ s.t. $f_i(\alpha_i) = 0\ \forall i = 1, 2, ..., n$.
Set $\alpha_j = 0\ \forall n+1 \leq j \leq m$. Then $0 = \sum_{i=1}^{n} g_i(\alpha_1, ..., \alpha_m) f_i(\alpha_i) = 1\ (\rightarrow\leftarrow)$ □
Let M be a maximal ideal of FS s.t. $I \subseteq M$
Now, let $L_1 = F[S]/M$ which is a field and $F \hookrightarrow F[S]/M =: L_1$
Also, $\forall f \in F[x]$ with $\deg f \geq 1$, we have $f(\overline{x_f}) = \overline{f(x_f)} = \overline{0} \rightsquigarrow f(x)$ has a root $\overline{x_f} \in L_1$.
By induction, $\exists L_1 \subseteq L_2 \subseteq \cdots$ s.t. $\forall f \in L_n[x]$ has a root in L_{n+1}.
Let $\widetilde{L} := \bigcup_{n=1}^{\infty} L_i$ which is a field and it is alg. closed by construction.
Take $L := \{\alpha \in \widetilde{L} | \alpha \text{ is alg}/F\}$. By Prop.3.2.3. L is alg. closure of F. □

Lemma 3.2.1. (Key lemma) Let $F(\alpha)/F$ be algebraic and $\sigma : F \to L$. Then
$\exists$ an extension τ of σ from $F(\alpha)$ to $L \iff \exists \beta \in L$ s.t. $m^{\sigma}_{\alpha,F}(\beta) = 0$

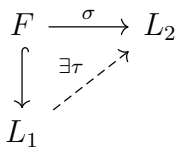
Proof: ($\Rightarrow$) Let $\beta = \tau(\alpha)$. Then $m_{\alpha,F}(\alpha) = 0 \rightsquigarrow m^{\sigma}_{\alpha,F}(\beta) = 0$
($\Leftarrow$) τ comes from the following diagram:

$$\begin{array}{ccc}
F & \xrightarrow{\sigma} & F^{\sigma} \subseteq L \\
\downarrow & & \downarrow \\
F[x] & \xrightarrow{\sim} & F^{\sigma}[x] \\
\downarrow & & \downarrow \\
F[x]/\langle m_{\alpha,F}\rangle & \xrightarrow{\sim} & F^{\sigma}[x]/\langle m_{\alpha,F}\rangle \\
\wr\downarrow ev_{\alpha} & & \wr\downarrow ev_{\beta} \\
F(\alpha) = F[\alpha] & \xrightarrow{\exists\tau} & F^{\sigma}[\beta] \subseteq L
\end{array}$$

and $\alpha \xrightarrow{ev_{\alpha}^{-1}} \overline{x} \xrightarrow{\sim} \overline{x} \xrightarrow{\beta} \beta \implies \tau(\alpha) = \beta$

□

Lemma 3.2.2. (Main lemma) If L_1/F is algebraic and $\sigma : F \to L_2$ with L_2 is algebraically closed, then σ extends to a homo. $\tau : L_1 \to L_2$



Proof: Let $S = \{(E, \theta) | F \subseteq E \subseteq L_1, \theta \text{ extends } \sigma\} \neq \emptyset$ (since $(F, \sigma) \in S$)

Define a partial order of $S : (E_1, \theta_1) \leq (E_2, \theta_2) \iff E_1 \subseteq E_2$ and $\theta_2|_{E_1} = \theta_1$

Given a chain $\mathcal{C} = \{(E_i, \theta_i) | i \in \Lambda\}$ in S, let $E = \bigcup_{i \in \Lambda} E_i$ which is a field containing $E_i \ \forall i$ and $\theta : E \to L_2$ defined by $E_i \ni \alpha \mapsto \theta_i(\alpha)$ which is well-defined. Then (E, θ) is a least upper bound for the chain $\mathcal{C}$. By Zorn's lemma, $\exists$ a maximal element $(L.\tau) \in S$

Claim: $L = L_1$

pf. Suppose not, say $\alpha \in L_1 \setminus L$ which is alg/F and thus is alg/L. Since L_2 is alg. closed, $\exists \beta \in L_2$ s.t. $m^{\tau}_{\alpha.L} = 0$. By key lemma, $\exists \tau' : \begin{array}{ccc} L(\alpha) & \to & L_2 \\ \alpha & \mapsto & \beta \end{array}$ s.t. $\tau'|_{L_2} = \tau \rightsquigarrow (L(\alpha), \tau') \gneq (L, \tau)$ $(\to\leftarrow)$ □

Theorem 3.2.3. (Uniqueness of algebraic closure) Any two algebraic closure L_1, L_2 of F are isomorphic.

Proof: Consider the inclusion map $\sigma : R \hookrightarrow L_2$

Since L_1/F is alg. and L_2 is alg. closed, by main lemma, $\exists\ 0 \neq \tau : L_1 \to L_2$ s.t. $\tau|_F = \mathrm{id}_F \rightsquigarrow L_1 \simeq \tau(L_1)$

Note L_1 is alg. closed $\rightsquigarrow L_1^{\tau}$ is also alg.closed. Also, $\forall \beta \in L_2, \beta$ is alg/F and thus is alg/$L^{\tau} \rightsquigarrow \beta \in L_1^{\tau} \implies L_2 \subseteq L_1^{\tau} \rightsquigarrow L_1^{\tau} = L_2$ i.e. $L_1 \simeq L_2$ □

3.3 Normal extensions

Definition 3.3.1. Let $f(x) \in (F[x] \setminus F)$. L is called a **splitting field** of f over F if L is the smallest field over F which f split.

Theorem 3.3.1. (Existence of a splitting field) If $\deg f = n > 0$, then $\exists$ a splitting field L of f over F s.t. $[L : F] \leq n!$

Proof: By induction on n. $n = 1 : f(x) = ax + b \rightsquigarrow L := F(\frac{-b}{a}) = F$ done!

$n > 1$. By Kronecker thm, $\exists F_1/F$ and $\alpha_1 \in F_1$ s.t. $f(\alpha_1) = 0$. By division algorithm, $\exists f_1(x) \in F(\alpha_1)[x]$ which $\deg f_1 = n - 1$ s.t. $f(x) = (x - \alpha_1) f_1(x)$.

By induction hypothesis, $\exists$ a splitting field L of f_1 over $F(\alpha_1)$ with $[L : F(\alpha)] \leq (n-1)!$. By def, $f_1(x) = a(x - \alpha_2) \cdots (x - \alpha_n)$ with $\alpha_i \in L \ \forall i = 2, ..., n$

Hence, $L = F(\alpha_1)(\alpha_2, ..., \alpha_n) = F(\alpha_1, \alpha_2, ...\alpha_n)$ which is a splitting field of f over F and

$$[L : F] = [L : F(\alpha)][F(\alpha) : F] \leq (n-1)! \cdot \deg m_{\alpha_1, F}(x) \leq (n-1)! \deg f = n!$$

Note: Let F^a be the alg. closure of F and $f(x) = a(x-\alpha_1)\cdots(x-\alpha_n)$. Then $L = F(\alpha_1, ..., \alpha_n)$ □

Theorem 3.3.2. Let $\sigma : F \to F'$ and $\begin{cases} L \text{ be a splitting field of } f(x) \text{ over } F \\ L' \text{ be a splitting field of } f^\sigma(x) \text{ over } F^\sigma \end{cases}$

Then $\exists \tau : L \xrightarrow{\sim} L'$ s.t. $\tau|_F = \sigma$. Moreover, the numbers of such τ is $\leq [L:F]$ and it is precisely equal to $[L:F]$ if f^σ has distinct roots in L'

Proof: By induction on $n = \deg f$. $n = 1 : L = F$ and $L' = F'$, so $\tau = \sigma$

$n > 1$, assume $f(\alpha) = 0$. Since $m_{\alpha,F}|f \rightsquigarrow m^\sigma_{\alpha,F}|f^\sigma, \exists \beta \in L'$ s.t. $m^\sigma_{\alpha,F}(\beta) = 0$

By key lemma, $\exists \sigma_1 : F(\alpha) \xrightarrow{\sim} F^\sigma(\beta)$ s.t. $\sigma_1|_F = \sigma$

There are at most $\deg m^\sigma_{\alpha,F} = \deg m_{\alpha,F} = [F(\alpha):F]$ distinct roots of $m^\sigma_{\alpha,F}$, so there are at most $[F(\alpha):F]$ extensions of σ.

On the other hands, we can write $f(x) = (x-\alpha)f_1(x)$ with $f_1(x) \in F(\alpha)[x]$. Note, L can we regard as a splitting field of f_1 over $F(\alpha)$ and $f^\sigma(x) = f^{\sigma_1}(x) = (x - \sigma_1(\alpha))f_1^{\sigma_1}(x)$. Similarly, $f_1^{\sigma_1}(x) \in F'(\beta)[x]$ and L' is also a splitting field of $f_1^{\sigma_1}$ over $F'(\beta)$. By induction hypothesis, $\exists \tau : L \to L'$ s.t. $\tau|_{F(\alpha)} = \sigma_1$

For fix $\sigma_1 : F(\alpha) \to F'(\beta)$. The number if such τ is $\leq [L : F(\alpha)]$ and " = " if f_1^σ has distinct roots. Totally, the number of such $\tau \leq [L:F(\alpha)][F(\alpha):F] = [L:F]$ and " = " if f^σ has distinct roots. □

Corollary 3.3.1. (Uniqueness of the splitting field)

Any two splitting fields of f over F are isomorphism

Proof: Apply identity in Theorem 3.3.2 □

Example 3.3.1. $f(x) = x^p - 2$ with p being a prime

- $m_{\sqrt[p]{2},\mathbb{Q}} = x^p - 2$ since $x^p - 2$ is irr.
- Let $\zeta_p = e^{\frac{2\pi i}{p}}$ be the p-th root of unity, then $\sqrt[p]{2}, \sqrt[p]{2}\zeta_p, ..., \sqrt[p]{2}\zeta_p^{p-1}$ are all root of $f(x)$
- $L = \mathbb{Q}(\sqrt[p]{2}, \zeta_p)$ is the splitting field of f over $\mathbb{Q}$
  - $[L:\mathbb{Q}] = [L:\mathbb{Q}(\zeta_p)][\mathbb{Q}(\zeta_p):\mathbb{Q}] \rightsquigarrow (p-1)|[L:Q] \leq p(p-1)$
    since $x^{p-1} + x^{p-2} + \cdots + x + 1$ is irr. and have a root ζ_p
    and $m_{\sqrt[p]{2},\mathbb{Q}(\zeta_p)}|m_{\sqrt[p]{2},\mathbb{Q}} \implies [\mathbb{Q}(\zeta)(\sqrt[p]{2})] \leq [\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = p$
  - $[L:\mathbb{Q}] = [L:\mathbb{Q}(\sqrt[p]{2})][\mathbb{Q}(\sqrt[p]{2}):\mathbb{Q}] \rightsquigarrow p|[L:Q]$
  - $[L:\mathbb{Q}] = p(p-1)$

Definition 3.3.2. L/F is called a **normal extension** if $\forall \alpha \in L$ is alg/F and $m_{\alpha,F}$ splits over L

Theorem 3.3.3. Let $L/F \subseteq F^a/F$. TFAE

(1) $\forall 0 \neq \sigma : L/F \to F^a/F$ (which means σ is a homo. fixing F) $\implies \sigma(L) = L$

(2) L is the splitting field of a family of polynomials in $F[x]$

(3) $\forall$ irr. poly. $f(x) \in F[x] \implies$ either $f(x)$ has no roots in L or $f(x)$ splits over L

Proof:

- (1) $\Rightarrow$ (2) Let $\alpha \in L$ which is alg/F. By def, $m_{\alpha,F}$ splits over F^a
  For any $\beta \in F^a$ with $m_{\alpha,F}(\beta) = 0$. By ket lemma, $\exists \sigma_1 : F(\alpha) \xleftarrow{\sim} F(\beta)$
  $\because L/F$ is alg $\rightsquigarrow L/F(\alpha)$ is alg and F^a is alg. closed
  $\therefore$ By main lemma, $\exists \sigma : L \to F^a$ s.t. $\sigma|_{F(\alpha)} = \sigma_1$
  By assumption, $\sigma(\alpha) = \sigma_1(\alpha) = \beta \in L \rightsquigarrow m_{\alpha,F}$ splits over L and we get that L is the splittinn field of $\{m_{\alpha,F} | \alpha \in L\}$
- (1) $\Rightarrow$ (3) If $f(x)$ has a root α in L, then $f(x) = am_{\alpha,F}(x)$ for some $a \in F$. Similarly, $m_{\alpha,F}$ splits over $L \rightsquigarrow f$ split over L
- (2) $\Rightarrow$ (1) Let L be the splitting field of $\{f_i | i \in I\} \subseteq F[x]$
  Define $S = \{\alpha \in L | f_j(\alpha) = 0 \text{ for some } j \in I\}$. For given $0 \neq \sigma : L/F \to F^a/F$
  $\forall \alpha \in S$, say $f_j(\alpha) = 0 \implies f_j(\sigma(\alpha)) = 0 \rightsquigarrow \sigma(\alpha) \in S \subseteq L \implies \sigma(L) \subseteq L$
  For surjectivity, let $\beta \in L$ and $T = \{r \in L | m_{\beta,F}(\gamma) = 0\} \implies |T| < \infty$
  Consider $L_0 = F(T) \subseteq L$ and $[L_0 : F] < \infty$, Similarly, $\sigma(\gamma) \in T \rightsquigarrow \sigma(L_0) \subseteq L_0$.
  Since σ is a monomorphism, $[\sigma(L_0) : F] = [L_0 : F] \implies \sigma(L_0) = L_0$
  and thus $\beta \in L_0 \subseteq \operatorname{Im} \sigma$
- (3) $\Rightarrow$ (1) For given $\sigma : L/F \to F^a/F$ and $\alpha \in L$, $\sigma(\alpha)$ is a root of $m_{\alpha,F}(x)$
  $\because m_{\alpha,F}$ is irr. $\therefore m_{\alpha,F}$ splits over $L \rightsquigarrow \sigma(\alpha) \in L$. Hence, $\sigma(L) \subseteq L$
  By the same argument as (2) $\Rightarrow$ (1), $\sigma(L) = L$

□

Corollary 3.3.2. L/F is finite normal $\iff$ L is a splitting field of some polynomial over F

Proof: ($\Rightarrow$) Let $L = F(\alpha_1, ..., \alpha_n)$
$\because L$ is the splitting field of $\{m_{\alpha,F} | \alpha \in L\}$ $\therefore$ if L' is the splitting field of $\{m_{\alpha_i,F} | i = 1, ..., n\} \implies L' \subseteq L$
and $L = F(\alpha_1, ..., \alpha_n) \subseteq L' \subseteq L \rightsquigarrow L' = L$. Then L is the splitting field of $f := m_{\alpha_1,F} m_{\alpha_2,F} \cdots m_{\alpha_n,F}$
($\Leftarrow$) By theorem 3.3.3, L/F is normal
$\because L = F(\alpha_1, \alpha_2, ..., \alpha_n)$ with $f(x) = a(x - \alpha_1) \cdots (x - \alpha_n) \in F[x]$
$\therefore a_i$ is alg/$F \rightsquigarrow [L : F] < \infty$ □

Example 3.3.2. If $L \supseteq E \supseteq F$ with L/F is normal, then L/E is also normal but it not always has E/F is normal.
eg. $L = \mathbb{Q}(\sqrt[3]{2}, \omega) \rightsquigarrow L/\mathbb{Q}$ is normal but $E/ : F = \mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal.

Theorem 3.3.4. Let L/F be finite normal and $L \supseteq E \supseteq F$. TFAE

(1) E/F is normal

(2) $\forall \sigma \in \mathrm{Aut}(L/F) \implies \sigma(E) \subseteq E$

(3) $\forall \sigma \in \mathrm{Aut}(L/F) \implies \sigma(E) = E$

Proof: (1) $\Rightarrow$ (2) $\Rightarrow$ (3) had done before.
(3) $\Rightarrow$ (1) For $\alpha \in E \subseteq L$ with α is alg/F and $\beta \in L$ be a root of $m_{\alpha,F}$

$$\begin{array}{ccc} L & \overset{\sigma}{\underset{\sim}{\dashrightarrow}} & L \\ \uparrow & & \uparrow \\ F(\alpha) & \xrightarrow[\sim]{\exists \sigma_0} & F(\beta) \\ \uparrow & & \uparrow \\ F & \xhookrightarrow{\mathrm{id}} & F \end{array}$$

Consider $\mathrm{id} : F \to F$. By key lemma, $\exists \sigma_0 : F(\alpha) \xrightarrow{\sim} F(\beta)$ with $\sigma_0|_F = \sigma$
By Cor.3.3.2, L is the splitting field of f over F, and thus L is the splitting field of f over $F(\alpha)$ and L is the splitting field of $f^{\sigma_0}(= f)$ over $F(\beta)$. By Thm.3.3.2, $\exists \sigma : L \to L$ with $\sigma|_{F(\alpha)} = \sigma_0 \rightsquigarrow \beta = \sigma_0(\alpha) = \sigma(\alpha) \in E$ □

3.4 Separable extensions

Definition 3.4.1.

- A polynomial $f(x) \in F[x]$ is said to be **separable** over F if its irreducible factors have no multiple root in its splitting field L/F
- $\alpha \in L$ is said to be **separable** over F if $m_{\alpha,F}$ is separable over F
- L/F is said to be **separable** if $\forall \alpha \in L$ is separable over F
- If $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in F[x]$, then $f'(x) := n a_n x^{n-1} + \cdots 2a_2 x + a_1$ $(\rightsquigarrow (fg)' = f'g + fg')$

Criterion: Let $f(x)$ be monic with $\deg f > 0$ in $F[x]$. Then
$f(x)$ has no multiple roots $\iff \gcd(f, f') = 1$
pf. ($\Rightarrow$) Write $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$ with $\alpha_1, ..., \alpha_n \in F^a$ are distinct
Then $f'(x) = \sum_{i=1}^{n} \frac{f(x)}{x - \alpha_i} \rightsquigarrow (x - \alpha_i) \nmid f'(x) \rightsquigarrow \gcd(f, f') = 1$
($\Leftarrow$) Suppose $f(x) = (x - \alpha)^k g(x)$ with $k > 1$ and $g(x) \in F[x]$
$\rightsquigarrow f'(x) = (x - \alpha)^{k-1} ((k-1)g(x) + (x - \alpha)g'(x)) \rightsquigarrow (x - \alpha) | f(x), f'(x)$
$\rightsquigarrow (x - \alpha) | \gcd(f, f') = 1$ $(\rightarrow\leftarrow)$

Corollary 3.4.1. α is multiple root of $f(x) \iff \alpha$ is common roots of f and f'

Theorem 3.4.1. Any irreducible polynomial $f(x)$ is not separable over $F \iff F = p > 0$ and $f(x) = g(x^p)$ for some $g(x) \in F[x]$

Proof: ($\Rightarrow$) Let $\alpha \in F^a$ is a multiple root of $f(x) \rightsquigarrow m_{\alpha,F} | f, f'$
$\because f$ is irr. $\therefore m_{\alpha,F} \sim f \rightsquigarrow \deg m_{\alpha,F} = \deg f > \deg f' \rightsquigarrow f' \equiv 0$
If $F = 0$, then $f = c \in F$ ($\rightarrow\leftarrow$). We must have $F = p > 0$
Let $f(x) = b_0 + b_1 x + \cdots + b_m x^m$, $f' \equiv 0 \rightsquigarrow ib_i = 0 \ \forall \ i$. So if $b_i \neq 0$, then $p | i$.
That is $f(x) = b_0 + b_p x^p + \cdots + b_{np} x^{np} = g(x^p)$, where $g(x) = \sum_{i=0}^{n} b_{ip} x^i$

($\Leftarrow$) $f(x) = g(x^p) \rightsquigarrow f' \equiv 0$. so if $m_{\alpha,F} | f \rightsquigarrow m_{\alpha,F} | 0 = f' \rightsquigarrow \alpha$ is the multiple root of f □

Note: $f(x)$ is irreducible $\implies$ $g(x)$ is irreducible and not all b_i are in F^p,
where $F^p := \{x^p | x \in F\}$
pf. If $g(x) = g_1(x)g_2(x) \rightsquigarrow f(x) = g_1(x^p)g_2(x^p)$ ($\rightarrow\leftarrow$)
If $\forall i \ b_i = a_i^p \rightsquigarrow f(x) = a_0^p + a_p^p x^p + \cdots + a_{np}^p x^{np} = (a_0 + a_p x + \cdots a_{np} x^n)^p$ ($\rightarrow\leftarrow$)

Definition 3.4.2. F is said to be **prefect** if either $F = 0$ or $F = p$ with $F^p = F$

Property 3.4.1. F is perfect $\iff$ every polynomial in $F[x]$ is separable

Proof: ($\Rightarrow$) Ok!
($\Leftarrow$) If $F = p$ and $F^p \neq F$. Pick $b \in F \setminus F^p$
Claim: $x^p - b$ is inseparable over F
pf. We need to prove that $x^p - b$ is irr. in $F[x]$
If $x^p - b = g(x)h(x)$ in $F[x]$ with $g(x)$ monic and $1 \leq \deg g \leq p - 1$
Pick $\alpha \in F^a$ with $\alpha^p - b = 0$. Then $x^p - b = (x - \alpha)^p$
Since $F(\alpha)[x]$ is UFD $\implies$ $g(x) = (x - \alpha)^k \in F[x] \rightsquigarrow \alpha^k \in F$
$\because \gcd(p, k) = 1 \therefore \exists a, b \in \mathbb{Z}$ s.t. $ap + bk = 1 \rightsquigarrow \alpha = (\alpha^p)^a (k)^b \in F$ ($\rightarrow\leftarrow$) □

Theorem 3.4.2. Let $[L : F] = d$ and $0 \neq \sigma : F \to L'$. If L/F is separable $\forall \alpha \in L$, $m_{\alpha,F}^{\sigma}$ splits over L'. Then $\exists$ exactly d monomorphisms $\tau : L \to L'$ with $\tau|_F = \sigma$
Otherwise (without sep. or split), $\exists r < d$ such mono. τ

Proof:

- $m_{\alpha,F}$: separable $\implies$ $m_{\alpha,F}^{\sigma}$: Let E, E' be the splitting field of $m_{\alpha,F}, m_{\alpha,F}^{\sigma}$ over F

$$\begin{array}{ccc} E & \xrightarrow[\sim]{\tau} & E' \\ \uparrow & & \uparrow \\ F & \xrightarrow{\sigma} & F' \end{array}$$

  and τ be arbitrary extends σ from $E \to E'$. Write $m_{\alpha,F} = \prod_{i=1}^{\ell} (x - \alpha_i)$ with distinct roots α_i. Then $m_{\alpha,F}^{\sigma} = m_{\alpha,F}^{\tau}(x - \tau(\alpha_i))$ have distinct roots $\tau(\alpha_i)$.

- $m_{\alpha,F}^{\sigma}$ has ℓ distinct roots in $L' \rightsquigarrow \exists$ exactly ℓ mono. $\tau_1 : F(\alpha) \to L'$ s.t. $\tau_1|_F = \sigma$

- By induction on $d := \rightsquigarrow \tau = \sigma$

  For $d > 1$, pick $\alpha \in L \setminus F \rightsquigarrow \exists$ exactly $[F(\alpha) : F]$ mono. $\tau_1 : F(\alpha) \to L'$ s.t. $\tau_1|_F = \sigma$ (Otherwise, $r < [F(\alpha) : F]$ mono. τ_1)

  - $L/F(\alpha)$ is separable: Since $\forall \beta \in L,\ m_{\beta,F(\alpha)} | m_{\beta,F}$
  - $\forall \beta \in L, m^{\tau}_{\beta,F(\alpha)} | m^{\tau}_{\beta,F} = m^{\sigma}_{\beta,F}$: splits over $L' \rightsquigarrow m^{\tau}_{\beta,F(\alpha)}$ splits over L'
  - By induction hypothesis, $\exists$ exactly $[L : F(\alpha)]$ mono. $\tau : L \to L'$ s.t. $\tau|_{F(\alpha)} = \tau_1$ (Otherwise, $\exists r < [L : F(\alpha)]$ mono. τ)
    Totally, $\exists$ exactly $[L : F(\alpha)][F(\alpha) : F] = [L : F]$ mono. $\tau : L \to L'$ s.t. $\tau|_F = \sigma$ (Otherwise, $\exists r < [L : F]$ mono. τ)

□

Theorem 3.4.3. Given $F(\alpha_1, ..., \alpha_n)/F$ if α_i is sep$/F(\alpha_1, ..., \alpha_{i-1})$, then $F(\alpha_1, ..., \alpha_n)/F$ is separable.

Proof: Let L be the splitting field of $f(x) = \prod_{i=1}^{n} m_{\alpha_i,F}$ which is normal over F

Claim: Define $L_i = F(\alpha_1, ..., \alpha_n)$, then
$\exists\ [L_j : F]$ mono. $\tau_j : L_j \to L$ with $\tau|_F = \mathrm{id}_F$ □

pf. By induction on j, $j = 0 \rightsquigarrow \tau_0 = \sigma = \mathrm{id}_F$
For $j > 0$, observe that $m_{\alpha_j,L_{j-1}} | m_{\alpha_j,F} \rightsquigarrow m^{\tau_{j-1}}_{\alpha_j,L_{j-1}} | m^{\tau_{j-1}}_{\alpha_j,F} = m^{\sigma}_{\alpha_j,F} = m_{\alpha_j,F}$
Since $m_{\alpha,F}$ splits over $L \rightsquigarrow m_{\alpha_j,L_{j-1}}$ splits over L
Since α_j is sep. over L_{j-1}, by key lemma, $\exists$ exactly $[L_{j-1}(\alpha_j) : L_{j-1}]$ mono. $\tau : L_j \to L$ s.t. $\tau_j|_{L_{j-1}} = \tau_{j-1}$. Also, by induction hypothesis, $\exists [L_{j-1} : F]$ mono. $\tau_j : L_{j-1} \to L$ s.t. $\tau_{j-1}|_F = \mathrm{id}_F$. Hence, $\exists [L_j : L_{j-1}][L_{j-1} : F] = [L_j : F]$ mono. $\tau_j : L_j \to F$ s.t. $\tau_j|_F = \mathrm{id}_F$. Since L/F is normal, $\forall \beta \in F(\alpha_1, ..., \alpha_n),\ m_{\beta,F}$ splits over L. By thm.2, $F(\alpha_1, ..., \alpha_n)/F$ must be separable to ensure $\exists$ exactly $[L_n : F]$ mono. $\tau_n : L_n \to L$ s.t. $\tau_n|_F = \mathrm{id}_F$

Theorem 3.4.4. L/F is separable $\iff$ $L/E, E/F$ is separable

Proof: ($\Rightarrow$) L/E is separable since $m_{\alpha,E} | m_{\alpha,F}$. $E/F \subseteq L/F$: separable

($\Leftarrow$) $\forall \alpha \in L, m_{\alpha,E} = x^n + a_1 x^{n-1} + \cdots + a_0 \in E[x] \rightsquigarrow \alpha$ is separable over $F(\alpha_1, ..., \alpha_n)$. a_i is separable over $F(a_1, ..., a_{i-1})$. By theorem.3.4.3, $F(\alpha_1, ..., \alpha_n, \alpha)/F$ is separable □

Remark 3.4.1. Let $\sigma : F \xrightarrow{\sim} F'$. Let $f(x) \in F[x]$ with a splitting field L and $f^{\sigma} \in F'[x]$ with a splitting field L'. Then $\exists$ at most $[L : F]$ isom. $\tau : L \xrightarrow{\sim} L'$ s.t. $\tau|_F = \sigma$ and " = " holds if $f(x)$ is separable. (Notice that L'/F' is normal)

If L is a splitting field of f over F, then $|\operatorname{Aut}(L/F)| \leq [L : F]$ and " = " holds if L/F is separable.

Chapter 4

Galois theory

4.1 Galois extensions

Definition 4.1.1. L/F is a **Galois extension** if L/F is finite, normal and separable

Property 4.1.1. L/F is Galois $\iff |\operatorname{Aut}(L/F)| = [L:F] < \infty$

Proof: ($\Rightarrow$)Since L/F is finite normal extension, L is the splitting field of f over F and f is separable over $F \rightsquigarrow |\operatorname{Aut}(L/F)| = [L:F] < \infty$

($\Leftarrow$) Consider $\mathrm{id}_F : F \to F$ and by Thm.3.4.2. there exists at least $[L:F]$ monomorphisms $\tau : L/F \to L/F \rightsquigarrow L/F$ is separable. $\forall \alpha \in L, m_{\alpha,L}$ splits over F, which means L/F is normal and thus L/F is Galois. □

Example 4.1.1. $f(x) \in \mathbb{Q}[x]$ and L is splitting field of $f \rightsquigarrow L/\mathbb{Q}$ is Galois

Example 4.1.2. $f(x) = x^3 - 2 \rightsquigarrow L = \mathbb{Q}(\sqrt[3]{2}, \omega) \rightsquigarrow [L:\mathbb{Q}] = 6, |\operatorname{Aut}(L/\mathbb{Q})| = 6$

4.2 Finite fields

Theorem 4.2.1. There exists a finite field L with $|L| = q \iff q = p^n$ for some prime p and $n \in \mathbb{N}$

In this situation, L is unique up to isomorphism and we denoted by $\mathbb{F}_q$

Proof: ($\Rightarrow$) Let $L = p$ and $[L : \mathbb{Z}/p\mathbb{Z}] = n$ ($\because \{\overline{0}, \overline{1}, ..., \overline{p-1}\} \subseteq L$) $\rightsquigarrow q = p^n$

($\Leftarrow$) Let L be the splitting field of $f(x) = x^{p^n} - x$ over $\mathbb{Z}/p\mathbb{Z}$

Claim: $S = \{$the set of all roots of $f\}$ is a field.

pf. $(\alpha \pm \beta)^{p^n} = \alpha \pm \beta, (\alpha\beta)^{p^n} = \alpha\beta, (\alpha^{-1})^{p^n} = \alpha^{-1}$ □

Since L is the smallest field containing all roots of $f \rightsquigarrow L = S$

Also, $f' = -1$ has not root $\rightsquigarrow f$ has no multiple root i.e. $|L| = p^n$

Now, for any finite field L' with $|L'| = q, \forall \alpha \in L', \alpha^{p^n} = \alpha \rightsquigarrow L'$ is also a splitting field of f over $\mathbb{Z}/p\mathbb{Z}$. Hence, it is unique up to isomorphism. □

Theorem 4.2.2. If $n \in \mathbb{N}$ and $\mathbb{F}_q$ is a finite field, then $\exists! L/\mathbb{F}_q$ s.t. $[L : \mathbb{F}_q] = n$ ($L \simeq \mathbb{F}_{q^n}$) and it is Galois. Morover, $\mathrm{Aut}(\mathbb{F}_q^n/\mathbb{F}_q) = \langle \sigma_q \rangle$, where $\begin{array}{rccc} \sigma_q : & \mathbb{F}_{q^n} & \to & \mathbb{F}_{q^n} \\ & \alpha & \mapsto & \alpha^q \end{array}$

Proof: By Thm.4.2.1. $q = p^r$ for some $r \in \mathbb{N}$, Then $q^n = p^{nr}$. By Thm.4.2.1 $F_{q^n} = F_{q^{nr}}$ is the splitting field of $x^{p^{nr}} - x$ over $\mathbb{F}_p$ and thus $\mathbb{F}_{q^n}/\mathbb{F}_q$ is Galois.

For $\mathbb{F}_{q^n} \supseteq \mathbb{F}_q \supseteq \mathbb{F}_p$ and by $\mathbb{F}_{q^n}/\mathbb{F}$ is separable, normal and finite, we have $\mathbb{F}_{q^n}/\mathbb{F}_q$ is separable, normal and finite and thus $\mathbb{F}_{q^n}/\mathbb{F}_q$ is Galois and $|\mathrm{Aut}(\mathbb{F}_{q^n}/\mathbb{F}_q)| = [\mathbb{F}_{q^n} : \mathbb{F}_q] = n$

- $\sigma \in \mathrm{Aut}(\mathbb{F}_{q^n}/\mathbb{F}_q)$
  - homo: $(\alpha+\beta)^q = (\alpha^p + \beta^p)^{p^{r-1}} = \cdots = \alpha^q + \beta^q, (\alpha\beta)^q = \alpha^q\beta^q$
  - isom: σ_1 is $1-1$ and $|\mathbb{F}_{q^n}| < \infty$, so it is isom,
  - Fixes $\mathbb{F}_q$: $\forall \alpha \in \mathbb{F}_q, \alpha^q = \alpha$
- $o(\sigma_q) = n$
  - $\sigma^n = \mathrm{id} : \sigma_q^n(\alpha) = \alpha^{q^n} = \alpha \ \forall \alpha \in \mathbb{F}_{q^n}$
  - $o(\sigma_q) \geq n$: if $\sigma_q^m = \mathrm{id}$ for some $m < n$. Then $\alpha = \sigma_q^m(\alpha) = \alpha^{q^m} \ \forall \alpha \in \mathbb{F}_{q^n}$. But $x^{q^m} - x$ has only q^m roots. $(\to\leftarrow)$

  Hence, $\mathrm{Aut}(\mathbb{F}_{q^n}/\mathbb{F}_q) = \langle \sigma_q \rangle$ □

Property 4.2.1.

- $\{\text{subfield of } \mathbb{F}_{p^n}\} \longleftrightarrow \{\mathbb{F}_{p^m} : m|n\}$

  $pf.$ $E \subseteq \mathbb{F}_{q^n} \rightsquigarrow |E| = p^m$. Let $[\mathbb{F}_{q^n} : E] = \ell \rightsquigarrow p^n = (p^m)^\ell \implies m|n$

  Conversely, $\forall \alpha \in \mathbb{F}_{p^m}, \alpha^{p^m} = \alpha$. Let $n = m\ell$ and $q = p^m$

  $\rightsquigarrow \alpha = \alpha^q = \alpha^{q^2} = \cdots = \alpha^{q^\ell} = \alpha^{p^n} \implies \alpha \in \mathbb{F}_{p^n}$
- $\mathbb{F}_{p^{n_1}}, \mathbb{F}_{p^{n_2}} \subseteq \mathbb{F}_{p^{n_1 n_2}} \rightsquigarrow \bigcup_{n\geq 1} \mathbb{F}_{p^n}$ is a field. Actually, $\bigcup_{n\geq 1} \mathbb{F}_{p^n} = \mathbb{F}_p^a$

  $pf.$ $(\subseteq)$ OK! $(\supseteq)$ $\forall \alpha \in \mathbb{F}_p^a, \alpha$ is alg/$\mathbb{F}_p$. Let $n = \deg m_{\alpha,\mathbb{F}_p} \rightsquigarrow \alpha \in \mathbb{F}(\alpha) = \mathbb{F}_{p^n}$
- $\forall n \in \mathbb{N}, \exists$ irr. poly. in $\mathbb{F}_q[x]$ of degree n

  $pf.$ $\because (\mathbb{F}_{q^n}^\times, \cdot, 1)$ is cyclic, say $\mathbb{F}_{q^n}^\times = \langle \alpha \rangle \therefore \mathbb{F}_{q^n}^\times \subseteq \mathbb{F}_q(\alpha) \subseteq \mathbb{F}_{q^n}^\times \rightsquigarrow \mathbb{F}_{q^n} = \mathbb{F}(\alpha)$

  Then $m_{\alpha,\mathbb{F}_q}$ is irr. of degree $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$

Theorem 4.2.3. $x^{p^n} - x =$ the product of all distinct monic irr. poly in $\mathbb{F}_p[x]$ of degree d, where d run through all divisors of n.

($eg.$ $x^8 - x = x(x-1)(x^3+x^2+1)(x^3+x+1)$ in $\mathbb{F}_2$)

Proof: Since $\mathbb{F}_p$ is a perfect field, all irr. poly. in $\mathbb{F}_p[x]$ are separable. Also, if $f(x), g(x)$ are two monic irr. poly. in $\mathbb{F}_p[x]$ with $f(\alpha) = g(\alpha)$, then $f = m_{\alpha,\mathbb{F}_p} = g$. Hence, we can get the equality by checking that they have the same roots.

- LHS|RHS: $\forall \alpha \in \mathbb{F}_{p^n},\ \deg m_{\alpha,\mathbb{F}_p} = [\mathbb{F}_p(\alpha) : \mathbb{F}_p] \big| [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$, thus $m_{\alpha,\mathbb{F}_p}$ appears in RHS
- If β is a roots of some monic irr. poly. $p(x) \in \mathbb{F}_p[x]$ with $d = \deg p | n$, then $p(x) = m_{\beta,\mathbb{F}_p} \rightsquigarrow |\mathbb{F}_p(\beta)| = p^d$ and thus $\beta^{p^d} = \beta \implies \beta = \beta^{p^d} = \cdots = \beta^{p^n}$

Remark 4.2.1. If $\psi_p(d)$ is the number of monic irr. poly. of degree d in $\mathbb{F}_p[x]$, then $p^n = \sum_{d|n} d\psi_p(d)$

□

Definition 4.2.1. Möbius μ-function:

$$\mu(n) = \begin{cases} 1 & \text{, if } n = 1 \\ 0 & \text{, if } n \text{ has a square factor} \\ (-1)^r & \text{, if } n \text{ is a product of } r \text{ distinct prime factor} \end{cases}$$

Property 4.2.2. If $n \in \mathbb{N}$, then $\sum_{d|n} \mu(d) = \lfloor \frac{1}{n} \rfloor$

Definition 4.2.2.

- A real or complex valued function defined on $\mathbb{N}$ is called an **arithmetic function**
- Given f, g : two arithmetic function
  The **Dirichlet product** of f and g is defined to be $(f * g)(n) = \sum_{d|n} f(d)g(\frac{n}{d})$
  ($\rightsquigarrow f * g = g * f, (f * g) * h = f * (g * h)$)
- $I(n) = \lfloor \frac{1}{n} \rfloor$ is called the **identity function** ($\forall\ f, (f * I)(n) = (I * f)(n) = f(n)$)
- Define $u(n) = 1 \rightsquigarrow (\mu * u)(n) = (u * \mu)(n) = I(n)$

Property 4.2.3. (Möbius inverse formula) $f(n) = \sum_{d|n} g(d) \implies g(n) = \sum_{d|n} f(d)\mu(\frac{n}{d})$

Proof: Notice that $f(n) = \sum_{d|n} g(d)u(\frac{n}{d}) \implies f = g * u$
$\implies g = g * I = g * (u * \mu) = (g * u) * \mu = f * \mu$ □

Property 4.2.4. $p^n = \sum_{d|n} d\psi(d) \implies \psi(n) = \frac{1}{n} \sum_{d|n} p^n \mu(\frac{n}{d})$

Example 4.2.1.

- $\nu(n) =$ the number of positive factors of $n = \sum_{d|n} u(d) \rightsquigarrow 1 = u(n) = \sum_{d|n} \nu(d)\mu(\frac{n}{d})$
- $\sigma(n) =$ the sum of all positive factors of $n = \sum_{d|n} d \rightsquigarrow n = \sum_{d|n} \sigma(d)\mu(\frac{n}{d})$

- $\varphi(n)$ = Eulur φ-function
  - $\varphi(ab) = \varphi(a)\varphi(b)$ for $\gcd(a,b) = 1$
  - $F(n) := \sum_{d|n} \varphi(d) \rightsquigarrow F(p^r) = 1 + (p-1) + \cdots + (p^r - p^{r-1}) = p^r$

$$n = \prod_{i=1}^{k} p_i^{\alpha_i} \rightsquigarrow F(n) = \prod_{i=1} F(p_i^{\alpha_i}) = n \implies n = \sum_{d|n} \varphi(d) \rightsquigarrow \varphi(n) = \sum_{d|n} d\mu(\tfrac{n}{d})$$

4.3 Fundamental theorem of Galois theory

Recall: L/F : Galois = finite + separable + normal $\implies |\operatorname{Gal}(L/F)| = [L:F]$

Definition 4.3.1.
- If L/F is Galois, then define $\operatorname{Gal}(L/F) := \operatorname{Aut}(L/F)$
- If $G \leq \operatorname{Aut}(L/F)$, then define $L^G := \{\alpha \in L | \sigma(\alpha) = \alpha \ \forall \sigma \in G\}$

First, we recall a theorem in Homework 18.

Theorem 4.3.1. (Primitive element theorem) Let L be a finite extension of F.

- There exists an element $\alpha \in L$ such that $L = F(\alpha)$ if and only if there exists only a finite number of fields E such that $F \subset E \subset L$.
- If L is separable over F, then there exists an element $\alpha \in L$ such that $L = F(\alpha)$

Theorem 4.3.2. (Artin) If G is a finite subgroup of $\operatorname{Aut}(L)$, then L/L^G is Galois, $|G| = [L : L^G]$ and $G = \operatorname{Gal}(L/L^G)$

Proof: Let $\alpha \in L$ and $\{\sigma_1.\sigma_2, ..., \sigma_r\}$ be a maximal set of G such that $\sigma_1(\alpha), ..., \sigma_n(\alpha)$ are distinct.

- $\forall \tau \in G,\ \{(\tau \circ \sigma_i)(\alpha) | i = 1, ..., r\} = \{\sigma_i(\alpha) | i = 1, ..., r\}$
  $\tau\sigma_i(\alpha) = \tau\sigma_j(\alpha) \rightsquigarrow \sigma_i(\alpha) = \sigma_j(\alpha) \rightsquigarrow i = j$
  If $\exists\ \tau(\sigma_i(\alpha)) \notin \{\sigma_i(\alpha) | i = 1, ..., r\}$
  $\rightsquigarrow |\{\tau\sigma_i(\alpha) | i = 1, ..., r\} \cup \{\sigma_i(\alpha) | i = 1, ..., r\}| > r$ $(\rightarrow\leftarrow)$
- $\tau = \sigma_i^{-1} \implies \alpha \in \{\sigma_i(\alpha) | i = 1, ..., r\} \rightsquigarrow \alpha$ is root of $f_\sigma(x) = \prod_{i=1}^{r} (x - \sigma_i(\alpha))$
- Since the coefficient of $f_\alpha(x)$ are elementary symmetric poly. in $\sigma_1(\alpha), \sigma_2(\alpha), ..., \sigma_r(\alpha)$ and together with the 1st fact, $f_\alpha^\tau = f_\alpha\ \forall \tau \in G$ i.e. $f_\alpha(x) \in L^G[x]$
- $f_\alpha(x)$ is separable and splits over $L \rightsquigarrow L$ is a splitting field of $\{f_\alpha \in L^G[x] | \alpha \in L\}$ over $L^G \rightsquigarrow L/L^G$ is normal, separable.
- $[L : L^G] \leq |G| : \forall \alpha \in L,\ m_{\alpha, L^G} | f_\alpha \rightsquigarrow [L^G(\alpha) : L^G] \leq \deg f_\alpha \leq |G|$
  Let $\beta \in L$ s.t. $[L^G(\beta) : L^G]$ is max, say $m = [L^G(\beta) : L^G] \leq |G|$
  Claim: $L = L^G(\beta)$ $(\rightsquigarrow [L : L^G] = m \leq |G|)$

pf. If $\alpha_0 \in L^G \setminus L^G(\beta)$, then by the primitive element theorem, $L^G(\beta, \alpha_0) = L^G(\gamma)$ for some $\gamma \in L$.

However, $[L^G(\gamma) : L^G] = [L^G(\beta, \alpha_0) : L^G] > [L^G(\beta) : L^G]$ $(\rightarrow\leftarrow)$ □

- So L/L^G is Galois. By def, $|G| \leq |\operatorname{Gal}(L/L^G)| = [L : L^G] \leq |G| \rightsquigarrow |G| = [L : L^G]$ $\implies |G| = | = [L; L^G] = |\operatorname{Gal}(L/L^G)| \implies G = \operatorname{Gal}(L/L^G)$

□

Corollary 4.3.1. L/F is Galois $\iff L^{\operatorname{Gal}(L/F)} = F$

Proof: ($\Leftarrow$) By Artin theorem, $L/L^{\operatorname{Gal}(L/F)}$ is Galois $\implies L/F$ is Galois.

($\Rightarrow$) $|\operatorname{Gal}(L/F)| = [L : F]$. By Artin theorem, $[L : F] = |\operatorname{Gal}(L/F)| = [L : L^{\operatorname{Gal}(L/F)}]$. Since $F \subseteq L^{\operatorname{Aut}(L/F)} \subseteq L \implies F = L^{\operatorname{Gal}(L/F)}$ □

Theorem 4.3.3. (Fundamental theorem of Galois theory) Let L/F be Galois and $G = \operatorname{Gal}(L/F)$. Then

$$\begin{array}{ccc} \{E | E \text{ is a field and } F \subseteq E \subseteq L\} & \longleftrightarrow & \{H | H \leq G\} \\ E & \longmapsto & \operatorname{Gal}(L/E) \\ L^H & \longleftarrow & H \end{array}$$

- $\begin{cases} H \mapsto L^H \mapsto \operatorname{Gal}(L/L^H) = H & \text{(By Artin thm.)} \\ E \mapsto \operatorname{Gal}(L/E) \mapsto L^{\operatorname{Gal}(L/E)} = E & \text{(By Cor.4.3.1)} \end{cases}$
- If $E_1 = L^{H_1}, E_2 = L^{H_2}$, then $E_1 \subseteq E_2 \iff H_2 \leq H_1$
- If $E = L^H$, then $H \lhd G \iff E/F$ is normal:

  pf. E/F is normal $\iff \forall \sigma \in G, \sigma(E) = E \iff \forall \sigma \in G, \operatorname{Gal}(L/\sigma(E)) = \operatorname{Gal}(L/E) = H$

  $\tau \in \operatorname{Gal}(L/\sigma(E)) \iff \tau(\sigma(x)) = \sigma(x)\ \forall x \in E \iff \sigma^{-1}\tau\sigma(x) = x\ \forall x \in E \iff \sigma^{-1}\tau\sigma \in \operatorname{Gal}(L/E) \iff \tau \in \sigma H \sigma^{-1}$

  Hence, E/F is normal $\iff \forall \sigma \in G, H = \sigma H \sigma^{-1}\ \forall \sigma \in G \iff H \lhd G$ □
- If $H \lhd G$, then $G/H \simeq \operatorname{Gal}(E/F)$:

  pf. $H \lhd G \rightsquigarrow E/F$ is normal $\rightsquigarrow E/F$ is Galois

  Define $\phi : \begin{array}{ccc} G & \rightarrow & \operatorname{Gal}(E/F) \\ \sigma & \mapsto & \sigma|_E \end{array}$ (Since E/F is normal $\rightsquigarrow \sigma(E) = E$)

  For $\tau \in \operatorname{Gal}(E/F)$

$$\begin{array}{ccc} L & \overset{\exists\sigma}{\underset{\sim}{\dashrightarrow}} & L \\ {\scriptstyle \text{splitting field of } f \text{ over } E}\uparrow & & \uparrow{\scriptstyle \text{splitting field of } f^\tau \text{ over } E} \\ E & \xrightarrow[\sim]{\tau} & E \\ \uparrow & & \uparrow \\ F & \xrightarrow{\text{id}} & F \end{array}$$

Since L/F is finite normal extension, it is a splitting field of $f \in F[x]$ over $F \implies$ L is a splitting field of f, f^τ over F. Then exists σ extend τ form L to L and thus $\sigma|_E = \tau \rightsquigarrow \phi$ is onto.

And $\sigma \in \ker\phi \iff \sigma|_E = \mathrm{id}_E \iff \sigma \in \mathrm{Gal}(L/E) = H \rightsquigarrow \ker\phi = H$

By 1st iso. thm, $G/H \simeq \mathrm{Gal}(E/F)$

- $E_1 = L^{H_1}, E_2 = L^{H_2}$, then $E_1 \cap E_2 = L^{\langle H_1, H_2\rangle}, E_1E_2 = L^{H_1 \cap H_2}$

  $pf.$ $\alpha \in L^{\langle H_1,H_2\rangle} \iff \alpha \in L^{H_1} \cap L^{H_2} = E_1 \cap E_2$

  $\tau \in H_1 \cap H_2 \iff \tau$ fixed $E_1 = F(\alpha_1, ..., \alpha_n)$ and $E_2 = F(\beta_1, ..., \beta_m) \iff \tau$ fixed $F(\alpha_1, ..., \alpha_n, \beta_1, ..., \beta_m) = E_1E_2$

Property 4.3.1. Let L/F be Galois and N/F be arbitrary extension.Then LN/N is Galois and $\begin{array}{rccc}\phi: & \mathrm{Gal}(LN/N) & \xrightarrow{\sim} & \mathrm{Gal}(L/(L\cap N)) \\ & \sigma & \mapsto & \sigma|_L\end{array}$

Proof. Let L be a splitting field of a separable poly. $f \in F[x]$ over F, say $L = F(\alpha_1, ..., \alpha_n)$ with $\alpha_1, ..., \alpha_n$ are distinct roots of f. Then $LN = N(\alpha_1, ..., \alpha_n)$ which can be regard as a splitting field of f over $N \rightsquigarrow LN/N$ is Galois.

- ϕ is well-defined :

  $\because f(\sigma(\alpha_i)) = \sigma(f(\alpha_i)) = 0 \therefore \{\alpha_i\} = \{\sigma(\alpha_i)\}$

  Hence, $\forall\ h(\alpha_1, ..., \alpha_n) \in F(\alpha_1, ..., \alpha_n) = L, \sigma(h(\alpha_1, ..., \alpha_n)) = h(\sigma(\alpha_1), ..., \sigma(\alpha_n)) \in L$ i.e. $\sigma(L) \subseteq L$

- ϕ is $1-1$: $\sigma \in \ker\phi \iff \sigma|_L = \mathrm{id}_L \iff \sigma(\alpha_i) = \alpha_i\ \forall\ i \iff \sigma(LN) = \mathrm{id}_{LN}$

- ϕ is onto : Let $H = \mathrm{Im}\,\phi \rightsquigarrow H \leq \mathrm{Gal}(L/(L \cap N))$

  Claim: $L^H = L \cap N$ ($\rightsquigarrow H = \mathrm{Gal}(L/(L \cap N))$

  $pf.$ ($\supseteq$) $\forall x \in L \cap N.\ \forall \tau \in H$, say $\sigma|_L = \tau,\ \tau(x) = \sigma(x) = x$

  ($\subseteq$) $\forall \sigma \in \mathrm{Gal}(LN/N), \sigma(x) = x\ \forall x \in L^HN \rightsquigarrow N \subseteq L^HN \subseteq L^{\mathrm{Gal}(LN/N)} = N$

  $\rightsquigarrow N = L^HN \rightsquigarrow L^H \subseteq N$

Remark 4.3.1. If L/F is Galois and N/F is finite, then

$$[LN : F] = \frac{[L : F][N : F]}{[L \cap N : F]}$$

$pf.$ $\frac{[LN:F]}{[N:F]} = [LN : N] = [L : L \cap N] = \frac{[L:F]}{L\cap N:F}$

Definition 4.3.2 (Galois group)**.** Let $f(x) \in F[x]$ be separable and L be a splitting field of f over F. We called $\mathrm{Gal}(L/F)$ is the **Galois group** of $f(x)$ (Sometimes we will write $\mathrm{Gal}(f)$)

Remark 4.3.2. If $\deg f = n$, then $\mathrm{Gal}(L/F)$ can be regard as a subgroup of S_n
pf. Let $\alpha_1, ..., \alpha_n$ be all roots of f and define $R = \{\alpha_1, ..., \alpha_n\}$
$\forall \sigma \in \mathrm{Gal}(L/F), f(\sigma(\alpha)) = \sigma(f(\alpha)) = 0 \ \forall\ \alpha \in R \rightsquigarrow \sigma|_R$ is bijection.
Consider $\begin{array}{rccc} \phi: & \mathrm{Gal}(L/F) & \to & S_n \\ & \sigma & \mapsto & \sigma|_R \end{array}$ is homomorphism.

Example 4.3.1. For $n \in \mathbb{N}$, $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois and $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \sigma_p \rangle \simeq C_n$
$\{\text{subfields of } \mathbb{F}_{p^n}/\mathbb{F}_p\} \longleftrightarrow \{\mathbb{F}_{p^d} : d|n\}$ with $[E : \mathbb{F}_p] = d \longleftrightarrow \mathbb{F}_{p^d}$
$\{\text{subgroups of } C_n\} \longleftrightarrow \{\langle \sigma_p^d \rangle : d|n\}$ with $|H| = \frac{n}{d} \longleftrightarrow \langle \sigma_p^d \rangle$
Hence, $\mathbb{F}_{p^d} \longleftrightarrow |\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^d})| = \frac{n}{d} \longleftrightarrow \langle \sigma_p^d \rangle$

Theorem 4.3.4. $f(x)$ is sep. irr. with $\deg f = n$, then $\mathrm{Gal}(f) = \mathrm{Gal}(L/F)$ is a transitive subgroup of S_n

Proof: Let $R = \{\alpha_1, ..., \alpha_n\}$ is the set of roots for f, $L = F(\alpha_1, ..., \alpha_n)$. For α_i, α_j with $i \neq j, m_{\alpha_i,F} = \frac{1}{a_n} f = m_{\alpha_j,F}$, by key lemma, $\exists \tau : F(\alpha_i) \xrightarrow{\sim} F(\alpha_j)$. Since L is splitting field of f over $F(\alpha_i)$ and f^τ over $F(\alpha_j)$, there exists σ extend τ form L to $L \implies \exists \sigma \in \mathrm{Gal}(L/F)$ s.t. $\sigma(\sigma_i) = \sigma_j$ □

4.4 Example

Theorem 4.4.1. Let $F \neq 2$ and $f(x)$ is irreducible separable polynomial in $F[x]$ with $\deg f = n$. Let L be a splitting field of f over F, say $L = F(\alpha_1, ..., \alpha_n)$, where $\alpha_1, ..., \alpha_n$ are all distinct roots of f.
Define $\delta = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j) \in L$. Then

$$F(\delta) = L^{\mathrm{Gal}(L/F) \cap A_n}$$

Proof: Any transposition τ, $\tau(\delta) = -\delta \neq \delta$, so $\forall \sigma \in (\mathrm{Gal}(L/F) \cap A_n), \sigma(\delta) = \delta \implies F(\delta) \subseteq L^{\mathrm{Gal}(L/F) \cap A_n}$
We know that

$$|\mathrm{Gal}(L/F)/(\mathrm{Gal}(L/F) \cap A_n)| = \begin{cases} 1 & \rightsquigarrow \mathrm{Gal}(L/F) \leq A_n, \delta \in F \implies F(\delta) = F = L^{\mathrm{Gal}(L/F) \cap A_n} \\ 2 & \rightsquigarrow \exists \text{odd permutation } \tau', \tau'(\delta) = -\delta \end{cases}$$

For second case, $\delta \notin F$ but $\delta^2 \in F \implies [F(\delta) : F] = 2$

$$\begin{aligned} [L^{\mathrm{Gal}(L/F) \cap A_n} : F] &= |\mathrm{Gal}(L^{\mathrm{Gal}(L/F \cap A_n)}/F)| \\ &= |\mathrm{Gal}(L/F)/\mathrm{Gal}(L/(L^{\mathrm{Gal}(L/F) \cap A_n}))| = \frac{|\mathrm{Gal}(L/F)|}{|\mathrm{Gal}(L/F) \cap A_n|} = 2 \end{aligned}$$

Combine with $F \subseteq F(\delta) \subseteq L^{\mathrm{Gal}(L/F) \cap A_n}$, we have $F(\delta) = L^{\mathrm{Gal}(L/F) \cap A_n}$ □

Definition 4.4.1 (discriminant)**.** The **discriminant** of f is defined by $D := \delta^2$

Example 4.4.1. Let $f(x) = x^3+px+q$ be irreducible in $\mathbb{Q}(x)$ and $L = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$ be a splitting field of f over $\mathbb{Q}$ with $\alpha_1, \alpha_2, \alpha_3$: roots of f

$\because f$ is irr.

$\therefore \mathrm{Gal}(L/\mathbb{Q})$ is a transitive subgroup of S_3, that is A_3 ($\delta \in \mathbb{Q}$) or S_3 ($\delta \notin \mathbb{Q}$)

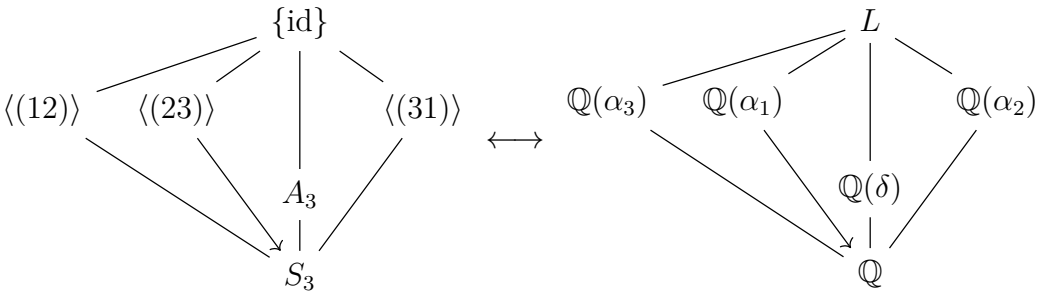
Let $A = \begin{pmatrix} 1 & 1 & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 \end{pmatrix} \implies \det A = \delta$

$$D = \delta^2 = \det AA^T = \det \begin{pmatrix} 1 & 1 & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 \end{pmatrix} \begin{pmatrix} 1 & \alpha_1 & \alpha_2 \\ 1 & \alpha_2 & \alpha_2^2 \\ 1 & \alpha_3 & \alpha_3^2 \end{pmatrix}$$

$$= \det \begin{pmatrix} 3 & \sum_{i=1}^3 \alpha_i & \sum_{i=1}^3 \alpha_i^2 \\ \sum_{i=1}^3 \alpha_i & \sum_{i=1}^3 \alpha_i^2 & \sum_{i=1}^3 \alpha_i^3 \\ \sum_{i=1}^3 \alpha_i^2 & \sum_{i=1}^3 \alpha_i^3 & \sum_{i=1}^3 \alpha_i^4 \end{pmatrix} = \det \begin{pmatrix} 3 & 0 & -2p \\ 0 & -2p & -3q \\ -2p & -3q & 2p^2 \end{pmatrix} = -4p^3 - 27q^2$$

Remark: So we know how to classify the Galois group of cubic polynomial. In Homework 21, we will tell you how to classify the Galois group of quartic polynomial.

Example 4.4.2. $\begin{cases} x^3 + 3x + 1 & \rightsquigarrow D = -135 \notin \mathbb{Q}^2 \rightsquigarrow \mathrm{Gal}(f) \simeq S_3 \\ x^3 - 3x + 1 & \rightsquigarrow D = 81 \in \mathbb{Q}^2 \rightsquigarrow \mathrm{Gal}(f) \simeq A_3 \end{cases}$



Example 4.4.3. $f(x) = x^4 + 2 \in \mathbb{Q}[x]$

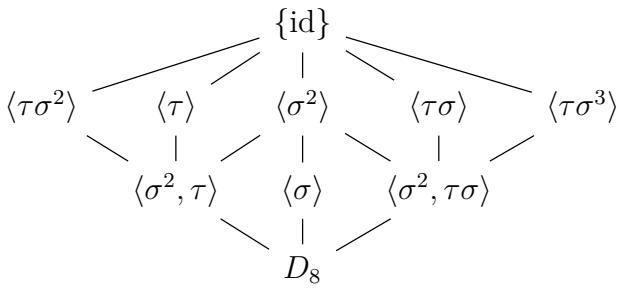
- Find the splitting field $L : x^4 + 2 = 0 \rightsquigarrow x = \frac{\sqrt[4]{2}(\pm\sqrt{2}\pm\sqrt{2}i)}{2}$
  and we can check that $\mathbb{Q}(\sqrt[4]{2}, i)$ is the splitting field of f over Q
- $[L : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2})(i) : \mathbb{Q}(\sqrt[4]{2}))][\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 8$. Let

$$\sigma : \begin{array}{ccc} L & \longrightarrow & L \\ \sqrt[4]{2} & \longmapsto & \sqrt[4]{2}i \\ i & \longmapsto & i \end{array} \qquad \tau : \begin{array}{ccc} L & \longrightarrow & L \\ \sqrt[4]{2} & \longmapsto & \sqrt[4]{2} \\ i & \longmapsto & -i \end{array}$$

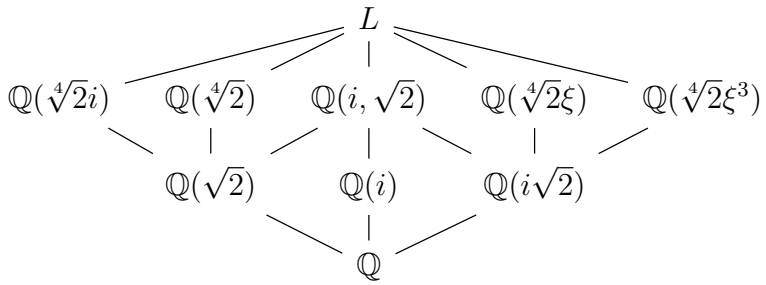
Then $o(\sigma) = 4, o(\tau) = 2$ and $\tau\sigma\tau^{-1} = \sigma^3 \implies \mathrm{Gal}(L/\mathbb{Q}) \simeq D_8$

- We want to see the correspondent, first we see this table:

	$\sqrt[4]{2}$	i	$\sqrt{2}$	$\frac{\sqrt{2}+i\sqrt{2}}{2} = \xi$
id	$\sqrt[4]{2}$	i	$\sqrt{2}$	ξ
σ	$\sqrt[4]{2}i$	i	$-\sqrt{2}$	$-\xi$
σ^2	$-\sqrt[4]{2}$	i	$\sqrt{2}$	ξ
σ^3	$-\sqrt[4]{2}i$	i	$-\sqrt{2}$	$-\xi$
τ	$\sqrt[4]{2}$	$-i$	$\sqrt{2}$	$-\xi i$
$\tau\sigma$	$\sqrt[4]{2}i$	$-i$	$-\sqrt{2}$	ξi
$\tau\sigma^2$	$-\sqrt[4]{2}$	$-i$	$\sqrt{2}$	$-\xi i$
$\tau\sigma^3$	$-\sqrt[4]{2}i$	$-i$	$-\sqrt{2}$	ξi



And it correspondent is



Theorem 4.4.2. (Ruffni-Abel theorem) Assume $F = 0$. The general equation of the n-th degree os not solvable by radical (we will learn it in the future) if $n \geq 5$. In fact, let $f(x) = x^n - t_1x^{n-1} + t_2x^{n-2} - \cdots + (-1)^n t_n \in F(t_1, ..., t_n)[x] =: K[x]$, where t_i are variables and L be a splitting field of f over K. Then $\mathrm{Gal}(L/K) \simeq S_n$ which is not solvable.

Before prove Ruffni-Abel theorem, we see a key property.

Property 4.4.1. Let $L = F(x_1, ..., x_n)$ and $s_1 = \sum x_i, s_2 = \sum x_ix_j, ..., s_n = x_1x_2 \cdots x_n$ be elementary symmetric polynomial in $x_1, ..., x_n$ (x_i are variables). If $K = F(s_1, ..., s_n) \subseteq L$, then L/K is Galois and $\mathrm{Gal}(L/K) \simeq S_n$

Proof: Write $f(x) = (x - x_1)(x - x_2) \cdots (x - x_n) = x^n - s_1x^{n-1} + s_2x^{n-2} - \cdots + (-1)^n s_n \in K[x]$.

Clearly, L is splitting field of f over $K \rightsquigarrow L/K$ is Galois and

$$\begin{array}{ccc} \mathrm{Gal}(L/K) & \hookrightarrow & S_n \\ \sigma & \mapsto & \sigma|_R \end{array}$$

where $R = \{x_1, ..., x_n\}$.
Conversely, for $\sigma \in S_n$, σ can be regarded as an auto. in $\mathrm{Gal}(L/K)$ via.

$$\begin{array}{rccc} \sigma: & L & \to & L \\ & x_i & \mapsto & x_{\sigma(i)} \end{array}$$

Since $\{x_{\sigma(i)}\} = \{x_i\} \implies \sigma(s_i) = s_i \ \forall i \rightsquigarrow \sigma|_K = \mathrm{id}_K \rightsquigarrow \sigma \in \mathrm{Gal}(L/K)$ □

Corollary 4.4.1. (Fundamental theorem of symmetric polynomial)
$F(s_1, ..., s_n) = K = L^{S_n} = \{f(x_1, ..., x_n) : f(x_{\sigma(1)}, ..., x_{\sigma(n)}) = f(x_1, ..., x_n) \ \forall \sigma \in S_n\}$

Corollary 4.4.2. For any finite group G, by Cayley theorem, $G \hookrightarrow S_n$ for some n. So $\mathrm{Gal}(L/L^G) \simeq G \rightsquigarrow G$ is Galois group.

Now, we can prove Ruffni-Abel theorem.

pf. Let $L = K(z_1, ..., z_n)$, where $z_1, ..., z_n$: roots of $f(x)$
$\rightsquigarrow t_1 = \sum z_i, t_2 = \sum z_i z_j, \cdots, t_n = z_1 \cdots z_n$
Let $F(s_1, ..., s_n)$ and $F(x_1, ..., x_n)$ be given in Prop.4.4.1
Since $t_1, t_2, ..., t_n$ are variables,

$$\begin{array}{rccc} \exists\tau: & F[t_1, ..., t_n] & \longrightarrow & F[s_1, ..., s_n] \\ & t_i & \longmapsto & s_i \end{array}$$

Also, $x_1, ..., x_n$ are variables,

$$\begin{array}{rccc} \exists\sigma: & F[x_1, ..., x_n] & \longrightarrow & F[z_1, ..., z_n] \\ & x_i & \longmapsto & z_i \end{array}$$

Now, $\sigma \circ \tau(t_i) = \sigma(s_i) = t_i \implies \sigma \circ \tau = \mathrm{id} \rightsquigarrow \tau$ is $1-1$ and that τ is an isom.
Then $\exists$ an extension $\tau' : F(t_1, ..., t_n) \xrightarrow{\sim} F(s_1, ..., s_n)$ ($s_1, ..., s_n$: alg. indep/F)
Notice that
$\tau' : f(x) \mapsto f^{\tau'} = x^n - s_1 x^{n-1} + s_2 x^{n-2} - \cdots + (-1)^n s'_n = (x - x_1) \cdots (x - x_n)$

$$\begin{array}{ccc} F(z_1, ..., z_n) & \overset{\exists\sigma'}{\overset{\sim}{\dashrightarrow}} & F(x_1, ..., x_n) \\ \uparrow \text{splitting field of } f \text{ over } F(t_1,...,t_n) & & \uparrow \text{splitting field of } f^{\tau'} \text{ over } F(s_1,...,s_n) \\ F(t_1, ..., t_n) & \xrightarrow{\tau'} & F(s_1, ..., s_n) \end{array}$$

Hence, $\mathrm{Gal}(L/K) \simeq S_n$ □

Example 4.4.4. (Newton identity) Let $P_k = \sum_{i=1}^{n} x^k$ and $S_i = \sum_{sym} x_1 x_2 \cdots x_i$, then

$$k s_k = \sum_{i=1}^{k} (-1)^i S_{k-i} P_i$$

Proof: Let $f(x) = \prod_{i=1}^{n}(x - x_i)$, then

$$\frac{f'(x)}{f(x)} = (\log f(x))' = \left(\log \prod_{i=1}^{n}(x - x_i)\right)' = \sum_{i=1}^{n} \frac{1}{x - x_i}$$

$$\implies x\sum_{i=1}^{n} iS_{n-i}(-1)^{n-i}x^{i-1} = f(x)\left(\sum_{i=1}^{n}\frac{1}{1-\frac{x_i}{x}}\right) = \left(\sum_{i=0}^{n}(-1)^{n-i}S_{n-i}x^i\right)\left(\sum_{i=1}^{n}\sum_{j\geq 0}\frac{x_i^j}{x^j}\right)$$

Consider coefficient of x^{n-k} in both side, then

$$(-1)^k kS_k = \sum_{i=0}^{n}(-1)^{n-(n-k+i)}S_{n-(n-k+i)}P_i = \sum_{i=1}^{k}(-1)^{k-i}S_{k-i}P_i$$

□

4.5 Applications 1

Theorem 4.5.1. $\mathbb{C}$ is algebraic closed

Proof:
Recall:

- $\forall f(x) \in \mathbb{R}[x]$ with $\deg f$ is odd, then $\exists \alpha \in \mathbb{R}$ s.t. $f(\alpha) = 0$
- $\mathbb{C}^2 = \mathbb{C}$

  Let $\alpha = a + bi \rightsquigarrow c := \frac{a+\sqrt{a^2+b^2}}{2}, d := \frac{a-\sqrt{a^2+b^2}}{2} \rightsquigarrow \alpha = (c + di)^2$

Given $g(x) \in \mathbb{C}[x]$, let α be a root of g and $E := \mathbb{R}(i)(\alpha)$
Since α is alg/$\mathbb{R}(i)$ and $\mathbb{R}(i)/\mathbb{R}$ is alg. $\implies$ α is alg/$\mathbb{R}$
Let L be the splitting field of $(x^2+1)m_{\alpha,\mathbb{R}}(x)$ over $\mathbb{R}$. Since $\mathbb{R} = 0$, we know that $L/\mathbb{R}$ is separable, finite and normal $\implies$ $L/\mathbb{R}$ is Galois and we have $L \supseteq \mathbb{C} \supseteq \mathbb{R}$
Claim: $L = \mathbb{R}(i)$
Let $G = \mathrm{Gal}(L/\mathbb{R}) \rightsquigarrow |G| = [L : G]$ and $2 = [\mathbb{R}(i) : \mathbb{R}]\big|[L : \mathbb{R}]$.
Pick $H \in \mathrm{Syl}_2(G)$ and $F = L^H$. By primitive element theorem, $F = \mathbb{R}(\beta)$
$\because [L : \mathbb{R}] = [L : L^H][L^H : \mathbb{R}] \implies [\mathbb{R}(\beta) : \mathbb{R}]$ is odd $\implies \deg m_{\beta,\mathbb{R}}$ is odd.
Since $m_{\beta,\mathbb{R}}$ has a root in $\mathbb{R}$ and $m_{\beta,\mathbb{R}}$ is irr. $\implies$ $m_{\beta,\mathbb{R}}(x) = x - \beta$
$\rightsquigarrow F = \mathbb{R}$ and thus $G = H$ is a 2-group.
Consider $G_1 = \mathrm{Gal}(L/\mathbb{R}(i))$. If $G_1 \neq \{e\}$, then $\exists G_2 \leq G_1$ s.t. $(G_2 : G_1) = 2$
Let $K = L_2^G \rightsquigarrow [K : \mathbb{R}(i)] = \frac{[L:R(i)]}{[L:K]} = \frac{|G_1|}{|G_2|} = 2$.
Since $K/\mathbb{R}(i)$ is separable, we have $K = \mathbb{R}(i)(\gamma) \rightsquigarrow m_{\gamma,\mathbb{C}} = x^2 + ax + b$.
But $\frac{-a\pm\sqrt{a^2-4b}}{2} \in \mathbb{C} \rightsquigarrow K = \mathbb{R}(i)$ $(\rightarrow\leftarrow)$ □
Hence, $\mathbb{C}$ is algebraic closed. □

Property 4.5.1. Let $f(x) \in \mathbb{Q}[x]$ be irreducible of degree p : prime
If f has exactly $(p-2)$ reals roots and 2 complex roots, then the Galois group of f over $\mathbb{Q}$ is S_p

Proof: Let L be a splitting field of f over $\mathbb{R}$ and R be the set of roots of f, say $R = \{\alpha_1, ..., \alpha_p\}$

Recall: $\begin{array}{ccc} G := \mathrm{Gal}(L/\mathbb{Q}) & \longrightarrow & S_p \\ \sigma & \longmapsto & \sigma|_R \end{array}$

- We define a relation on R : $\alpha_i \sim \alpha_j \iff (\alpha_i\ \alpha_j) \in G$ which is an equivalent relation :
  - $\alpha_i \sim \alpha_i$: $\mathrm{id} \in G$
  - $\alpha_i \sim \alpha_j \implies \alpha_j \sim \alpha_i$: Trivial
  - $\alpha_i \sim \alpha_j, \alpha_j \sim \alpha_k$: $(\alpha_i\ \alpha_j)(\alpha_j\ \alpha_k)(\alpha_i\ \alpha_j) = (\alpha_i\ \alpha_k)$
- $\big|[\alpha_i]\big| = \big|[\alpha_j]\big|$: $\because f$ is irr. $\therefore \exists \sigma \in G$ s.t. $\sigma(\alpha_i) = \alpha_j$

  Hence, $\tau :\ \begin{array}{ccc} [\alpha_i] & \longrightarrow & [\alpha_j] \\ \alpha_t & \longmapsto & \sigma(\alpha_t) \end{array}$
  - Well-defined : $(\alpha_j\ \sigma(\alpha_t)) = \sigma(\alpha_i\ \alpha_t)\sigma^{-1} \in G$
  - σ is $1-1 \rightsquigarrow \big|[\alpha_i]\big| \le \big|[\alpha_j]\big|$. By symmetry, $\big|[\alpha_j]\big| \le \big|[\alpha_j]\big| \implies \big|[\alpha_i]\big| = \big|[\alpha_j]\big|$
- $\because f(\overline{\alpha_i}) = \overline{f(\alpha_i)} = 0 \therefore$ We get an automorphism $\sigma :\ \begin{array}{ccc} L & \longrightarrow & L \\ \alpha_i & \longmapsto & \overline{\alpha_i} \end{array}$

  By assumption, let $\alpha_1, ..., \alpha_{p-2} \in \mathbb{R}, \alpha_{p-1}, \alpha_p \in \mathbb{C}$. Then, $\sigma|_R = (\alpha_{p-1}\ \alpha_p) \in G$
- $\because R = \bigcup [\alpha_i] \rightsquigarrow p = |R| \big| \sum \big|[\alpha_i]\big| \rightsquigarrow \big[\alpha_i]\big| p$ and $\big|[\alpha_{p-1}]\big| \ge 2 \rightsquigarrow \big|[\alpha_i]\big| = p$

  $\implies R = [\alpha_i] \rightsquigarrow \alpha_i \sim \alpha_j\ \forall i, j \implies (\alpha_i\ \alpha_j) \in G\ \forall i, j$

  Since S_p is generated by all 2-cycle $\implies G \simeq S_p$

□

Example 4.5.1. $f(x) = x^5 - 4x + 2$ has exactly 3 roots $\implies \mathrm{Gal}(f) \simeq S_5$

Theorem 4.5.2. (Lüroth's theorem) If $L = F(x)$ with x is trans/F, then $\forall E$: proper intermediate field between L and F, $\exists t$: trans/F s.t. $E = F(t)$

Proof:

Lemma. Let $t = \frac{f(x)}{g(x)} \in L \backslash F$ with $\gcd(f(x), g(x)) = 1$. Assume $n = \max\{\deg f, \deg g\}$. Then $L/F(t)$ is algebraic and $[F(x) : F(t)] = n$

pf. Write $f(x) = \sum_{i=0}^{n} a_i x^i, g(x) = \sum_{i=0}^{n} b_i x^i$, either $a_n \neq 0$ or $b_n \neq 0$ and $a_i, b_j \in F$

By def of t, we have $\sum_{i=0}^{n} (a_i - t b_i) x^i = 0$ and $(a_n - t b_n) \neq 0$

Then x is algebraic over $F(t)$ and $[F(x) : F(t)] \le n$

Claim: $h(y) = \sum_{i=0}^{n} (a_i - t b_i) y^i$ is irreducible in $F(t)[y]$ $(\rightsquigarrow [F(x) : F(t)] = n)$

pf. By Gauss lemma, it suffices to show that $h(y)$ is irr. in $F[t][y] = F[t, y]$

Assume that $h(y) = p(t, y)q(t, y)$ in $F[t, y]$ with $\deg_t p = 1$ and $q \in F[y] \setminus F$

Note that $q(y) | f(y), g(y) \rightsquigarrow q(y) | \gcd(f(y), g(y)) = 1 \rightsquigarrow q(y) \in F$ $(\rightarrow\leftarrow)$ □

□

For $s \in E \setminus F$, by Lemma x is alg/$F(s) \rightsquigarrow x$ is alg/E
Let $u(y) = m_{x,E}(y)$ and $\exists \beta(x) \in F[x]$ s.t.

$$\beta(x)u(y) = a_n(x)y^n + \cdots + a_1(x)y + a_0(x) =: v(x,y)$$

is primitive in $F[x][y]$, where $[L : E] = n$
Since x is not alg. over $F, \exists$ some $\frac{a_i(x)}{\beta(x)} \notin E \setminus F$
Let $t = \frac{a_i(x)}{\beta(x)}$ and write $t = \frac{f(x)}{g(x)}$ with $\gcd(f,g) = 1$. Let $m = \max\{\deg f, \deg g\}$
By lemma, $m = [F(x) : F(t)] \leq [F(x) : E] = n$ ($\because F(t) \subseteq E$)
Claim: $n \geq m$
pf. We consider the expression $\ell = f(x)g(y) - g(x)f(y)$
$\implies \frac{\ell}{g(x)} = \frac{f(x)}{g(x)}g(y) - f(y) \in E[y]$ and $g(x)^{-1}\ell$ has x as a zero
$\implies u(y) | g^{-1}(x)\ell$ in $E[y] \rightsquigarrow v(x,y) = \beta(x)u(y) | \beta(x)g(x)^{-1}\ell$ in $E[y] \subseteq F(x)[y]$
$\implies v(x,y) | \ell$ in $F(x)[y]$
$\because v(x,y)$ is primitive in $F[x][y]$ $\therefore v(x,y) | \ell(x,y)$ in $F[x][y]$ and say $\ell = vq$ for some $q(x,y) \in F[x][y]$. Now, $\deg_x \ell \leq m$ and $\deg_x v \geq m$. Since $\ell = vq \rightsquigarrow \deg_x \ell = \deg_x v = m$ and $\deg_x q = 0 \implies q \in F[y]$. In particular, q is primitive in $F[x][y]$. By Gauss lemma, ℓ is also primitive in $F[x][y]$. As ℓ is skew-symmetric in x and y, ℓ is also primitive in $F[y][x]$. But $q \in F[y]$ and $q | \ell$, so $q \in F$. Hence

$$n = \deg_y v = \deg_v \ell = \deg_x \ell = \deg_x v \geq m$$

□

By Claim, $n = m \rightsquigarrow E = F(t)$ and $F(x)/F(t)$ is alg. $\rightsquigarrow t$: trans/F □

Example 4.5.2. $E = F(y,z) \subseteq F(x)$ with $y = x^3 + x^{-3}, z = x^2 + x^{-2}$. Then $E = F(x + x^{-1})$

4.6 Cyclotomic extensions

Recall: $\zeta \in F$ is an n-th root of unity if $\zeta^n = 1$

- If $F = p$, then $x^{p^m} = 1 \rightsquigarrow (x-1)^{p^m} = 0 \rightsquigarrow x = 1$
  ($n = p^t m, \gcd(p,m) = 1$. $x^n = 1 \iff (x^m - 1)^{p^t} = 0 \iff x^m = 1$)
- If $F = p$ and $p | n$, then $x^n - 1$ is separable since $nx^{n-1} \neq 0$
  Define $\mu_n := \{\text{all } n\text{-th root unity in } F^a\} \leq ((F^a)^\times, \cdot, 1)$
  Fact: Every finite multiplication group in a field is cyclic
  pf. Assume G is a finite group of $F^\times$. Since G is abelian, by fundamental theorem of finite abelian group

$$G \simeq \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r, \ m_i | m_{i+1} \ \forall i$$

  If $r \geq 2$, then $m_r < n$. In RHS, each element satisfies $x^{m_r} - 1 = 0$.
  However, in a field, $x^{m_r} - 1 = 0$ has at most m_r roots, but $|LHS| = |G| > m_r (\rightarrow\leftarrow)$

Definition 4.6.1. Let $\mu_n = \langle \zeta_n \rangle$. ζ is called a primitive n-th root of unity. ($\zeta_n^n = 1$ and $\zeta_n^d \neq 1 \ \forall 0 < d < n$)

Note: $\{1, \zeta_n, ..., \zeta_n^{n-1}\}$ is the set of all n-th root of unity and $\{\zeta_n^d | \gcd(n,d) = 1\}$ is the set of all primitive n-th unity in F^a

Property 4.6.1. $F(\zeta_n)/F$ is Galois and we say it is **Cyclotomic extension**

Proof:

- ζ_n is alg$/F \rightsquigarrow F(\zeta_n)/F$ is finite
- separable : $m_{\zeta_n,F} | x^n - 1$ which is separable$\rightsquigarrow m_{\zeta_n,F}$ is separable
- normal : $\forall \sigma : F(\zeta)/F \to F^a/F$, $\sigma(\zeta_n)^n = \sigma(\zeta_n^n) = 1 \rightsquigarrow \sigma(\zeta_n) = \zeta_n^j \in F(\zeta_n)$
  $\implies \sigma(F(\zeta_n)) \subseteq F(\zeta_n) \rightsquigarrow F(\zeta_n)/F$ is normal

□

Property 4.6.2. $\mathrm{Gal}(F(\zeta_n)/F) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$

Proof: Define

$$\begin{array}{ccc} \mathrm{Gal}(F(\zeta_n)/F) & \longrightarrow & (\mathbb{Z}/n\mathbb{Z})^\times \\ (\sigma_k : \zeta_n \mapsto \zeta_n^k) & \longmapsto & \overline{k} \end{array}$$

for $1 \leq k \leq n$ and $\gcd(k,n) = 1$

- homo : $\sigma_{k_1} \circ \sigma_{k_2}(\zeta_n) = \zeta^{k_1 k_2} = \sigma_{k_1 k_2}(\zeta_n)$
- $1-1$: $\overline{k} = \overline{1} \iff \sigma_k = \sigma_1 = \mathrm{id}$

□

Note that we have

$$|\mathrm{Gal}\,(F(\zeta_n)/F)| \big| |\,(\mathbb{Z}/n\mathbb{Z})^\times\,| = \varphi(n)$$

and equality will not always right.
eg. $\zeta_5 = e^{\frac{2\pi i}{5}} \rightsquigarrow [\mathbb{R}(\zeta) : \mathbb{R}] = 2 < \varphi(5)$
(In fact, every finite extension of $\mathbb{R}$ is $\mathbb{R}$ or $\mathbb{C}$)

Theorem 4.6.1. $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ ($\implies \mathrm{Gal}(F(\zeta_n))/F) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$

Proof: Let $f(x) = m_{\zeta_n,\mathbb{Q}}(x) \rightsquigarrow f(x) | x^n - 1$, say $x^n - 1 = f(x)h(x)$ in $\mathbb{Q}(x)$
By Gauss lemma and some discuss, $f, h \in \mathbb{Z}[x]$
Let p be a prime s.t. $p \nmid n$ and **Claim:** $f(\zeta_n^p) = 0$
pf. Assume not, $h(\zeta_n^p) = 0$ and thus ζ_n is a root of $h(x^p) \rightsquigarrow f(x) | h(x^p)$, say $h(x^p) = f(x)g(x)$. In $\mathbb{F}_p[x]$, $\left(\overline{h}(x)\right)^p = \overline{h}(x^p) = \overline{f}(x)\overline{g}(x) \rightsquigarrow \overline{h}(x)$ and $\overline{f}(x)$ have common root in $\mathbb{F}_p$, which means $x^n - 1$ have multiple root a in $\mathbb{F}_p \rightsquigarrow a^n = 1$ and $na^{n-1} = 0 \rightsquigarrow p | n$ $(\to\leftarrow)$ □
Hence, $f(\zeta_n^p) = 0$. By induction, it is clear that $f(\zeta_n^{p_1^{\alpha_1} \cdots p_k^{\alpha_k}}) = 0$ for $p_i \nmid n$, which means $f(\zeta_n^m) = 1 \ \forall \gcd(m,n) = 1$.
Hence, $\varphi(n) \leq \deg m_{\zeta_n,\mathbb{Q}} \leq \varphi(n) \implies [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg m_{\zeta_n,\mathbb{Q}} = n$ □

Corollary 4.6.1. $\gcd(m,n)=1 \implies \mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n)=\mathbb{Q}$

Proof: Claim: $\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n)=\mathbb{Q}(\zeta_{mn})$

- $(\subseteq)$ $\begin{cases}\zeta_n^{mn}=1 & \rightsquigarrow \zeta_n=\zeta_{mn}^i\in\mathbb{Q}(\zeta_{mn})\\ \zeta_m^{mn}=1 & \rightsquigarrow \zeta_m=\zeta_{mn}^j\in\mathbb{Q}(\zeta_{mn})\end{cases}$
- $(\supseteq)$ $\begin{cases}\zeta_{mn}^n \text{ is a primitive } m\text{-th root of unity}\\ \zeta_{mn}^m \text{ is a primitive } n\text{-th root of unity}\end{cases}$

  $\exists a,b\in\mathbb{Z}$ s.t. $am+bn=1 \rightsquigarrow \zeta_{mn}=(\zeta_{mn}^m)^a\,\zeta_{mn}^n)^b\in\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n)$

$$\varphi(mn)=[\mathbb{Q}(\zeta_{mn}):\mathbb{Q}]=\frac{[\mathbb{Q}(\zeta_m):\mathbb{Q}][\mathbb{Q}(\zeta_n):\mathbb{Q}]}{[\mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n):\mathbb{Q}]}=\frac{\varphi(m)\varphi(n)}{[\mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n):\mathbb{Q}]}$$

Hence, $\mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n)=\mathbb{Q}$ □

Definition 4.6.2. $\Phi_n(x)=\prod_{\substack{1\le k<n\\ \gcd(k,n)=1}}(x-\zeta_n^k)$ is called n-th **cyclotomic polynomial** in $\mathbb{Z}[x]$

Property 4.6.3. $x^n-1=\prod_{d|n}\Phi_d(x)$

Proof: Both side have no multiple root, so it is suffices to show thet have same root and it is trivial. □

Definition 4.6.3 (**Legendre symbol**)**.** Let $\alpha\in\mathbb{Z}$, define

$$\left(\frac{\alpha}{p}\right)=\left(\frac{\overline{\alpha}}{p}\right)=\begin{cases}0 & \text{if } \alpha\equiv 0 \pmod p\\ 1 & \text{if } \alpha\equiv x^2 \pmod p \text{ for some } p\not| x\\ -1 & \text{if } \alpha\not\equiv x^2 \pmod p \text{ for all } x\end{cases}$$

Property 4.6.4.

$$\left(\frac{\alpha}{p}\right)=\alpha^{\frac{p-1}{2}}\ \forall\alpha\in\mathbb{F}_p^\times$$

Proof: $\forall\alpha\in\mathbb{F}_p^\times$, let $\beta\in\mathbb{F}_p^a$ s.t. $\beta^2=\alpha\rightsquigarrow(\beta^{p-1})^2=\alpha^{p-1}=1$. Thus,

$$\alpha^{\frac{p-1}{2}}=\beta^{p-1}=\begin{cases}1 & \text{if } \beta\in\mathbb{F}_p \iff \left(\frac{\alpha}{p}\right)=1\\ -1 & \text{if } \beta\notin\mathbb{F}_p \iff \left(\frac{\alpha}{p}\right)=-1\end{cases}$$

□

Corollary 4.6.2.

$$\left(\frac{\alpha}{p}\right)\left(\frac{\beta}{p}\right)=\left(\frac{\alpha\beta}{p}\right)$$

Theorem 4.6.2. Every quadratic extension of $\mathbb{Q}$ is contained in a cyclotomic extension

Proof: Let $L = \mathbb{Q}(a)$ with $m_{a,\mathbb{Q}} = x^2 + bx + c \rightsquigarrow a = \frac{-b \pm \sqrt{b^2-4c}}{2} \rightsquigarrow L = \mathbb{Q}(\sqrt{b^2-4ac}) \subseteq \mathbb{Q}(\sqrt{-1}, \sqrt{D})$, where D is square free with $|b^2 - 4ac| = x^2 D$

- $\sqrt{-1} \in \mathbb{Q}(\zeta_4), \sqrt{2} \in \mathbb{Q}(\zeta_8)$
- **Claim:** $\sqrt{p} \in \begin{cases} \mathbb{Q}(\zeta_p) & \text{if } p \equiv 1 \pmod 4 \\ \mathbb{Q}(\zeta_p, \sqrt{-1}) & \text{if } p \equiv 3 \pmod 4 \end{cases}$

  pf. Let

$$s = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \zeta_p^k \rightsquigarrow s^2 = \sum_{k=1}^{p-1} \sum_{\ell=1}^{p-1} \left(\frac{k\ell}{p}\right) \zeta_p^{k+\ell}$$

  For any $1 \le \ell < p$, $\left\{\overline{k\ell} | 1 \le k < p\right\} = \left\{\overline{k} | 1 \le k < p\right\}$, so

$$s^2 = \sum_{1 \le k.\ell < p} \left(\frac{(k\ell)\ell}{p}\right) \zeta_p^{k\ell+\ell} = \sum_{1 \le k,\ell < p} \left(\frac{k}{p}\right) \zeta_p^{(k+1)\ell} = \sum_{\ell=1}^{p-1} \left(\frac{-1}{p}\right) + \sum_{k=2}^{p-1} \left(\frac{k}{p}\right) \sum_{\ell=1}^{p-1} \zeta_p^{(k+1)\ell}$$
$$= (p-1)\left(\frac{-1}{p}\right) - \sum_{k=2}^{p-1} \left(\frac{k}{p}\right) = p\left(\frac{-1}{p}\right) - \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) = p\left(\frac{-1}{p}\right)$$

  Hence, $s = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \pmod 4 \\ \sqrt{-p} & \text{if } p \equiv 3 \pmod 4 \end{cases} \implies \sqrt{p} \in \begin{cases} \mathbb{Q}(\zeta_p) & \text{if } p \equiv 1 \pmod 4 \\ \mathbb{Q}(\zeta_p, \sqrt{-1}) & \text{if } p \equiv 3 \pmod 4 \end{cases}$ □

  Write $D = p_1 p_2 \cdots p_k$, then

$$L = \mathbb{Q}(\sqrt{D}, \sqrt{-1}) \subseteq \mathbb{Q}(\sqrt{p_1}) \cdots \mathbb{Q}(\sqrt{p_k}) \mathbb{Q}(\sqrt{-1})$$
$$\subseteq \mathbb{Q}(\zeta_{p_1}) \cdots \mathbb{Q}(\zeta_{p_k}) \mathbb{Q}(\zeta_8) \subseteq \mathbb{Q}(\zeta_{8 p_1 p_2 \cdots p_k})$$

□

Example 4.6.1.

- $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times \simeq C_{p-1}$
- For $H \le \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, we want to find $\mathbb{Q}(\zeta_p)^H$: Let $\alpha = \sum_{\sigma \in H} \sigma(\zeta_p)$

  $\forall \tau \in H, \tau(\alpha) = \sum_{\sigma \in H} \tau \circ \sigma(\zeta_p) = \sum_{\sigma \in H} \sigma(\zeta_p) = \alpha \implies \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\zeta_p)^H$

  Since $\{\zeta_p, ..., \zeta_p^{p-1}\}$ is linearly independent over $\mathbb{Q}$. If $\tau \notin H$ and fix α, that is

$$\sum_{\sigma \in H} \sigma(\zeta_p) = \sum_{\sigma \in H} \tau \circ \sigma(\zeta_p) = \tau(\zeta_p) + \cdots$$

  there exists $\sigma \in H$ s.t. $\sigma(\zeta_p) = \tau(\zeta_p) \implies \sigma^{-1}\tau(\zeta_p) = \zeta \implies \sigma^{-1}\tau = \mathrm{id}$

  Hence, $\tau = \sigma \in H$ $(\rightarrow\leftarrow)$ and thus $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}(\alpha)) = H \implies \mathbb{Q}(\zeta_p)^H = \mathbb{Q}(\alpha)$

4.7 Norm and trace

- Let $L = F(\alpha)$ with $f(x) = m_{\alpha,F}(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ being separable
  - $\exists$ exactly n monomorphism $\sigma_i : L \longrightarrow F^a$ fixing F and $\sigma_i(\alpha)$ consists of all roots of f
  - $f(x) = \prod_{i=1}^{n}(x - \sigma(\alpha_i)) \rightsquigarrow -a_{n-1} = \sum_{i=1}^{n}\sigma_i(\alpha), (-1)^n a_0 = \prod_{i=1}^{n}\sigma_i(\alpha)$
  - Consider the F-linear transformation $\begin{array}{rccc} T_\alpha : & F(\alpha) & \longrightarrow & F(\alpha) \\ & x & \longmapsto & \alpha x \end{array}$, then

$$[T_\alpha]_{\{1,\alpha,\ldots,\alpha^n\}} = \begin{pmatrix} 0 & 0 & 0 & \cdots & & 0 & -a_0 \\ 1 & 0 & 0 & & & 0 & -a_1 \\ 0 & 1 & 0 & & & 0 & -a_2 \\ \vdots & & & \ddots & & & \vdots \\ 0 & & & & 1 & 0 & -a_{n-1} \\ 0 & 0 & 0 & \cdots & 0 & 1 & -a_n \end{pmatrix} \rightsquigarrow \begin{cases} \mathrm{Tr}[T_\alpha] = -a_{n-1} \\ \det[T_\alpha] = (-1)^n a_0 \end{cases}$$

- f is inseparable ($F = p > 0$)

  $\rightsquigarrow f(x) = f_{sep}(x^{p^k})$ where f_{sep} is sep. and irr. of $\deg m$

  If $f_{\text{sep}} = (x-\beta_1)(x-\beta_2)\cdots(x-\beta_m)$, then $f(x) = (x^{p^k}-\beta_1)(x^{p^k}-\beta_2)\cdots(x^{p^k}-\beta_m)$ and let $\{\alpha_1, ..., \alpha_m\}$: the set of roots of $f \rightsquigarrow \beta_i = \alpha_i^{p^k} \rightsquigarrow f(x) = ((x-\alpha_1)\cdots(x-\alpha_m))^{p^k}$
  - $\beta_i = \alpha_i^{p^k}$ is sep. over F with $[F(\beta_i) : F] = m$ and α_i is **purely inseparable** (See Homework 18) over $F(\beta_i)$ with $[F(\alpha_i) : F(\beta_i)] = p^k \implies F(\alpha_i)/F((\beta_i)$: purely inseparable

$$\begin{array}{c} L = F(\alpha_i) \\ \uparrow{\scriptstyle purely\ insep.} \\ F(\beta_i) \subseteq L \\ \uparrow{\scriptstyle sep.} \\ F \end{array}$$

  - Define $L_{\text{sep}} = \{r \in L | r \text{ is sep}/F\}$ (it is clear that L_{sep} is a field)
    If $r \in F(\alpha_i) \setminus F(\beta_i)$ is sep$/F \rightsquigarrow r$ is sep$/F(\beta_i)$ $(\rightarrow\leftarrow) \implies L_{\text{sep}} = F(\beta_i)$
  - Define $[L : F]_s := m, [L : F]_i = p^k$

    $\exists$ exactly m monomorphisms $\sigma_i : L \to F^a$ fixing F and $f(x) = \prod_{i=1}^{m}(x - \sigma_i(\alpha))^{p^k}$

Proposition 4.7.1. If L/F is finite and purely inseparable, then $[L : F] = p^n$ for some $n \geq 0$ ($F = p$)

Proof: Let $L = F(\alpha_1, ..., \alpha_)$ $\rightsquigarrow \alpha_i$: purely insep$/F \rightsquigarrow \alpha_i$: purely insep$/F(\alpha_1, ..., \alpha_{i-1}) \rightsquigarrow$ $m_{\alpha_i, F(\alpha_1,\ldots,\alpha_{i-1})} = x^{p^{n_i}} - \alpha_i^{p^{n_i}} \rightsquigarrow [L : F] = p^{\sum n_i}$ □

Proposition 4.7.2. Let L/F be alg. and $L_{\text{sep}} = \{\alpha : \alpha \text{ is sep}/F\}$, then

$$L_{\text{sep}}/F \text{ is sep. and } L/L_{\text{sep}} \text{ is purely insep.}$$

Proof: $\forall \alpha \in L, m_{\alpha,F} = f_{\text{sep}}(x^{p^k}) \rightsquigarrow \alpha^{p^k}$ is sep$/F \rightsquigarrow \alpha^{p^k} \in L_{\text{sep}}$ □

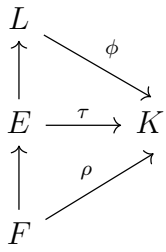
Definition 4.7.1. $[L : F]_{\text{sep}} = [L_{\text{sep}} : F]$ and $[L : F]_i = [L : L_{\text{sep}}]$
$(\rightsquigarrow [L : F]] = [L : F]_{\text{sep}}[L : F]_i)$

Proposition 4.7.3. Let $L \supseteq E \supseteq F$ and $[L : F] < \infty$, then

$$[L : F]_{\text{sep}} = [L : E]_{\text{sep}}[E : F]_{\text{sep}} \text{ and } [L : F]_i = [L : E]_i[E : F]_i$$

Proof: Let $K = F^a$ and ρ be a monomorphism $F \to K$

$$\begin{aligned}
[E : F]_{\text{sep}} &= \#\text{of distinct mono. } \tau : E \to K \text{ s.t. } \tau|_F = \rho \\
[L : E]_{\text{sep}} &= \#\text{of distinct mono. } \sigma : L \to K \text{ s.t. } \sigma|_F = \tau \\
[L : F]_{\text{sep}} &= \#\text{of distinct mono. } \phi : L \to K \text{ s.t. } \phi|_F = \rho
\end{aligned}$$



$$\implies [L : F]_{\text{sep}} = [L : E]_{\text{sep}}[E : F]_{\text{sep}}$$

□

Definition 4.7.2. Let $[L : F] < \infty$ and $\alpha \in L$. Let $\sigma_1, ...\alpha_m$ be the distinct mono. from L to F^a fixing F, where $m = [L : F]_{\text{sep}}$

$$N_F^L(\alpha) := \left(\prod_{i=1}^{m} \sigma_i(\alpha)\right)^{[L:F]_i} \text{ is the } \textbf{norm} \text{ of } \alpha$$

$$Tr_F^L(\alpha) := [L : F]_i \sum_{i=1}^{m} \sigma(\alpha) \text{is the } \textbf{trace} \text{ of } \alpha$$

Note: Let $\alpha \in L$ and $m_{\alpha,F} = x^n + a_{n-1}x^{n-1} + \cdots + a_0$

$$\begin{aligned}
N_F^L(\alpha) &= \left(\left(\prod_{i=1}^{m} \sigma_i(\alpha)\right)^{[F(\alpha):F]_i}\right)^{[L:F(\alpha)]_i} \\
&= \left(((-1)^n a_0)^{[L:F(\alpha)]_{\text{sep}}}\right)^{[L:F(\alpha)]_i} = ((-1)^n a_0)^{[L:F(\alpha)]} \in F \\
Tr_F^L(\alpha) &= [L : F(\alpha)](-a_{n-1}) \in F
\end{aligned}$$

Proposition 4.7.4. $L \supseteq E \supseteq F \implies N_F^L = N_F^E \circ N_E^L$ and $Tr_F^L = Tr_F^E \circ Tr_E^L$

Proof: Let $[E:F]_s = \ell$ and $[L:E]_s = t \implies [L:F]_s = \ell t$
Let $\{\tau_1, ..., \tau_\ell\}$ be distinct homo. from E to F^a fixing F
For fix i, let $\{\sigma_{i1}, ..., \sigma_{it}\}$ be distinct extend τ_i form L to F^a

$$\begin{array}{ccc} L & \xrightarrow[\sim]{\sigma_{ij}} & \sigma_{ij}(L) \\ \uparrow & & \uparrow \\ E & \xrightarrow[\sim]{\tau_i} & \tau_i(E) \end{array}$$

Consider $\tau_i : m_{\alpha,E} \mapsto m_{\alpha,E}^{\tau_i}$, we have

$$\left(\prod_{j=1}^{t} \sigma_{ij}(\alpha)\right)^{[L:E]_i} = ((-1)^n \tau_i(a_0))^{[L:E(\alpha)]}$$

$$\implies N_E^L(\alpha) = \tau_i^{-1}\left(\prod_{j=1}^{t} \sigma_{ij}(\alpha)\right)^{[L:E]_i}$$

Then composite τ_i :

$$N_F^E \circ N_E^L(\alpha) = \left(\prod_{i=1}^{\ell} \tau_i\left(N_F^L(\alpha)\right)\right)^{[E:F]_i} = \left(\prod_{i=1}^{\ell} \tau_i \tau_i^{-1}\left(\prod_{j=1}^{t} \sigma_{ij}(\alpha)\right)^{[L:E]_i}\right)^{[E:F]_i}$$

$$= \left(\prod_{i=1}^{\ell}\prod_{j=1}^{t} \sigma_{ij}(\alpha)\right)^{[L:F]_i} = N_F^L(\alpha)$$

Similarly, we have $Tr_F^L = Tr_F^E \circ Tr_E^L$ □

Theorem 4.7.1. L/F : finite, separable. Then

(1) $\mathrm{Tr} : L \to F$ us a non-zero linear functional

(2) the map $\begin{array}{ccc} L \times L & \longrightarrow & F \\ (x,y) & \longmapsto & Tr(xy) \end{array}$ is bilinear nondegenerate

(3) $\begin{array}{ccc} L & \longrightarrow & \hat{L} \\ x & \longmapsto & (\mathrm{Tr}_x : y \mapsto Tr(xy)) \end{array}$

Proof: It is clear that we only need to proof (1).
Assume $\sum_{i=1}^{m} \sigma_i(\alpha) = 0 \ \forall \alpha \in L$ with $m = [L:F]_s = [L:F]$
$\because \sigma_1 \neq \sigma_2 \therefore \exists \alpha_0 \in L$ s.t. $\sigma_1(\alpha_0) \neq \sigma_2(\alpha_0)$

$$\implies \begin{cases} \sum_{i=1}^{n} \sigma_i(\alpha_0\alpha) = 0 \ \forall \alpha \in L \\ \sum_{i=1}^{n} \sigma_1(\alpha_0)\sigma_i(\alpha) = 0 \ \forall \alpha \in L \end{cases} \implies \sum_{i=2}^{n} (\sigma_i(\alpha_0) - \sigma_1(\alpha_0))\sigma_i(\alpha) = 0 \ \forall \alpha \in L$$

Notice that $\sigma_2(\alpha_0) - \sigma_1(\alpha_0) \neq 0$, we can do this until getting

$$(\text{something not equal to } 0)\sigma_n(\alpha) = 0 \ \forall \alpha \in L$$

which implies $\sigma_n(\alpha) = 0 \ \forall \alpha \in L$ $(\rightarrow\leftarrow)$ □

Property 4.7.1. Let $L = F(\alpha)$ be sep/F and $f(x) = m_{\alpha,F}(x)$. Let

$$\frac{f(x)}{x-\alpha} = \beta_0 + \beta_1 x + \cdots + \beta_{n-1}x^{n-1} + x^n$$

with $\beta \in L$. Then the dual basis of $\{1, \alpha, ..., \alpha^{n-1}\}$ is

$$\left\{\frac{\beta_0}{f'(\alpha)}, \frac{\beta_1}{f'(\alpha)} ..., \frac{\beta_{n-1}}{f'(\alpha)}\right\}$$

Proof: Write $f(x) = (x-\alpha_1)\cdots(x-\alpha_n)$ with $\alpha_1 = \alpha$

Define $h_i(x) = \frac{f(x)}{x-\alpha_i} \rightsquigarrow h_i(\alpha_j) = \begin{cases} 0 & \text{if } i \neq j \\ f'(\alpha_i) & \text{if } i = j \end{cases}$

Observe that for $0 \leq r \leq n-1$, $\sum_{i=1}^{n} h_i(x)\frac{a_i^r}{f'(\alpha_i)} - x^r$ has root $\alpha_1, ..., \alpha_n$ and deg $\leq n-1$. So $\sum_{i=1}^{n} h_i(x)\frac{\alpha_i^r}{f'(\alpha_i)} = x^r \ \forall 1 \leq r \leq n-1$

Let $\sigma_1, ..., \sigma_n : L \to F^a$ fixing F

$\forall j, \ \sigma_j\left(h_i(x)\frac{\alpha_i^r}{h'(\alpha_i)}\right) = \sigma_j\left(\frac{f(x)}{x-\alpha_i}\frac{\alpha_i^r}{h'(\alpha_i)}\right) = \frac{f(x)}{x-\sigma_j(\alpha)}\frac{\sigma_j(\alpha_i)^r}{f'(\sigma_j(\alpha_i))}$

Hence, $\sum_{j=1}^{n} \sigma_j\left(h_i(x)\frac{\alpha_i^r}{f'(\alpha_i)}\right) = \sum_{i=1}^{n} h_i(x)\frac{\alpha_i^r}{f'(\alpha_i)} = x^r \rightsquigarrow Tr\left(h_i(x)\frac{\alpha_i^r}{f'(\alpha_i)}\right) = x^r$

$\implies Tr\left(\beta_i x^i \frac{\alpha^r}{f'(\alpha)}\right) = \delta_{ir}x^i \implies Tr\left(\frac{\beta_i}{f'(\alpha)}\alpha^j\right) = \delta_{ij}$ □

4.8 Cyclic extensions

Definition 4.8.1. L/F is **cyclic extension** if L/F is Galois and Gal(L/F) is cyclic

First, we recall the theorem in Homework 24.

Theorem 4.8.1. (Artin theorem) Let G be a monoid and K be a field. Let $\chi_1, \chi_2, ..., \chi_n$ be distinct multiplication group homo. $G \to K$. Then $\chi_1, ..., \chi_n$ are linearly independent over K. (We say χ_i is **characters** of G in K)

Key application: Let $\sigma_1, ..., \sigma_n$ be distinct in Aut(K) and $k_1, ..., k_n \in K^\times$. Then

$$\exists x \in K \text{ s.t. } k_1\sigma_1(c) + \cdots + k_n\sigma_n(c) \neq 0$$

Theorem 4.8.2. Assume that $F \not| n$. Let L be the splitting of $x^n - a$ ($\rightsquigarrow$ sep.) over F and ζ_n be a primitive n-th root of unity. Then Gal$(L/F(\zeta_n))$ is cyclic of order dividing n. Moreover,

$$x^n - a \text{ is irreducible over } F(\zeta_n) \iff [L : F(\zeta_n)] = n \text{ i.e. } |\operatorname{Gal}(L/F(\zeta_n))| = n$$

Proof: Let α be a root of $x^n - a \rightsquigarrow \alpha, \alpha\zeta_n, ..., \alpha\zeta_n^{n-1}$ are all roots of $x^n - a$ and thus $L = F(\alpha, \zeta_n) = F(\zeta_n)(\alpha)$. Consider

$$\begin{array}{rccc} \phi: & \mathrm{Gal}(L/F(\zeta_n)) & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ & \begin{pmatrix} \sigma_k: & L & \to & L \\ & \alpha & \mapsto & \alpha\zeta_n^k \end{pmatrix} & \longrightarrow & \overline{k} \end{array}$$

- homo, : $\sigma_{k_1} \circ \sigma_{k_2}(\alpha) = \sigma_{k_1}(\alpha\zeta_n^{k_1}) = \alpha\zeta_n^{k_1+k_2} = \sigma_{k_1+k_2}(\alpha)$
- ϕ is $1-1$: $\sigma_k \in \ker\phi \iff \overline{0} = \overline{k} \iff \sigma_k = \sigma_0 = \mathrm{id}$

$x^n - a$ is irr. in $F(\zeta_n)[x] \iff m_{\alpha, F(\zeta_n)} = x^n - a \iff [L : F(\zeta_n)] = n$ □

Theorem 4.8.3. Assume that $F \not| n$. If L/F is a cyclic extension of deg n with $\zeta := \zeta_n \in F$, then L is a splitting field of some irreducible polynomial $x^n - a$ over F

Proof: Let $\mathrm{Gal}(L/F) = \langle\sigma\rangle$ with $o(\sigma) = n$. For $1, \sigma, ..., \sigma^{n-1}$. $\exists c \in L$ s.t.

$$\alpha := c + \zeta\sigma(c) + \zeta^2\sigma^2(c) + \cdots + \zeta^{n-1}\sigma^{n-1}(c) \neq 0$$

Observe that $\sigma(\alpha) = \zeta^{-1}\alpha \implies \alpha \notin F$ and $\sigma(\alpha^n) = \zeta^{-n}\alpha^n \rightsquigarrow \alpha^n \in F$. So $F(\alpha) = F(\zeta)(\alpha) = F(\zeta, \alpha)$ is a splitting field of $x^n - a$ over F, where $a = \alpha^n$. Also,

$$\sigma|_{F(\alpha)}: \begin{array}{ccc} F(\alpha) & \longrightarrow & F(\alpha) \\ \alpha & \longmapsto & \alpha\zeta^{-1} \end{array} \implies \langle\sigma|_{F(\alpha)}\rangle \leq \mathrm{Gal}(F(\alpha)/F)$$

Hence, $n = [L : F] \geq [F(\alpha) : F] = |\mathrm{Gal}(F(\alpha)/F)| \geq n \implies L = F(\alpha)$

By Thm 4.8.2, $x^n - a$ is irr. over F. □

We can generalize Theorem 4.8.3 :

Theorem 4.8.4. (Hilbert theorem 90) Let L/F be cyclic and $\mathrm{Gal}(L/F) = \langle\sigma\rangle$ with $o(\sigma) = n$. Then

(1) $\forall\alpha \in L \setminus \{0\}$, $N_F^L(\alpha) = 1 \iff \alpha = \frac{\sigma(\beta)}{\beta}$ for some $\beta \in L \setminus \{0\}$

(2) $\forall\alpha \in L$, $Tr_F^L(\alpha) = 0 \iff \alpha = \sigma(\beta) - \beta$ for some $\beta \in L$

Proof: ($\Leftarrow$) is trivial. In below, we only prove ($\Longleftrightarrow$)

(1) By Artin theorem, there exists $c \in L$ s.t.

$$\beta^{-1} := c + \sigma(\alpha)\sigma(c) + (\sigma(\alpha)\sigma^2(\alpha))\sigma^2(c) + \cdots + (\sigma(\alpha)\sigma^2(\alpha)\cdots\sigma^{n-1}(\alpha))\sigma^{n-1}(c) \neq 0$$

Then multiply α and take σ in both side :

$$\sigma(\alpha)\sigma(\beta^{-1}) = \beta^{-1} + \sigma\left(\prod_{i=0}^{n-1}\sigma^i(\alpha)\right)\sigma^n(c) - c = \beta^{-1} + \sigma\left(N_F^L(\alpha)\right)c - c = \beta^{-1}$$

which means $\alpha = \frac{\sigma(\beta)}{\beta}$ for some $\beta \in L \setminus \{0\}$

(2) By Artin theorem, there exists $c \in L$ s.t.

$$\beta_1 = c + \sigma(c) + \cdots + \sigma^{n-1}(c) \neq 0 \implies \sigma(\beta_1) = \beta_1$$

$$\begin{aligned} \beta_2 &:= \alpha\sigma(c) + (\alpha + \sigma(\alpha))\sigma^2(c) + \cdots + (\alpha + \sigma(\alpha) + \cdots + \sigma^{n-2}(\alpha))\sigma^{n-1}(c) \\ \implies \beta_2 - \sigma(\beta_2) &= \alpha\sigma(c) + \alpha\sigma^2(c) + \cdots \alpha\sigma^{n-1}(c) - (Tr_F^L(\alpha) - \alpha)\sigma^n(c) = \alpha\beta_1 \\ \implies \alpha &= \frac{\beta_2}{\beta_1} - \sigma\left(\frac{\beta_2}{\beta_1}\right) = \sigma(\beta) - \beta \end{aligned}$$

where $\beta = -\beta_2\beta_1^{-1} \in L$

□

Corollary 4.8.1. Let $F\big|p$ and $[L : F] = p$. Then

$$L/F \text{ is cyclic} \iff L = F(\alpha) \text{ where } \alpha \text{ is a root of } x^p - x - a = 0$$

Proof:

- ($\Leftarrow$) Observe $\begin{cases} \alpha_1^p - \alpha - a = 0 \\ \alpha_2^p - \alpha_2 - a = 0 \end{cases} \implies (\alpha_1 - \alpha_2)^p = \alpha_1 - \alpha_2 \implies \alpha_1 - \alpha_2 \in \mathbb{F}_p$

  So all roots of $x^p - x - a$ is $\alpha, \alpha + 1, ..., \alpha + (p - 1)$

  Let $\sigma : \alpha \mapsto (\alpha + 1) \rightsquigarrow \sigma^k : \alpha \mapsto (\alpha + k)$. So $\mathrm{Gal}(L/F) = \langle\sigma\rangle$

  ($\Rightarrow$) Let $\mathrm{Gal}(L/F) = \langle\sigma\rangle$ with $o(\sigma) = p$

  $\because Tr_F^L(1) = p = 0 \therefore \exists\alpha \in L$ s.t. $1 = \sigma(\alpha) - \alpha \rightsquigarrow \sigma : \alpha \mapsto (\alpha + 1)$

  Notice that $\alpha \notin F$, $1 \neq [F(\alpha) : F]\big|[L : F] = p \rightsquigarrow [F(\alpha) : F] = p$ and $F(\alpha) = L$

  On one hand, $\sigma^i(\alpha) = \alpha + i$ is a roots of $m_{\alpha,F}(x)$ for all i.

  On the other hand, $\alpha, \alpha + 1, \alpha + 2, ..., \alpha + (p - 1)$ are roots of $x^p - x - a$, where $a = \alpha^p - \alpha \in F$ ($\because \sigma(\alpha^p - \alpha) = (\alpha + 1)^p - (\alpha + 1) = \alpha^p - \alpha$)

  Hence, $x^p - x - a | m_{\alpha,F} \rightsquigarrow m_{\alpha,F} = x^p - x - a$

□

Corollary 4.8.2. Another proof of Theorem 4.8.3.

Proof: Let $\mathrm{Gal}(L/F) = \langle\sigma\rangle$ with $o(\sigma) = n$

$\because \zeta_n \in F$ and $N_F^L(\zeta_n^n) = \zeta_n^n = 1 \therefore \exists\alpha \in L \setminus \{0\}$ s.t. $\zeta_n = \frac{\sigma(\alpha)}{\alpha} \rightsquigarrow \sigma(\alpha) = \alpha\zeta_n$

Then $\alpha, \alpha\zeta_n, ..., \alpha\zeta_n^{n-1}$ are roots of $m_{\alpha,F} \rightsquigarrow m_{\alpha,F} = x^n - a$, where $a = \alpha^n$ □

Example 4.8.1. $\zeta := \zeta_{17}$. Consider $\begin{array}{ccc} \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) & \longrightarrow & (\mathbb{Z}/17\mathbb{Z})^\times \simeq \mathbb{Z}/16\mathbb{Z} \\ (\sigma_k : \zeta \mapsto \zeta^k) & \longmapsto & \overline{k} \end{array}$

and notice that $o(\overline{3}) = 16$ in $(\mathbb{Z}/17\mathbb{Z})^\times \implies \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \langle\sigma_3\rangle$ and write $\sigma := \sigma_3$

All nontrivial proper subgroups of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ are $\langle\sigma^2\rangle, \langle\sigma^4\rangle, \langle\sigma^8\rangle$

- $\langle\sigma^2\rangle : \begin{cases}\alpha_1 := \zeta + \sigma^2(\zeta) + \cdots + \sigma^{14}(\zeta) = \zeta + \zeta^{3^2} + \cdots + \zeta^{3^{14}} \in \mathbb{Q}(\zeta)^{\langle\sigma^2\rangle} \\ \alpha_2 := \zeta^3 + \sigma^2(\zeta^3) + \cdots + \sigma^{14}(\zeta^3) = \zeta^3 + \zeta^{3^3} + \cdots + \zeta^{3^{15}} \in \mathbb{Q}(\zeta)^{\langle\sigma^2\rangle}\end{cases}$

  $\implies \alpha_1 + \alpha = 4 - 1, \alpha_1\alpha_2 = -4 \implies x^2 + x - 4 = 0 \implies \alpha_1, \alpha_2 = \frac{-1\pm\sqrt{17}}{2}$

  Hence, $\mathbb{Q}(\zeta)^{\langle\sigma^2\rangle} = \mathbb{Q}(\sqrt{17})$

- $\langle\sigma^4\rangle : \begin{cases}\beta_1 := \zeta + \zeta^{3^4} + \zeta^{3^8} + \zeta^{3^{12}} \in \mathbb{Q}(\zeta)^{\langle\sigma^4\rangle} \\ \beta_2 := \zeta^3 + \zeta^{3^5} + \zeta^{3^9} + \zeta^{3^{13}} \in \mathbb{Q}(\zeta)^{\langle\sigma^4\rangle} \\ \beta_3 := \zeta^{3^2} + \zeta^{3^6} + \zeta^{3^{10}} + \zeta^{3^{14}} \in \mathbb{Q}(\zeta)^{\langle\sigma^4\rangle} \\ \beta_4 := \zeta^{3^3} + \zeta^{3^7} + \zeta^{3^{11}} + \zeta^{3^{15}} \in \mathbb{Q}(\zeta)^{\langle\sigma^4\rangle}\end{cases} \implies \begin{cases}\beta_1 + \beta_3 = \alpha_1, \beta_1\beta_3 = -1 \\ \beta_2 + \beta_4 = \alpha_2, \beta_2\beta_4 = -1\end{cases}$

  Hence, $\mathbb{Q}(\zeta)^{\langle\sigma^4\rangle} = \mathbb{Q}\left(\sqrt{\frac{17-\sqrt{17}}{2}}\right)$

- $\langle\sigma^8\rangle : \gamma_i := \zeta^{3^{i-1}} + \zeta^{3^{i+7}}$ for $i = 1, 2, ..., 8 \implies \gamma_1 + \gamma_5 = \beta_1, \gamma_1\gamma_5 = \beta_2$

  Hence, $\mathbb{Q}(\zeta)^{\langle\sigma^8\rangle} = \mathbb{Q}(\gamma_1)$

$$\mathbb{Q}(\zeta) \xleftarrow{2} \mathbb{Q}(\gamma_1) \xleftarrow{2} \mathbb{Q}(\beta_1) \xleftarrow{2} \mathbb{Q}(\alpha_1) \xleftarrow{2} \mathbb{Q}$$

Since $\zeta = \cos\frac{2\pi}{17} + i\sin\frac{2\pi}{17} \rightsquigarrow \zeta^{3^8} = \zeta^{-1} = \cos\frac{2\pi}{17} - i\sin\frac{2\pi}{17} \implies \gamma_1 = 2\cos\frac{2\pi}{17}$
$[\mathbb{Q}(\gamma_1) : \mathbb{Q}] = 2^3$ is constructible$\rightsquigarrow$ The regular 17-gon is constructible

Definition 4.8.2. A real number r is **constructible** if we can construct line segment of length $|r|$ by using a rule and a compass.

Proposition 4.8.1.

$r \in \mathbb{R}$ is constructible $\iff \exists r_1, r_2, ..., r_{n+1} = r \in \mathbb{R}$ s.t. $\begin{cases}r_1 \in \mathbb{Q} \\ r_{i+1}^2 \in \mathbb{Q}(r_1, ..., r_i)\end{cases}$

pf. By brutally discuss.

4.9 Abelian extensions

In this section, Galois = separable + normal not require finite

Definition 4.9.1.

- A Galois extension L/F is of **exponent** m if $\forall\sigma \in \mathrm{Gal}(L/F),\ \sigma^m = \mathrm{id}$
- $F^{\times m} := \{a^m | a \in F^\times\}$
- $a \in F,\ a^{\frac{1}{m}},\ \sqrt[m]{a} := \alpha \in F^a$ if $\alpha^m = a$ (Note : α is not unique)
- $B \subseteq F^\times$ with $F^{\times m} \subseteq B$. Let $F_B = F(B^{\frac{1}{m}})$ = the smallest field in F^a containing $a^{\frac{1}{m}}\ \forall a \in B$

Theorem 4.9.1. Let $F = p$ and $p \not| m$. Assume $\zeta_m \in F$ and $\mu_m = \langle\zeta_m\rangle$. Then

- F_B/F is Galois, abelian of exponent m
- $$\begin{array}{rccc} \Phi: & \mathrm{Gal}(F_B/F)\times B & \longrightarrow & \mu_m \\ & (\sigma, a=\alpha^m) & \longmapsto & \frac{\sigma(\alpha)}{\alpha} \end{array}$$
  is a bi-group homomorphism
  - $\Phi(\sigma,a)=1\ \forall\sigma\in\mathrm{Gal}(F_B/F) \iff a\in F^{\times m}$
  - $\Phi(\sigma,a)=1\ \forall a\in B \iff \sigma$ is the identity
- F_B/F is finite $\iff (B:F^{\times m})<\infty$. In this case, $[F_B:F]=(B:F^{\times m})$

Proof:

- For $a\in B, x^m-a$ splits over F_B since $\alpha,\alpha\zeta_m,...,\alpha\zeta_m^{m-1}\in F_B \rightsquigarrow F_B$ is the splitting field of $\{x^m-a|a\in B\}$ and x^m-a are separable since $p\not| m \rightsquigarrow F_B/F$ is Galois
- Let $G=\mathrm{Gal}(F_B/F)$ and $\sigma,\tau\in G$. For $a\in B$ and $a^{\frac{1}{m}}=\alpha$,
$$\begin{cases}\sigma(\alpha)=\alpha\omega_\sigma \\ \tau(\alpha)=\alpha\omega_\tau\end{cases} \text{ with } \omega_\sigma,\omega_\tau\in\mu_m$$
Then $\tau(\sigma(\alpha))=\tau(\alpha\omega_\sigma)=\alpha\omega_\tau\omega_\sigma=\alpha\omega_\sigma\omega_\tau=\sigma(\tau(\alpha))\rightsquigarrow G$ is abelian
- $\sigma^m(\alpha)=\alpha\omega_\sigma^m=\alpha\rightsquigarrow\sigma^m=\mathrm{id}$ i.e. G is of exponent m.
- - Φ is well-defined : If $\alpha_1^m=\alpha_2^m=a\rightsquigarrow\alpha_1=\alpha_2\omega$ for some $\omega\in\mu_m$
$$\frac{\sigma(\alpha_1)}{\alpha_1}=\frac{\sigma(\alpha_2)\omega}{\alpha_2\omega}=\frac{\sigma(\alpha_2)}{\alpha_2}$$
  - $\Phi_\sigma; B\to\mu_m$ is gp.homo.: $\Phi_\sigma(a_1a_2)=\frac{\sigma(a_1a_2)}{a_1a_2}=\frac{\sigma(a_1)}{a_1}\frac{\sigma(a_2)}{a_2}=\Phi_\sigma(a_1)\Phi_\sigma(a_2)$
  - $\Phi_a: G\to\mu_m$ is gp.homo.:
    $\Phi_a(\sigma_1\sigma_2)=\frac{\sigma_1(\sigma_2(\alpha))}{\alpha}=\frac{\sigma((\alpha\omega_{\sigma_2})}{\alpha}=\omega_{\sigma_1}\omega_{\sigma_2}=\Phi_a(\sigma_1)\Phi_a(\sigma_2)$
  - $\langle\sigma,a\rangle=1\ \forall a\in B \iff \frac{\sigma(\alpha)}{\alpha}=1\ \forall\alpha\in B^{\frac{1}{m}} \iff \sigma=\mathrm{id}_{F_B}$
    $\langle\sigma,a\rangle=1\ \forall\sigma\in G \iff \frac{\sigma(\alpha)}{\alpha}=1\ \forall\sigma\in G \iff \alpha\in F^\times \iff a\in F^{\times m}$

    Hence, $G\times B/F^{\times m}\to\mu_m$ is a non-degenerate bi-group homo. form.
    If $|G|<\infty$, then $B/F^{\times m}\hookrightarrow\mathrm{Hom}(G,\mu_m)=G^\wedge$
    (**Def:** $\mathrm{Hom}(G_1,G_2)=\{f: G_1\to G_2 \text{ is homo.}\}$)
    and $|B/F^\times|\le|G^\wedge|=|G|$ (We will explain last equation later)
    Since $|B/F^\times|<\infty$, $G\hookrightarrow\mathrm{Hom}(B/F^\times,\mu_m)$ and $|G|\le|\,(B/F^\times)^\wedge\,|=|B/F^\times|$
    Hence, $[F_B:F]=|G|=|B/F^\times|=(B:F^\times)$ □

Property 4.9.1. Let G be a finite abelian group and K be algebraic closed with $K \not| |G|$ and define **dual group** with $G^\wedge := \mathrm{Hom}(G, K^\times)$.

$$\sigma, \tau : G \to K^\times \implies \sigma\tau : G \to K^\times \text{ with } x \mapsto \sigma(x)\tau(x)$$

Then $G \simeq G^\wedge$

Proof: If $G \simeq G_1 \times G_2$, then $\mathrm{Hom}(G, F^\times) \simeq \mathrm{Hom}(G_1, F^\times) \times \mathrm{Hom}(G_2, F^\times)$

By fundamental theorem of finite abelian group, we can assume that G is cyclic. Say $G = \langle a \rangle \simeq \mathbb{Z}/d\mathbb{Z}$, then $G^\wedge = \{\sigma : a \mapsto x \in K | x^d = 1\} \rightsquigarrow G^\wedge \simeq \langle \zeta_m \rangle \simeq G$ □

Theorem 4.9.2. If $F = p \not| m$ and $\zeta_m \in F$, then

$$\begin{array}{ccccc} \{\text{subgroups of } F^\times \text{ containing } F^{\times m}\} & \longleftrightarrow & \{\text{abelian extensions of } F \text{ of exponent } m\} \\ B & \overset{T}{\longmapsto} & F_B \end{array}$$

Proof:

- $B_1 \subset B_2 \rightsquigarrow F_{B_1} \subset F_{B_2}$
- $F_{B_1} \subset F_{B_2} \implies B_1 \subset B_2 : \forall b \in B_1, F(b^{\frac{1}{m}}) \subseteq F(B^{\frac{1}{m}}) \rightsquigarrow F(b^{\frac{1}{m}}) \subseteq F(a_1^{\frac{1}{m}}, ..., a_n^{\frac{1}{m}})$

  for some $a_1, ..., a_n \in B_2$. Let $\begin{cases} B_2' = \langle a_1, ..., a_n \rangle F^{\times m} \subseteq B_2 \\ B_3 = \langle b, a_1, ..., a_n \rangle F^{\times m} \end{cases}$

  $\because F(b^{\frac{1}{m}}) \subseteq F(B_2'^{\frac{1}{m}}) \therefore F(B_3^{\frac{1}{m}}) = F(B_2'^{\frac{1}{m}}) \implies F_{B_3} = F_{B_2'}$

  And $[F_{B_2'} : F], [F_{B_3} : F] < \infty \rightsquigarrow \begin{cases} [F_{B_2'} : F] = (B_2' : F^{\times m}) \\ [F_{B_3} : F] = (B_3 : F^{\times m}) \end{cases} \implies B_2' = B_3$

  i.e. $b \in B_2' \subseteq B_2$. Hence, T is $1-1$.
- Fact: Let L_1/F and L_2/F be finite Galois with $L_1 \cap L_2 = F$. Then

$$\begin{array}{cccc} \Phi : & \mathrm{Gal}(L_1L_2/F) & \simeq & \mathrm{Gal}(L_1/F) \times \mathrm{Gal}(L_2/F) \\ & \sigma & \mapsto & (\sigma|_{L_1}, \sigma|_{L_2}) \end{array}$$

  pf. Since L_1/F and L_2/F are normal, $\sigma|_(L_1) = L_1$ and $\sigma|_{L_2}(L_2) = L_2$.

  •• Φ is $1-1$: $\sigma|_{L_1} = \mathrm{id}_{L_1}, \sigma|_{L_2} = \mathrm{id}_{L_2} \rightsquigarrow \sigma = \mathrm{id}_{L_1L_2}$

  •• Φ is onto:

$$|\operatorname{Im}\Phi| = |\operatorname{Gal}(L_1L_2/F)| = [L_1L_2 : F] = \frac{[L_1 : F][L_2 : F]}{[L_1 \cap L_2 : F]} = [L_1 : F][L_2 : F]$$

  □
- T is onto : Let L be an abelian extension of F of exponent m. $\forall \alpha \in L \rightsquigarrow$ a splitting field L_α of $m_{\alpha,F}$ over F is a subfield of L ($\because L/F$ is normal) and $[L_\alpha : F] < \infty$

  $G := \mathrm{Gal}(L_\alpha/F) \simeq \mathrm{Gal}(L/F)/\mathrm{Gal}(L/L_\alpha)$ is finite abelian, then

  $G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_{\ell_\alpha}\mathbb{Z}$ with $d_i | m$ and $\mathbb{Z}/d_i\mathbb{Z} := G_i$

Let $L_{\alpha,i:} = L_\alpha^{G_1\times\cdots\times\{e\}\times\cdots\times G_{\ell_\alpha}}$ (replace i-th to $\{e\}$) $\rightsquigarrow L_{\alpha,i}/F$ is Galois and

$$\mathrm{Gal}(L_{\alpha,i}/F) \simeq G_1\times\cdots\times G_{\ell_\alpha}/(G_1\times\cdots\times G_{\ell_\alpha} \simeq G_i \simeq \mathbb{Z}/d_i\mathbb{Z}$$

By Thm 4.8.3, $L_{\alpha,i} = F(b_i^{\frac{1}{d_i}}) = F(a_i^{\frac{1}{m}})$, where $a_i = b_i^{\frac{m}{d_i}}$

And by Fact, $\alpha \in L_\alpha = L_{\alpha,1}L_{\alpha,2}\cdots L_{\alpha,\ell_\alpha} = F(a_1^{\frac{1}{m}}, a_2^{\frac{1}{m}}, ..., a_{\ell_\alpha}^{\frac{1}{m}})$

Hence, $\alpha \in L = F(a_{\alpha,i}^{\frac{1}{m}} : \alpha \in L, i = 1, ..., \ell_\alpha)$. Let $B = \langle a_{\alpha,i} : \alpha \in L, i = 1, ..., \ell_\alpha\rangle F^{\times m}$,

then $F_B = L$

□

Remark 4.9.1. If $m =$ $F = p$. Define $\begin{array}{rccc}\mathcal{P}: & F & \longrightarrow & F \\ & \alpha & \longmapsto & \alpha^p - \alpha\end{array}$, then

$$\mathcal{P}(\alpha_1+\alpha_2) = (\alpha_1+\alpha_2)^p - (\alpha_1+\alpha_2) = \alpha_1^p - \alpha_1 + \alpha_2^p - \alpha_2 = \mathcal{P}(\alpha_1) + \mathcal{P}(\alpha_2)$$

$\Longrightarrow$ $\mathcal{P}$ is additive homo. So $\mathcal{P}(F) \leq F$
Denoted $\mathcal{P}^{-1}(a)$ is one root of $x^p - x - a$ for $a \in F$ (Which is not unique)
If B is an additive subgroup of F containing $\mathcal{P}(F)$, then $F_B := F(P^{-1}(B))$.
By similarly idea, we have

$$\begin{array}{ccc} G\times B & \longrightarrow & \mathbb{Z}/p\mathbb{Z} \\ (\sigma, a = \mathcal{P}(\alpha)) & \longmapsto & \sigma(\alpha) - \alpha \end{array} \Longrightarrow G\times B/\mathcal{P}(F) \longrightarrow \mathbb{Z}/\partial\mathbb{Z}$$

$$\begin{array}{ccccc} \{\text{additive subgroup of } F \text{ containing } \mathcal{P}^{-1}(F)\} & \longleftrightarrow & \{\text{abelian extensions of } F \text{ of exponent } p\} \\ B & \overset{T}{\longmapsto} & F_B \end{array}$$

4.10 Solution by radicals

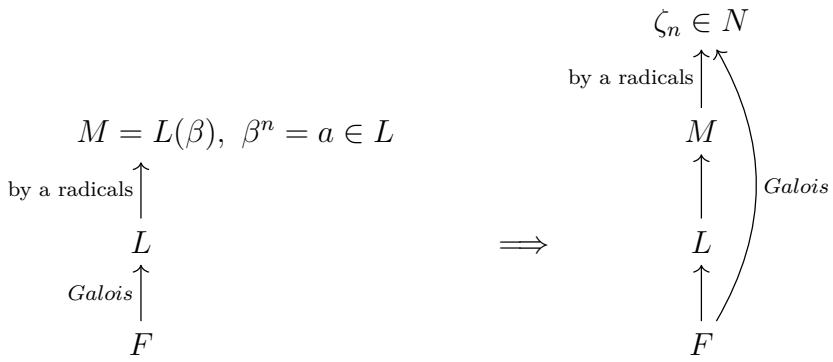
Definition 4.10.1.

- Given L/F and $\beta \in L$, β is called a **radical** over F if $a = \beta^n \in F$ for some $n > 0$ (or $\beta = a^{\frac{1}{n}}$)
- L/F is called an extension **by radical** if
  $\exists L = L_n \subset L_{n-1} \subset \cdots \subset L_0 = F$ s.t. $\forall i = 1, ..., n, L_i = L_{i-1}(\beta_i)$ and β_i is a radical over L_{i-1}
- $f(x) \in F[x]$ is **solvable by radicals** if $\exists L/F$ is an extension by radicals s.t. $f(x)$ is splits over L

We finally reached our final goal in this semester :

Theorem 4.10.1. (Main theorem) Under some assumption on F,
a separable polynomial $f(x) \in F[x]$ is solvable by radicals $\Longleftrightarrow$ $\mathrm{Gal}(f)$ is solvable

Lemma 4.10.1. Assume that $F \not| n$. Given left diagram, $\exists N$ satisfy right diagram.



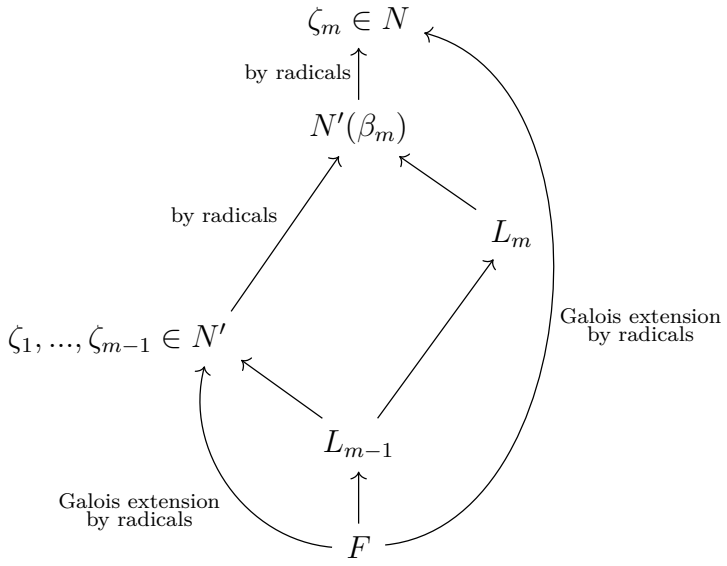
Proof: We know that $M(\zeta_n) = L(\zeta_n, \beta)$ is a splitting field of $x^n - a$ over L. If we set $f(x) = \prod_{\sigma \in \mathrm{Gal}(L/F)} (x^n - \sigma(a))$ and $\sigma(a) = \beta_\sigma$, then all coefficients are elementary symmetric poly. in $\{\sigma(a) | \sigma \in \mathrm{Gal}(L/F)\}$ which are fixed by $\mathrm{Gal}(L/F)$ and thus lie in F, i.e. $f(x) \in F[x]$.

Let L be a splitting field of $g(x)$ over F and N be a splitting field of $f(x)g(x)$ over F. So $N = M(\zeta_n, \beta_\sigma : \sigma \in \mathrm{Gal}(L/F))$ and N/F is Galois. □

Lemma 4.10.2. Let $L = L_m \subset L_{m-1} \subset \cdots \subset L_0 = F$ s.t. $L_i = L_{i-1}(\beta_i), \beta_i^{n_i} = a_i \in L_{i-1}$. If $F \not| n_1 n_2 \cdots n_m$, then $\exists N/L$ s.t. N/F is a Galois extension by radicals and $\zeta_{n_i} \in N\ \forall i = 1, ..., m$

Proof: By induction on m. $m = 1, L = F(\beta_1)$ with $\beta_1^{n_1} = a_1 \in F$. Set $N = L(\zeta_{n_1}) = F(\beta_1, \zeta_{n_1})$ which is a splitting field of $x^{n_1} - a_1$ over $F \rightsquigarrow N/F$ is Galois.

For $m > 1$, by induction hypothesis, $\exists N'/L_{m-1}$ s.t. N'/F is Galois extension by radicals and $\zeta_{n_i} \in N'\ \forall i = 1, ..., m-1$. By Lemma 4.10.1, $\exists N/N'(\beta_m)$ is an extension by radicals s.t. N/F is Galois and N contains ζ_m and N/F is extension by radicals.



□

Now, we will prove both directions of main theorem :

Theorem 4.10.2. Let $L = L_m \supset L_{m-1} \supset \cdots \supset L_0 = F$ s.t. $L_i = L_{i-1}(\beta_i), \beta_i^{n_i} = a_i \in L_{i-1}\ \forall i = 1, ..., m$ and $F \not| n_1 n_2 \cdots n_m$. If a separable polynomial $f(x) \in F[x]$ splits over F, then $\mathrm{Gal}(f)$ is solvable.

Proof: Set $n = \mathrm{lcm}(n_1, ..., n_m)$ and $\zeta := \zeta_n$. By Lemma 4.10.2, we can assume that L/F is a Galois extension by radicals and $\zeta \in L$.

Consider $L = L(\zeta) \supset L_{m-1}(\zeta) \supset \cdots \supset L_0(\zeta) = L_0 = F$ and define $L_0' = L_0, L_i' = L_{i-1}(\zeta)\ \forall i = 1, ..., (m+1)$ and $G_i = \mathrm{Gal}(L/L_i')\ \forall i$

- $G_0 = \mathrm{Gal}(L/F)$ is abelian and $G_{m+1} = \mathrm{Gal}(L/L) = \{e\}$
- $G_i/G_{i+1} = \mathrm{Gal}(L/L_i')/\mathrm{Gal}(L/L_{i+1}') \simeq \mathrm{Gal}(L_{i+1}/L_i)$ is cyclic $\forall i = 1, 2, ..., m$
  since $L_{i+1}' = L_i'(\beta_i)$ is a splitting field of $x^{n_i} - a_i$ over L_i'
  Hence, G_1 is solvable.
- $G_0/G_1 \simeq \mathrm{Gal}(L_1'/L_0') = \mathrm{Gal}(F(\zeta)/F) \hookrightarrow \mathbb{Z}/n\mathbb{Z}$
  $\implies G_0/G_1$ is cyclic and thus solvable $\implies G_0 = \mathrm{Gal}(L/F)$ is solvable

Let N be a splitting field of f over F. So $\mathrm{Gal}(N/F) \simeq \mathrm{Gal}(L/F)/\mathrm{Gal}(L/N)$ is solvable. □

Theorem 4.10.3. Let $f(x)$ be separable in $F[x]$ and L be a splitting field of f over F. Assume that $F \not| |\mathrm{Gal}(L/F)|$. If $\mathrm{Gal}(L/F)$ is solvable, then f is solvable by radicals.

Proof: Let $|\mathrm{Gal}(L/F)| = n, \zeta := \zeta_n$ and N be a splitting field of f over $F(\zeta)$, i.e. $N = LF(\zeta)$. Since $\mathrm{Gal}(LF(\zeta)/F(\zeta)) \simeq \mathrm{Gal}(L/L \cap F(\zeta)) \leq \mathrm{Gal}(L/F)$ and $\mathrm{Gal}(L/F)$ is solvable, we have $\mathrm{Gal}(LF(\zeta)/F(\zeta))$ is solvable. Say

$$\{e\} \lhd G_m \lhd G_{m-1} \lhd \cdots \lhd G_0 = \mathrm{Gal}(N/F(\zeta)) \text{ with } G_{i-1}/G_i : \text{cyclic}$$

If we set $N_i = N^{G_i}$, then $N = N_m \supset N_{m-1} \supset \cdots \supset N_0 = F(\zeta)$
and $G_i := \mathrm{Gal}(N/N_i) \rightsquigarrow G_{i-1}/G_i \simeq \mathrm{Gal}(N_i/N_{i-1})$. Thus N_i/N_{i-1} is cyclic extension. Notice that $n_j := [N_j : N_{j-1}] = \mathrm{Gal}(N_j/N_{j-1}) = \frac{|G_{j-1}|}{|G_j|} \big| |G_0| \big| n\ \forall j$

So $\begin{cases} \zeta \in N_{j-1} & \rightsquigarrow \zeta_{n_j} \in N_{j-1} \\ F \not| n & \rightsquigarrow F \not| n_i \end{cases} \implies N_j = N_{j-1}(\beta_i)$ with $\beta_i^{n_i} \in N_{i-1}$
$\implies N/F(\zeta)$ is an extension by radicals
$\implies N/F$ is an extension by radicals □

Property 4.10.1. Let G be a transitive subgroup of S_p. Then

(1) $p \big| |G|$

pf. Define $G_1 = \{\sigma \in G | \sigma(1) = 1\}$. $\because G$ is transitive $\therefore \exists \sigma_i \in G$ s.t. $\sigma_i(1) = i$ and $\forall \sigma \in G$, if $\sigma(1) = k \rightsquigarrow \sigma_k^{-1}\sigma(1) = 1 \rightsquigarrow \sigma_k^{-1}\sigma \in G_1 \rightsquigarrow \sigma \in \sigma_k G_1$

That is $G = \bigcup_{i=1}^{p} \sigma_i G_1 \rightsquigarrow p = (G : G_1) \big| |G|$ □

(2) If $\{e\} \neq H \lhd G$, then H is also transitive

pf. Define $i \sim j \iff \exists \sigma \in H$ s.t. $\sigma(i) = j$ and it is easy to check " $\sim$ " is an equivalence relation. Also, $\forall i, j\ \exists \sigma \in G$ s.t. $\sigma(i) = j$, then define $\begin{matrix}[i] & \longrightarrow & [j] \\ k & \longmapsto & \sigma(k)\end{matrix}$

Well define: If $k \in [i] \rightsquigarrow \exists \tau \in H$ s.t. $\tau(i) = k \rightsquigarrow \underline{\sigma\tau\sigma^{-1}}_{\in H}(j) = \sigma(k)$

So we have $\big|[i]\big| \leq \big|[j]\big|$. By symmetric, $\big|[j]\big| \leq \big|[i]\big| \implies \big|[i]\big| = \big|[j]\big|$

$\implies p = \sum \big|[i]\big| \rightsquigarrow \big|[i]\big| = 1$ or p

Since $H \neq \{e\} \implies |[i]| \neq 1 \rightsquigarrow |[i]| = p \rightsquigarrow H$ is transitive. □

4.11 Galois resolvent

In this section, we assume that $f(x)$ be separable in $F[x]$ and $L = F(\alpha_1, ..., \alpha_n)$ be a splitting field of $f(x)$ over F, where α_i are all roots of f
And our goal is find the Galois group: $\mathrm{Gal}(L/F)$

Definition 4.11.1. Let $\theta := y_1\alpha_1 + \cdots + y_n\alpha_n$, $\forall \sigma \in S_n$, define

$$\begin{cases}\sigma_y(\theta) = y_{\sigma(1)}\alpha_1 + \cdots + y_{\sigma(n)}\alpha_n \\ \sigma_\alpha(\theta) = y_1\alpha_{\sigma(1)} + \cdots + y_n\alpha_{\sigma(n)}\end{cases}$$

$\implies \sigma_y \circ \sigma_\alpha(\theta) = \sigma_\alpha \circ \sigma_y(\theta) = \theta \implies \sigma_\alpha = (\sigma_y)^{-1} = \sigma_y^{-1}$ and $\sigma_y = (\sigma_\alpha)^{-1} = \sigma_\alpha^{-1}$
In $L(x, y_1, ..., y_n)$, define the **Galois resolvent** is (write $y = \{y_1, ..., y_n\}$)

$$G(x, y) = \prod_{\sigma \in S_n} (x - \sigma_y(\theta)) = \prod_{\sigma \in S_n} (x - \sigma_\alpha^{=1}(\theta)) = \prod_{\sigma \in S_n} (x - \sigma_\alpha(\theta))$$

Now, we can do some basic discussions on Galois resolvent :

Each coefficient of G is a symmetric polynomial of $\alpha_1, ..., \alpha_n$, so it can be expressed in terms of the coefficient of $f(x)$ (by Corollary 4.4.1) and thus $G(x, y) \in F[x, y_1, ..., y_n]$. By Gauss lemma, $F[x, y_1, ..., y_n]$ is UFD.

We can decompose $G(x, y)$ into irr. factors in $F[x, y_1, ..., y_n]$

$$G(x, y) = P_1(x, y)P_2(x, y) \cdots P_r(x, y)$$

Note : $\forall \sigma \in S_n,\ G = \sigma_y G = (\sigma_y P_1)(\sigma_y P_2) \cdots (\sigma_y P_r)$ and P_i : irr. $\implies \sigma_y P_i$: irr, so σ induce a permutation of $P_1, P_2, ..., P_r$. We may assume $(x - \theta)|P_1$

Property 4.11.1.

$$G := \{\sigma \in S_n : \sigma_y P_1 = P_1\} = \{\sigma \in S_n : (x - \sigma_y(\theta)) = \sigma_y(x - \theta)|P_1\}$$

Proof:
$(\subseteq)\ x - \theta|P_1 \implies \sigma_y(x - \theta)|\sigma_y P_1 = P_1 \supseteq \sigma_y(x - \theta)|\sigma_y P_1, P_1 \rightsquigarrow \sigma_y P_1 = P_1$ □

Property 4.11.2. $\mathrm{Gal}(L/F) = G$

Proof: ($\subseteq$) For $\sigma \in \mathrm{Gal}(L/F) \hookrightarrow S_n$, we extend σ to an automorphism

$$\begin{array}{rccc} \widetilde{\sigma}: & L(y_1,...,y_n) & \longrightarrow & L(y_1,...,y_n) \\ & y_i & \longmapsto & y_i \\ & \alpha_i & \longmapsto & \alpha_{\sigma(i)} \end{array}$$

which fixes $F(y_1,...,y_n)$

$\because \widetilde{\sigma}(\theta) = \sigma_\alpha(\theta)$ and θ share the same minimal polynomial over $F(y_1,...,y_n)$ and by Gauss lemma, P_1 : irr. over $F[y_1,...,y_n][x] \rightsquigarrow P_1$: irr. over $F(y_1,...,y_n)[x]$

$\therefore P_1 = m_{\theta,F(y_1,...,y_n)} = m_{\sigma_\alpha(\theta),F(y_1,...,y_n)} \rightsquigarrow x - \sigma_y^{-1}(\theta) = x - \sigma_\alpha(\theta) | P_1$

$\rightsquigarrow \sigma^{-1} \in G$ i.e. $\sigma_y^{-1} P_1 = P_1 \implies P_1 = \sigma_y P_1 \rightsquigarrow \sigma \in G$

($\supseteq$) $\forall \sigma \in G$, $P_1 = m_{\theta,F(y_1,...,y_n)} = m_{\sigma_y(\theta),F(y_1,...,y_n)}$, so

$\exists\ \widetilde{\sigma} \in \mathrm{Aut}(L(y_1,...,y_n)/F(y_1,...,y_n))$ s.t. $\widetilde{\sigma}(\theta) = \sigma_y(\theta) = \sigma_\alpha^{-1}(\theta)$

$\widetilde{\sigma}|_L \in \mathrm{Gal}(L/F)$ and $\widetilde{\sigma}(\alpha_i) = \alpha_{\sigma^{-1}(i)} \rightsquigarrow \sigma^{-1} \in \mathrm{Gal}(L/F) \rightsquigarrow \sigma \in \mathrm{Gal}(L/F)$ □

Remark 4.11.1. $\{\sigma \in S_n | \sigma_y(P_i) = P_i\} \simeq \mathrm{Gal}(L/F)$

Proof: If $\sigma_y'(P_1) = P_i$, then we replace θ by $\theta' = \sigma_y'(\theta)$

So $\deg P_1 = \deg P_2 = \cdots = \deg P_r = |\mathrm{Gal}(L/F)|$ □

Theorem 4.11.1. (Main theorem) Given $f(x)$ monic separable in $\mathbb{Z}[x]$, assume that $p \nmid$ the discriminant D of $f(x)$. Then the Galois group of $\overline{f}(x)$ in $\mathbb{Z}/p\mathbb{Z}[x]$ is a subgroup of the Galois group of $f(x)$.

Note:

- Every finite extension of $\mathbb{Z}/p\mathbb{Z}$ is cyclic
- If $\overline{f}(x)$ is irr. in $\mathbb{Z}/p\mathbb{Z}[x]$ and into Galois group is $\langle\sigma\rangle \subseteq S_n$, then σ must be a cycle of length n. (irreducible $\implies$ transitive)
- If $\overline{f}(x) = \overline{f_1}(x)\overline{f_2}(x)\cdots\overline{f_r}(x)$ in $\mathbb{Z}/p\mathbb{Z}[x]$ with $\overline{f_i}$: irreducible of $\deg \overline{f_i} = m_i$, then $\mathrm{Gal}(f)$ contains a permutation of type $(\alpha_{11}\cdots\alpha_{1m_1})\cdots(\alpha_{r1}\cdots\alpha_{rm_r})$

Proof: By using resultant (we will see it later), the discriminant of $\overline{f}(x)$ is $\overline{D}$ and $p \nmid D \rightsquigarrow \overline{D} \neq \overline{0}$ in $\mathbb{Z}/p\mathbb{Z}$, so $\overline{f}(x)$ is separable.

As above, write $G(x,y) = P_1(x,y)P_2(x,y)\cdots P_r(x,y)$ in $\mathbb{Z}[x,y_1,...,y_n]$

Observe that if $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ has roots $\alpha_1, \alpha_2, ..., \alpha_n$ then $\overline{f}(x) = x^n + \overline{a_{n-1}}x^{n-1} + \cdots + \overline{a_0}$ has roots $\beta_1, \beta_2, ..., \beta_n$ with $s_i(\beta_1,..,\beta_n) = \overline{s_i(\alpha_1,...,\alpha_n)}$ in $\mathbb{Z}/p\mathbb{Z}$ for $i = 1,...,n$. Let $\theta_p = y_1\beta_1 + \cdots y_n\beta_n$ and

$$G_p(x,y) := \prod_{\sigma \in S_n} (x - \sigma_y(\theta_p)) = \overline{G}(x,y)$$

In $\mathbb{Z}/p\mathbb{Z}[x,y_1,...,y_n]$, $G_p = \overline{G} = \overline{P_1}\cdots\overline{P_r} = (P_{11}\cdots P_{1s_1})\cdots(P_{r1}\cdots P_{rs_r})$ with P_{ij} irr. in $\mathbb{Z}/p\mathbb{Z}[x,y_1,...,y_n]$. So we have

$$\begin{aligned} \mathrm{Gal}(\overline{f}) &= \{\sigma \in S_n | \sigma_y P_{11} = P_{11}\} \subseteq \{\sigma \in S_n | \sigma_y \overline{P_1} = \overline{P_1}\} \\ &= \{\sigma \in S_n | \sigma_y P_1 = P_1\} = \mathrm{Gal}(f) \end{aligned}$$

(Since we only change on $y_1,...,y_n$) □

Definition 4.11.2 (resultant)**.** Let R be an commutative ring and $f(x) = \sum_{i=0}^{n} a_i x^i, g(x) = \sum_{i=0}^{m} b_i x^i \in R[x]$. We define the **resultant** of f and g be the determinant of

$$R(f,g) := \begin{vmatrix} a_n & a_{n-1} & a_{n-2} & \cdots & a_0 & & \\ & a_n & a_{n-1} & \cdots & a_1 & a_0 & \\ & & \ddots & & & & \ddots \\ & & & a_n & & & a_0 \\ b_m & b_{m-1} & b_{m-2} & \cdots & b_0 & & \\ & b_m & b_{m-1} & \cdots & b_1 & b_0 & \\ & & \ddots & & & & \ddots \\ & & & b_m & & & b_0 \end{vmatrix}$$

which have m times of $(a_n \cdots a_0)$ and n times of $(b_m \cdots b_0)$

Theorem 4.11.2. Let $\begin{cases} f(x) = a_n \prod_{i=1}^{n} (x - y_i) = \sum_{i=0}^{n} a_i x^i \\ g(x) = b_m \prod_{i=1}^{m} (x - z_i) = \sum_{i=0}^{m} b_i x^i \end{cases} \in R[y_1, ..., y_n, z_1, ..., z_m][x]$

where y_i, z_j are variables and $a_n, b_m \in R$, then

$$R(f,g) = a_n^m b_m^n \prod_{i,j} (y_i - z_j) = a_n^m \prod_i g(y_i) = (-1)^{mn} b_m^n \prod_j f(z_j)$$

Proof: We only need to prove the first equation.

- $R(f,g)$ is a homogeneous polynomial of $\deg mn$ in $R[y_1, ..., y_n, z_1, ..., z_m]$:

  Notice that $a_i = (-1)^{n-i} s_{n-i}(y_1, ..., y_n)$ is symmetric polynomial with $\deg(n-1)$ in $F[y_1, ..., y_n, z_1, ..., z_m]$, also b_i is.

  Times y_1^i in i-th row for $1 \le i \le m$ and y_1^j in $(m+j)$-th row for $1 \le j \le n$, then we will get a determinant with $i-$th column is homogeneous polynomial of $\deg i$, then $y_1^{\frac{m(m+1)+n(n+1)}{2}} R(f,g)$ is a homogenous polynomial of degree $\frac{(m+n)(m+n+1)}{2}$. So $R(f,g)$ is a homogeneous polynomial of degree $\frac{(m+n)(m+n+1)-m(m+1)-n(n+1)}{2} = mn$

- $g(y_i)|R(f,g)\ \forall i$: If $x|g(x)$, we can expand the determinant on last column and using induction, so we can assume that $x \not| g(x)$

  First, we times y_i^{m+n} on 1-th column. Second, add $y_i^{m+n+1-k}$ times of k-th column to 1-th column, then we will get

$$y_i^{m+n} R(f,g) = \begin{vmatrix} y_i^m f(y_i) = 0 & \text{somethings} \\ y_i^{m-1} f(y_i) = 0 & \text{somethings} \\ \vdots & \text{somethings} \\ y_i f(y_i) = 0 & \text{somethings} \\ y_i^n g(y_i) & \text{somethings} \\ y_i^{n-1} g(y_i) & \text{somethings} \\ \vdots & \text{somethings} \\ y_i g(y_i) & \text{somethings} \end{vmatrix} \begin{matrix} \\ \\ \\ \\ \implies g_i(y_i) | y_i^{m+n} R(f,g) \\ \implies g(y_i) | R(f,g) \\ \\ \\ \\ \end{matrix}$$

- $\prod_{i,j}(y_i - z_j)\big|R(f,g)$: Since $\prod_j (y_i - z_j)\big|R(f,g)\ \forall i$ and $\prod_j (y_{i_1} - z_j), \prod_j (y_{i_2} - z_j)$ has no common divisor for distinct i_1, i_2, $\implies \prod_{i,j}(y_{i_1} - z_j)\big|R(f,g)$ and degree in both are all mn, so $R(f,g) = c\prod_{i,j}(y_i - z_j)$ for some constant $c \in R$

- $c = a_n^m b_m^n$: When we take $y_1 = \cdots = y_n = 0$ and $z_1 = \cdots = z_m = 1$, then $a_0 = a_1 = \cdots = a_{n-1} = 0$ and $b_0 = (-1)^m b_m$. Then LHS$= a_n^m b_0^n = (-1)^{mn} a_n^m b_m^n$ and RHS$= (-1)^{mn} c \rightsquigarrow c = a_n^m b_m^n$

□

Corollary 4.11.1. $R(f,f') = (-1)^{\frac{n(n-1)}{2}} a_n^{2n-1} D$
$(\rightsquigarrow R(\overline{f}, \overline{f'}) = (-1)^{\frac{n(n-1)}{2}} \overline{a_n}^{2n-1} \overline{D} = \overline{R(f,f')})$

Proof: $R(f,f') = a_n^{n-1} \prod_{i=1}^{n} f'(\alpha_i) = a_n^{n-1} \prod_{i=1}^n a_n \prod_{j\neq i}(\alpha_i - \alpha_j) = a_n^{2n-1}(-1)^{\frac{n(n--1)}{2}} D$

□

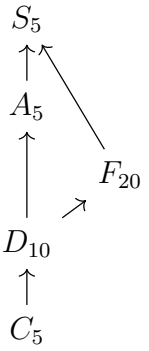
4.12 Applications 2

4.12.1 Quintic polynomials

We have already know how to classify the Galois group of Cubic polynomials and Quartic polynomials. In this subsection, we will discuss Galois group of Quintic polynomials.

- all transitive subgroup of S_5

cycle type	1	2	$2-2$	3	$2-3$	4	5
C_5	1						4
D_{10}	1		5				4
F_{20}	1		5			10	4
A_5	1		5	20			24
S_5	1	10	15	20	20	30	24



- transitive solvable subgroups of $S_5 : C_5, D_{10}, F_{20}$

  Since $(F_{20} : D_{10}) = (D_{10} : C_5) = 2 \rightsquigarrow \{e\} \lhd C_5 \lhd D_{10} \lhd F_{20}$ and factors are all cyclic. Thus, C_5, D_{10}, F_{20} are all transitive and solvable.

- transitive solvable subgroups of S_p :

  •• If G is transitive solvable subgroup of S_p, by Property 2.10.1, $p\big||G|$.
  By homework 27, $G \leq N(P)$ for some $P \in \mathrm{Syl}_p(S_P)$

Now, we give another method.

- Let G be a transitive subgroup of S_p and $\{e\} = G_n \lhd G_{n-1} \lhd \cdots \lhd G_0 = G$ with G_i/G_{i+1} : cyclic. By Property 2.10.1, $G_0, G_1, ..., G_{n-1}$ are all transitive and order are divided by p. So $G_{n-1} = \langle \sigma = (12\cdots p) \rangle$
  Affine transformation on $\mathbb{Z}/p\mathbb{Z}$, we get $\sigma \mapsto \begin{pmatrix} \mathbb{Z}/p\mathbb{Z} & \longrightarrow & \mathbb{Z}/p\mathbb{Z} \\ i & \longmapsto & i+1 \end{pmatrix}$ and define $\tau_{(a,b)}(k) = ak + b, F := \left(\{\tau_{(a,b)} : a \in (\mathbb{Z}/p\mathbb{Z})^\times,\ b \in \mathbb{Z}/p\mathbb{Z}\}, \circ\right) \rightsquigarrow |F| = p(p-1)$
  Construct $\Phi : \begin{matrix} F & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^\times \\ \tau_{(a,b)} & \longmapsto & a \end{matrix} \rightsquigarrow \ker\Phi = \{\tau_{(1,b)} | b \in \mathbb{Z}/p\mathbb{Z}\} = G_{n-1} \lhd F$
  and $F/G_{n-1} \simeq (\mathbb{Z}/p\mathbb{Z})^\times$: cyclic $\implies$ F is solvable
  Claim: Suppose $G_j F$, then $G_{j-1} \leq F$
  pf. $\forall \tau \in G_{j-1}, \tau\sigma\tau^{-1} \in G_{j-1} \leq F \rightsquigarrow \tau\sigma\tau^{-1} = \tau_{(a,b)}$ for some a, b. Since $\tau\sigma\tau^{-1}$ is p-cycle, which means $ax + b = \tau\sigma\tau^{-1}(x) = x$ has no solution in $\mathbb{Z}/p\mathbb{Z}$
  $\implies$ $a = 1$ and $b \neq 0 \rightsquigarrow \tau\sigma\tau^{-1} = \tau_{(1,b)} \implies \tau(k+1) = \tau(k) + b$
  $\implies$ $\tau(k) = bk + \tau(0) \implies \tau \in F$ □
  And thus $G \leq F$ (Note : $F = N(\langle\sigma\rangle)$)

- Example
  - $f(x) = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1 = m_{\zeta_{11}+\zeta_{11}^{-1},\mathbb{Q}}(x) \rightsquigarrow \mathrm{Gal}(f) = C_5$
  - $f(x) = x^5 - 2 \rightsquigarrow L = \mathbb{Q}(\zeta_5, \sqrt[5]{2}) \rightsquigarrow [L : \mathbb{Q}] = 20 \rightsquigarrow \mathrm{Gal}(f) \simeq F_{20}$
  - $f(x) = x^5 - 4x + 2$ has exactly 3 real roots and by Eisenstein's criterion f is irreducible over $\mathbb{Q} \rightsquigarrow \mathrm{Gal}(f) \simeq S_5$
  - $f(x) = x^5 + 20x + 16 : R(f, f') = 2^{16}5^6 \rightsquigarrow D = 2^{16}5^6 \rightsquigarrow \sqrt{D} \in \mathbb{Q}$
    $\implies$ $\mathrm{Gal}(f) \leq A_5$.
    - If f is not irr. over $\mathbb{Q}$, then $\overline{f}$ is not irr. over $\mathbb{Z}/3\mathbb{Z}$ and it is clear that $\overline{f}(x) = x^5 + 2x + 1$ has no root in $\mathbb{Z}/3\mathbb{Z} \rightsquigarrow \overline{f}(x) = (\deg 3)(\deg 2)$ in $\mathbb{Z}/3\mathbb{Z}[x]$
      $\implies$ $(a_1a_2a_3)(a_4a_5) \in \mathrm{Gal}(f)$ $(\rightarrow\leftarrow)$
    - In $\mathbb{Z}/7\mathbb{Z}$, $x^5 + 6x + 2 = (x^3 + 2x^2 + 5x + 5)(x - 4)(x - 5)$
      $\implies$ $(a_1a_2a_3) \in \mathrm{Gal}(f) \rightsquigarrow \mathrm{Gal}(f) \simeq A_5$
  - $f(x) = x^5 - 5x + 12 \rightsquigarrow D = 2^{12}5^6 \rightsquigarrow \sqrt{D} \in \mathbb{Q} \rightsquigarrow \mathrm{Gal}(f) \leq A_5$
    - In $\mathbb{Z}/3\mathbb{Z}$, $x^5 + x = x(x^2 + x + 2)(x^2 + 2x + 2) \rightsquigarrow (a_1a_2)(a_3a_4) \in \mathrm{Gal}(f)$
      $\rightsquigarrow \mathrm{Gal}(f) \simeq D_{10}$ or A_5
    - $f(x+3) = x^5 + 15x^4 + 90x^3 + 270x^2 + 400x + 240$, by Eisenstein's criterion, $f(x+3)$ is irr. over $\mathbb{Q}$ and thus f is also. f : sep.$\rightsquigarrow$ f has no multiple roots.
    - Let $\alpha_1, \alpha_2, ..., \alpha_5$ be the roots of $f(x)$
      Claim: If $\mathrm{Gal}(f) \geq D_{10}$, then $\alpha_i + \alpha_j$ $(1 \leq i < j \leq 5)$ are distinct.
      pf. Assume that $\mathrm{Gal}(f) = \langle \sigma = (12345), \tau = (23)(45) \rangle$ and claim is not hold, write $\alpha_{i_1} + \alpha_{i_2} = \alpha_{i_3} + \alpha_{i_4} \rightsquigarrow \alpha_{i_1+k} + \alpha_{i_2+k} = \alpha_{i_3+k} + \alpha_{i_4+k}$ $\forall k$
      So we only need to consider there cases : $\begin{cases} \alpha_1 + \alpha_2 = \alpha_3 + \alpha_4 \\ \alpha_1 + \alpha_3 = \alpha_2 + \alpha_4 \\ \alpha_1 + \alpha_2 = \alpha_3 + \alpha_5 \end{cases}$

Case1. $\alpha_1+\alpha_2=\alpha_3+\alpha_4=\sigma^2(\alpha_1+\alpha_2)=\alpha_5+\alpha_1 \rightsquigarrow \alpha_2=\alpha_5$ $(\rightarrow\leftarrow)$
Case2. $\alpha_1+\alpha_3=\alpha_2+\alpha_4=\sigma(\alpha_1+\alpha_3)=\alpha_3+\alpha_5 \rightsquigarrow \alpha_1=\alpha_5$ $(\rightarrow\leftarrow)$
Case3. $\alpha_1+\alpha_3=\tau(\alpha_1+\alpha_2)=\tau(\alpha_3+\alpha_5)=\alpha_2+\alpha_4$ back to Case.2 $(\rightarrow\leftarrow)$ □
$g(x):=\prod_{1\le i<j\le 5}(x-(\alpha_i+\alpha_j))\in\mathbb{Q}[x]$
$g(x)$ splits over $\mathbb{Q}(\alpha_i+\alpha_j:1\le i<j\le 5)=\mathbb{Q}(\alpha_i:1\le i\le 5)=L$
If $\mathrm{Gal}(f)\simeq A_5$, then $\mathrm{Gal}(f)$ acts transitively on the roots of $g \rightsquigarrow g$ is irr. over $\mathbb{Q}$. However, $g(x)=x^{10}+15x^6+132x^5-100x^2+240x-144=(x^5-5x^3+10x^2+30x+36)(x^5+5x^3-10x^2+10x-4)$ is reducible over $\mathbb{Q}$ $(\rightarrow\leftarrow)$ Hence, $\mathrm{Gal}(f)\simeq D_{10}$

4.12.2 Construct polynomials with Galois group is S_n

Although by Ruffni-Abel theorem, we know most of Galois group of polynomial with degree $=n\ge 5$ is S_n, we still construct infinite number of polynomials $f(x)\in\mathbb{Z}[x]$ (fix degree is n) s.t. $\mathrm{Gal}(f)\simeq S_n$

Theorem 4.12.1. (Hilbert's theorem) $\forall n\in\mathbb{N}$, there exists infinitely many $f(x)$ of $\deg n$ in $\mathbb{Z}[x]$ s.t. $\mathrm{Gal}(f)\simeq S_n$

Proof: We choose some monic polynomial as follow :

- $f_1(x)$ in $\mathbb{Z}[x]$ s.t. $\deg f_1=n$ and $f_1(x)$ is irr. in $\mathbb{Z}/2\mathbb{Z}[x]$
  (We can find the factor of $x^{2^n}-x$ with degree n in $\mathbb{Z}/2\mathbb{Z}[x]$)
- Let $g(x)$ be irr. in $\mathbb{Z}/3\mathbb{Z}[x]$ of $\deg n-1$ and define $f_2(x)$ of $\deg n$ s.t. $\overline{f_2}(x)=xg(x)$ in $\mathbb{Z}/3\mathbb{Z}[x]$
- Let $h(x)$ be irr. in $\mathbb{Z}/5\mathbb{Z}[x]$ of $\deg 2$
  If n is odd, let $p(x)$ be irr. of $\deg n-2$ and choose $f_3(x)$ of $\deg n$ s.t. $\overline{f_3}(x)=h(x)p(x)$ in $\mathbb{Z}/5\mathbb{Z}[x]$
  If n is even, let $p_1(x)$ and $p_2(x)$ be irr. in $\mathbb{Z}/5\mathbb{Z}[x]$ of $\deg 1$ and $n-3$, respectively. And choose $f_3(x)$ of $\deg n$ s.t. $\overline{f_3}(x)=h(x)p_1(x)p_2(x)$ in $\mathbb{Z}/5\mathbb{Z}[x]$

Now, let $f(x)=-15f_1(x)+10f_2(x)+6f_3(x)$ which is monic and $G=\mathrm{Gal}(f)$, D is the discriminant of f. Notice that $\overline{D}$ in $\mathbb{Z}/p\mathbb{Z}$ is the discriminant of $\overline{f}$ in $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}/p\mathbb{Z}$ are perfect field, which means f_1,f_2,f_3 are separable over $\mathbb{Z}/2\mathbb{Z},\mathbb{Z}/3\mathbb{Z},\mathbb{Z}/5\mathbb{Z}$, respectively. So we have $30\not| D$. Apply Theorem 4.11.1.:

- $\overline{f}(x)=\overline{f_1}(x)$: irr. in $\mathbb{Z}/2\mathbb{Z} \rightsquigarrow f(x)$: irr. and thus separable
- $\overline{f}(x)=\overline{f_2}(x)=xg(x)$ in $\mathbb{Z}/3\mathbb{Z} \rightsquigarrow G$ contains a $(n-1)$-cycle
- $\overline{f}(x)=\overline{f_3}(x)=\begin{cases}h(x)p(x) \text{ in } \mathbb{Z}/5\mathbb{Z} & \text{if } n: \text{odd}\\ h(x)p_1(x)p_2(x) \text{ in } \mathbb{Z}/5\mathbb{Z} & \text{if } n: \text{even}\end{cases}$

$$\rightsquigarrow \begin{cases}\rightsquigarrow ((a_1a_2)(a_3a_4\cdots a_n))^{n-2}=(a_1a_2)\in G\\ \rightsquigarrow ((a_1a_2)(a_3)(a_4\cdots a_n))^{n-3}=(a_1a_2)\in G\end{cases}$$

Hence, $\mathrm{Gal}(f)\simeq S_n$ □

Chapter 5

Homeworks

This are homework, sometimes we will use the result in the class or we will define some news and assume you know it in the class. Hope you get fun in Problem.

5.1

Problem 5.1.1. Let G be a commutative monoid

(a) Let $x_1, x_2, ..., x_n \in G$. Show that for given $\sigma \in S_n$,

$$\prod_{i=1}^{n} x_{\sigma(i)} = \prod_{i=1}^{n} x_i \tag{5.1}$$

(b) Let I and J be two sets and $f : I \times J \to G$ be a map such that $f(i,j) = e$ for almost all pairs (i,j). Show that

$$\prod_{i\in I}(\prod_{j\in J} f(i,j)) = \prod_{j\in J}(\prod_{i\in I} f(i,j)) \tag{5.2}$$

Problem 5.1.2. Let G a group and S be a nonempty set.

(a) Show that the set $M(S,G) := \{f : S \to G|\ f \text{ is a map}\}$ owns a natural group structure.

(b) Show that the set $\mathrm{Aut}(G) := \{f : G \to G|\ f \text{ is a group isomorphism}\}$ own a natural group structure.

Problem 5.1.3. Let H be a nonempty subset of a group G. Show that H is a subgroup if and only if for all $x, y \in H, xy^{-1} \in H$

Problem 5.1.4. Let G, G' be groups and $f : G \to G'$ be a group homomrphism. Show that $f(x^{-1}) = f(x)^{-1}$ for all $x \in G$.

5.2

Problem 5.2.1. A **partition** of a nomempty set S is a collection of nonempty subsets S_i of S with $i \in \Lambda$ such that $S_i \cap S_j = \emptyset$ for $i \neq j$ and $\cup_{i\in\Lambda} S_i = S$. An **equivalence relation** on S is a set $R \subset S \times S$ such that (1) $(x, x) \in R\ \forall x \in S$, (2) $(x, y) \in R$ implies $(y, x) \in R$ and (3) $(x, y), (y, z) \in R$ implies $(x, z) \in R$. Note that we write $x \sim y$ instead of $(x, y) \in R$. For $x \in S$, the equivalence class of x is defined to be the set $\{z \in S | x \sim z\}$.

(a) Show that given an equivalence relation $\sim$ on S, the associated equivalence classes form a partition of S.

(b) Conversely, show that if $\{S_i\}_{i\in\Lambda}$ is a partition of S, then it gives rise to an equivalence relation on S.

(c) For given a nutural number n, we define $a \equiv b$ if $n|(a - b)$ for $a, b \in \mathbb{Z}$. Show that $\equiv$ is an equivalence relation of $\mathbb{Z}$ and find the associated partition for $\mathbb{Z}$

Problem 5.2.2.

(a) In S_8, compute $(12345)(362)(4718)(12345)^{-1}$

(b) Find the subgroup of S_5 generated by $(123)(45)$

Problem 5.2.3.

(a) Show that $A_n = \langle (123), (124), ..., (12n)\rangle$ for $n \geq 3$.

(b) Show that $A_n = \langle (123), (234), ..., ((n-2)(n-1)n)\rangle$ for $n \geq 3$.

Problem 5.2.4. Let $D_{2n} = \langle \sigma, \tau | \sigma^n = 1,\ \tau^2 = 1,\ \tau\sigma = \sigma^{-1}\tau^{-1}\rangle$.

(a) Show that D_{2n} is also generated by τ and $\sigma\tau$.

(b) Let $G = \langle a, b | a^2 = b^2 = (ab)^n = 1\rangle$. Show that G is isomorphisc to D_{2n}.

(c) Show that $D_6 \approx \langle \begin{pmatrix} \cos(\frac{2\pi}{3}) & -\sin(\frac{2\pi}{3}) \\ \sin(\frac{2\pi}{3}) & \cos(\frac{2\pi}{3}) \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \rangle$

5.3

Problem 5.3.1. Let H be a subgroup of a group G. Show that the following statements are equivalent.

(a) H is a normal subgroup.

(b) $\forall x \in G, xHx^{-1} = H$

(c) $\forall x \in G, xH = Hx$

(d) $\forall x, y \in G, xHyH = xyH$

(e) H is the kernel of some group homomorphism.

Problem 5.3.2. Let $K \leq H \leq G$. Show that

$$(G : K) = (G : H)(H : K)$$

with the understanding that if two of the three indices appearing in this formula are finite, the so is the third and the formula holds.

Problem 5.3.3. Let G be a group $H.H'$ be subgroups. By a **double coset** of H, H' one means a subset of G of the form HxH'.

(a) Show that G is a disjoint union of double cosets.

(b) Let $\{c\}$ be a family of representatives for the double cosets. For each $a \in G$ denotes $[a]H'$ is the conjugate $aH'a^{-1}$ of H'. For each c we have a decomposition into ordinary cosets

$$H = \bigcup_c x_c(H \cap [c]H')$$

where $\{x_c\}$ is a family of elements of H, depending on c. Show that the element $\{x_c c\}$ form a family of left coset representatives for H' in G; that is

$$G = \bigcup_c \bigcup_{x_c} x_c cH$$

and the union is disjoint.

Problem 5.3.4. Let G be a group. A **commutator** in G is an element of the form $aba^{-1}b^{-1}$ with $a, b \in G$. Let G^c be the subgroup generated by the commutators. Then G^c is called the **commutator subgroup**. Show that G^c is normal and any homomorphism of G into an abelian group factors through G/G^c

5.4

Problem 5.4.1.

(a) If $G_1 \xrightarrow{f} G_2 \to G_3 \xrightarrow{g} G_4$ is exact, then "f is epi. $\iff$ g is monic"

(b) If $G_1 \xrightarrow{f} G_2 \to G_3 \to G_4 \xrightarrow{g} G_5$ is exact, then
"f : epi. and g mono. $\iff$ $G_3 = \{e\}$"

(c) Consider

$$\begin{array}{ccccccc} 0 & \longrightarrow & G_1 & \longrightarrow & G_2 & \longrightarrow & G_3 \quad : \text{exact} \\ & & & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} \\ 0 & \longrightarrow & G_1' & \longrightarrow & G_2' & \longrightarrow & G_3' \quad : \text{exact} \end{array}$$

Show that $\exists!\ f : G_1 \to G_1'$ s.t. the diagram commutes

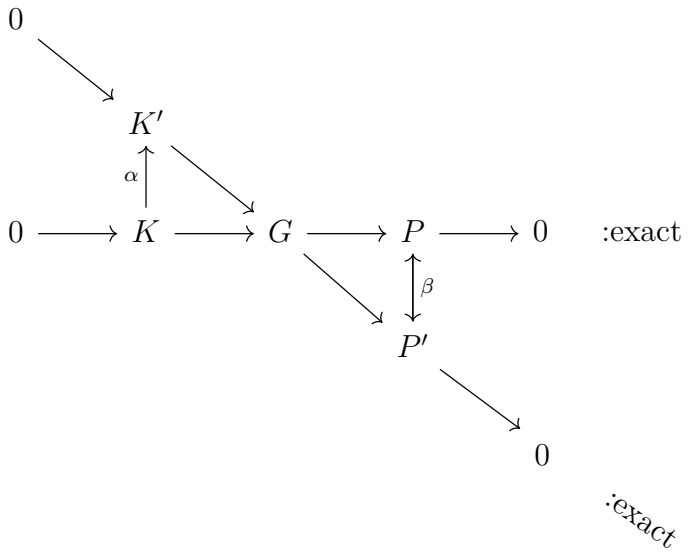
Similarly,

$$\begin{array}{ccccccc} 0 & \longrightarrow & G_1 & \longrightarrow & G_2 & \longrightarrow & G_3 \quad : \text{exact} \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \\ 0 & \longrightarrow & G_1' & \longrightarrow & G_2' & \longrightarrow & G_3' \quad : \text{exact} \end{array}$$

Show that $\exists!\ h : G_3 \to G_3$ s.t. the diagram commutes

(d) Let $f : G_1 \to G_2$. Show that $\exists\ 0 \to \ker f \to G_1 \xrightarrow{f} G_2 \to \operatorname{coker} f \to 0$: exact. where we define $\operatorname{coker} f := G_2/\operatorname{Im} f$ and assume $\operatorname{Im} f \lhd G_2$

(e) α : mono. and β : epi. Show that "$\ker \beta \neq 0 \iff \operatorname{coker} \alpha \neq 0$"



Problem 5.4.2. True or false : "$HK = KH \implies H \leq N(K)$ or $K \leq N(H)$"

Problem 5.4.3. Prove that the group of inner automorphisms of a group G is normal in $\operatorname{Aut}(G)$.

Problem 5.4.4. A group G is **metabelian** if it is has a normal subgroup H such that H and G/H are both abelian.

(a) Given an example for metabelian groups but not abelian groups.

(b) Show that any subgroup of a metabelian group is metabelian.

5.5

Problem 5.5.1. Let $T = T(n, k)$ be the uppeer triangular group of $\mathrm{GL}(n, k)$ with k being a field and $n \in \mathbb{Z}_{>0}$. Find an abelian tower ending with the trivial subgroup of T.

Problem 5.5.2. Let $\mathbb{Q}_8 := \langle i, j, k | i^2 = j^2 = k^2 = -1, ij = k, jk = i, ki = j \rangle$ be the **Quaternian group**. Exhibit a composition series for $\mathbb{Q}_8, D_8, \mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $(\mathbb{Z}/2\mathbb{Z})^3$, respectively.

Problem 5.5.3. Let $G^{(0)} = G, G^{(1)} = (G^{(0)})^c$ be the commutator subgroup of $G^{(0)}$ and $G^{(i+1)} = (G^{(i)})^c$ be the commutator subgroup of $G^{(i)}$ for all $i \geq 1$. Show that G is solvable if and only if $G^{(n)} = \{e\}$ for some n.

Problem 5.5.4. Let H be a subgroup of S_n with $n \geq 3$. Show that if $|H|$ is odd, then $H \subset A_n$

5.6

Problem 5.6.1. Show that $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is not cyclic for any $n \geq 3$.

Problem 5.6.2.

(a) Let p be an odd prime and let n be a positive integer. Show that $(1+p)^{p^{n-1}} \equiv 1 \pmod{p^n}$ but $(1+p)^{p^{n-2}}$ is not congruent to 1 $\pmod{p^n}$. Deduce that $(1+p)$ is an element of period p^{n-1} in the multiplicative group $(\mathbb{Z}/p^n\mathbb{Z})^\times$

(b) Let n be an integer with $n \geq 3$. Show that $(1 + 2^2)^{2^{n-2}} \equiv 1 \pmod{2^n}$ but $(1 + 2^2)^{2^{n-3}}$ is not congruent to 1 $\pmod{2^n}$. Deduce that 5 is an element of period 2^{n-2} in the multiplicative group $(\mathbb{Z}/2^n\mathbb{Z})^\times$

Problem 5.6.3.

(a) Let G be a finite abelian group. For a given $n \in \mathbb{Z}$, let n and $|G|$ be relatively prime. Show that the function $f : G \to G$ defined by $f(x) = x^n$ for all $x \in G$ is an isomorphism from G onto G.

(b) Let G be a group and the function $f : G \to G$ defined by $f(x) = x^n$ for all $x \in G$ be an isomorphism form G onto G where n is a positive integer. Show that $x^{n-1} \in Z_G$ for all $x \in G$.

(c) Let G be a group and the function $f : G \to G$ defined by $f(x) = x^3$ for all $x \in G$ be an isomorphism form G onto G. Show that G is abelian.

Problem 5.6.4. Let G be a finite abelian group. Show that if $d = o(ab)$ where $m = o(a)$ and $n = o(b)$, then $d | \operatorname{lcm}(m, n)$ and $\frac{mn}{\gcd(m,n)^2} \big| d$. In particular, this means that if m and n are relatively prime, then the order is multiplicative.

5.7

Problem 5.7.1. Assume that G is a finite group and p is the smallest prime dividing the order of G.

(a) Let H be a normal subgroup of order p in G. Show that H is in the center of G.

(b) Let H be a subgroup of index p in G. Show that H is a normal subgroup of G.

Problem 5.7.2. Let G be a finite group operating on a finite set S

(a) For each $s \in S$ show that

$$\sum_{t \in Gs} \frac{1}{\#(Gt)} = 1$$

(b) For each $x \in G$ define $f(x) =$ the number of element $s \in S$ such that $xs = s$. Prove that the number if orbits of G in S is equal to

$$\frac{1}{\#(G)} \sum_{x \in G} f(x)$$

Problem 5.7.3. Choose 9 pearls from pearls of different colors and chain them together to make a necklace. How many different necklaces can one have?

Problem 5.7.4. Let H be a proper subgroup of a finite group G. Show that G is not the union of all the conjugates of H.

5.8

Problem 5.8.1. Let $n \geq 5$.

(a) Let H and K be two subgroups of S_n such that N is a normal subgroup in H. Show that if H contains every 3-cycles and H/N is abelian, then N contains every 3-cycles.

(b) Show that S_n is not solvable.

Problem 5.8.2. Let H be a normal subgroup of A_n with $n \geq 5$.

(a) Show that if there is a (abc) in H, then $H = A_n$

(b) Show that if there is a $(ab)(cd)$ in H, then $H = A_n$.

(c) Show that A_n is simple for $n \geq 5$.

Problem 5.8.3. Show that the action of the alternating group A_n on $\{1, ..., n\}$ is $(n-2)$-transitive.

Problem 5.8.4. Let A_n be the alternating group of even permutations of $\{1, ..., n\}$. For $j = 1, ..., n$ let H_j be the subgroup of A_n fixing j, so $H_j \simeq A_{n-1}$, and $(A_n : H_j) = n$ for $n \geq 3$. Let $n \geq 3$ and let H be a subgroup of index n in A_n.

(a) Show that the action of A_n on cosets of H by left translation gives an isomorphism A_n with the alternating group of permutations of A_n/H.

(b) Show that there exists an automorphism of A_n mapping H_1 on H, and that such an automorphism is induced by an inner automorphism of S_n if and only if $H = H_i$ for some i.

5.9

Problem 5.9.1. Let $|G| = 1575$. Show that if a 3-Sylow subgroup of G is normal, then a 5-Sylow subgroup and a 7-Sylow subgroup are normal. In this situation, prove that G is abelian.

Problem 5.9.2. Show that no group of order 48 is simple and no group of order 30 is simple.

Problem 5.9.3. Let P be a p-group. Let A be a normal subgroup of order p. Prove that A is contained in the center of P.

Problem 5.9.4. Let G be a finite group and H a subgroup. Let P_H be a p-Sylow subgroup of H, Prove that there exists a p-Sylow subgroup P of G such that $P_H = P \cap H$.

Problem 5.9.5. Let H be a normal subgroup of a finite group G and assume that $\#(H) = p$, Prove that H is contained in every p-Sylow subgroup of G.

Problem 5.9.6. Let P, P' be p-Sylow subgroups of a finite group G.

(a) If $P' \subset N(P)$(normalizer of P), then $P' = P$

(b) If $N(P') = N(P)$, then $P' = P$

(c) We have $N(N(P)) = N(P)$

5.10

Problem 5.10.1. Assume that K is a cyclic group, H is an arbitrary group and ϕ_1, ϕ_2 are homomorphisms from K into $\mathrm{Aut}(H)$ such that $\phi_1(K)$ and $\phi_2(K)$ are conjugate subgroups of $\mathrm{Aut}(H)$. If K is infinite, then assume that ϕ_1, ϕ_2 are injective.

Prove by constructing an explicit isomorphism that the semidirect products of H and K with respect to ϕ_1, ϕ_2 are isomorphic.

Problem 5.10.2. Classify of groups of order 12.

Problem 5.10.3.

(a) Let H, N be normal subgroups of a finite group G. Assume that the orders of H, N are relatively prime. Prove that $xy = yx$ for all $x \in H$ and $y \in N$, and that $H \times N \simeq HN$.

(b) Let $H_1, H_2, ..., H_r$ be normal subgroups of G such that the order of H_i is relatively prime to the order of H_j for $i \neq j$. Prove that

$$H_1 \times ... \times H_r \simeq H_1 \cdots H_r$$

Problem 5.10.4. Let G be a finite group and let N be a normal subgroup such that N and G/N have relatively prime orders.

(a) Let H be a subgroup of G having the same order as G/N. Prove that $G = HN$.

(b) Let g be an automorphism of G. Prove that $g(N) = N$

Problem 5.10.5. Construct a non-abelian group of order 75. Classify all groups of order 75.

5.11

Problem 5.11.1. Let G be a finite abelian group. Show that there exist uniquely positive integers $m_1, m_2, ..., m_t$ such that $m_j | m_{j-1}$ for all $j \geq 2$ and

$$G \simeq \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_t\mathbb{Z}.$$

Here, $m_1, ..., m_t$ are called the invariant factors of G.

Problem 5.11.2. A group G is called a trosion group if all element of G have finite period. Let G be a torsion abelian group. Show that G is a direct sum of its subgroups $G(p)$ for all primes p such that $G(p) \neq \{e\}$.
Note that if $\{G_i\}_{i \in I}$ is a family of abelian group, then the direct product of $\{G_i\}_{i \in I}$ is

$$\prod_{i \in I} G_i = \{(x_i)_{i \in I} | x_i \in G_i\}$$

and the direct sum of $\{G_i\}_{i \in I}$ is

$$\bigoplus_{i \in I} G_i = \{(x_i) \in \prod_{i \in I} G_i | x_i = e \text{ for almost indices } i\}.$$

Problem 5.11.3. Viewing $\mathbb{Z}, \mathbb{Q}$ as additive groups, show that $\mathbb{Q}/\mathbb{Z}$ is a torsion group. Which has one and only one subgroup of order n for each integer $n \geq 1$, and that this subgroup is cyclic.

Problem 5.11.4. Let H be a subgroup of a finite abelian group G. Show that G has a subgroup that is isomorphism to G/H.

5.12

Problem 5.12.1. State and show the Three Isomorphism Theorems in the Ring theory.

Problem 5.12.2. Suppose that $1 \neq 0$ in A. Let S be a multiplicative subset of A not containing 0. Let $\mathfrak{p}$ be a maximal element in the set of ideals of A whose intersection with S is empty. Show that $\mathfrak{p}$ is prime.

Problem 5.12.3. Let $f : A \to A'$ be a surjective homomorphism of rings, and assume that A is local, $A' \neq 0$. Show that A' is local.

Problem 5.12.4. Let n be a positive integer and let $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ be its factorization into power of distinct primes. Show that

$$\mathbb{Z}/n\mathbb{Z} \simeq (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})$$

as a ring, so in particular we have the following isomorphism of multiplicative group:

$$(\mathbb{Z}/n\mathbb{Z})^\times \simeq (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})^\times$$

5.13

Problem 5.13.1. Show that any group is a quotient group of some free group.

Problem 5.13.2. Let P be a prime ideal of a commutative ring R and $S = R - P$. Show that R_S is a local ring. We also denote R_S by R_P.

Problem 5.13.3. Let R be an integral domain and $S = R - \{0\}$. Show that R_S is a field.

5.14

Problem 5.14.1. Let R be an integral domain.

Show that R is a UFD if and only if all irreducible elements in R are prime elements and all ascending chains on principal ideal are stable, that is, for any ascending chain $\langle a_1 \rangle \subset \langle a_2 \rangle \subset \cdots$, there exists k such that $\langle a_k \rangle = \langle a_{k+1} \rangle = \cdots$

Problem 5.14.2. Let $A_{-1} = \{a + b\sqrt{-1} | a \in \mathbb{Z}, b \in \mathbb{Z}\}, A_{-2} = \{a + b\sqrt{-2} | a \in \mathbb{Z}, b \in \mathbb{Z}\}$ and $A_{-5} = \{a + b\sqrt{-5} | a \in \mathbb{Z}, b \in \mathbb{Z}\}$.
Show that A_{-1} and A_{-2} are PID's, but A_{-5} is not a PID.

Problem 5.14.3. Let p be a prime integer. Show that

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

is irreducible in $\mathbb{Z}[x]$.

5.15

Problem 5.15.1. Given two extensions of fields $L/E, E/F$, show that

$$[L : F] = [L : E][E : F]$$

Problem 5.15.2. Given an extension of fields E/F and $A, B \subset E$(subset), show that

$$F(A \cup B) = F(A)(B)$$

Problem 5.15.3.

(a) Show that if $[E; F] = p$ for some prime integer p, then E/F is a simple extension.

(b) Let $E = F(\alpha)$ where α is algebraic over F, of odd degree. Show that $E = F(\alpha^2)$

Problem 5.15.4. Let $E = \mathbb{Q}(\alpha)$, where α is a root of the equation

$$\alpha^3 + \alpha^2 + \alpha + 2 = 0$$

Express $(\alpha^2 + \alpha + 1)(\alpha^2 + \alpha)$ and $(\alpha - 1)^{-1}$ in the form

$$a\alpha^2 + b\alpha + c$$

with $a, b, c \in \mathbb{Q}$

5.16

Problem 5.16.1. Let L/F be an algebraic extension and $\tau : L \to L$ be a monomorphism fixing F. Show that τ is an automorphism.

Problem 5.16.2. Let α and β be two elements which are algebraic over F. Let $f(X) = m_{\alpha,F}(X)$ and $g(X) = m_{\beta,F}(X)$. Suppose that $\deg f$ and $\deg g$ are relatively prime. Show that g is irreducible in the polynomial ring $F(\alpha)[X]$.

Problem 5.16.3. Let α be the real positive fourth root of 2. Find all intermediate fields in the extension $\mathbb{Q}(\alpha)$ of $\mathbb{Q}$

Problem 5.16.4. If α is a complex root of $X^6 + X^3 + 1$, find all homomorphisms $\sigma : \mathbb{Q}(\alpha) \to \mathbb{C}$

Problem 5.16.5. Let E, F be two finite extension of a field k, contained in a larger field K. Show that

$$[EF : k] \leq [E : k][F : k]$$

If $[E : k]$ and $[F : k]$ are relatively prime, show that one has an equality sign in the above relation.

5.17

Problem 5.17.1. Let E_1/F and E_2/F be normal sub-extensions of L/F. Show that $(E_1E_2)/F$ and $(E_1 \cap E_2)/F$ are also normal extensions.

Problem 5.17.2. Find the splitting field of $X^{p^8} - 1$ over the field $\mathbb{Z}/p\mathbb{Z}$.

Problem 5.17.3. Let α be a real number such that $\alpha^4 = 5$.

(a) Show that $\mathbb{Q}(i\alpha^2)$ is normal over $\mathbb{Q}$.

(b) Show that $\mathbb{Q}(\alpha + i\alpha)$ is normal over $\mathbb{Q}(i\alpha^2)$

(c) Show that $\mathbb{Q}(\alpha + i\alpha)$ is not normal over $\mathbb{Q}$.

Problem 5.17.4. Describe the splitting field of the following polynomials over $\mathbb{Q}$, and find the degree of each such splitting field.

(a) $X^2 - 2$ (b) $X^2 - 1$
(c) $X^3 - 2$ (d) $(X^3 - 2)(X^2 - 2)$
(e) $X^2 + X + 1$ (f) $X^6 + X^3 + 1$
(g) $X^5 - 7$

5.18

Problem 5.18.1. Let L be a finite extension of F.

(a) There exists an element $\alpha \in L$ such that $L = F(\alpha)$ if and only if there exists only a finite number of fields E such that $F \subset E \subset L$.

(b) If L is separable over F, then there exists an element $\alpha \in L$ such that $L = F(\alpha)$

Problem 5.18.2. Assume char $F = p > 0$. An element α algebraic over F is said to be purely inseparable over F if there exists a non-negative integer n such that $\alpha^{p^n} \in F$. An extension L/F is called a purely inseparable extension if each element of L is purely inseparable over F. Show TFAE

(1) L/F is purely inseparable

(2) For any $\alpha \in L$, its minimal polynomial $m_{\alpha,F}(x) = (x - \alpha)^m$ with $m \in \mathbb{N}$.

(3) For any $\alpha \in L$, its minimal polynomial $m_{\alpha,F}(x) = x^{p^r} - a$ with $r \in \mathbb{N}$.

(4) The only element of L which are separable over F are the elements of F itself.

(5) L is generated over F by a set of purely inseparable elements.

Problem 5.18.3. Suppose char $K = p$. Let $a \in K$. If $a \in K$. If a has no p-th root in K, show that $X^{p^n} - a$ is irreducible in $K[X]$ for all positive integers n.

Problem 5.18.4. Let $K = p$. Let α be algebraic over K. Show that α is separable if and only if $K(\alpha) = K(\alpha^{p^n})$ for all positive integers n.

5.19

Problem 5.19.1.

(a) Show that if F is a finite field, then F is not algebraically closed.

(b) Show that if F is a field such that $(F^\times \cdot, 1)$ is a cyclic group, then F is a finite field.

Problem 5.19.2. Let char $K = p$. Let L be a finite extension of K, and suppose $[L : K]$ prime to p. Show that L is separable over K.

Problem 5.19.3. Show that every element of a finite field can be written as a sum of two squares in that field.

Problem 5.19.4. Let k be a field of characteristic p and let t, u be algebraically independent over k. Prove the following:

(a) $k(t, u)$ has degree p^2 over $k(t^p, u^p)$

(b) There exists infinitely many extensions between $k(t, u)$ and $k(t^p, u^p)$.

5.20

Problem 5.20.1. For another proof of Artin's theorem without using the primitive element theorem, we can show the inequality "$[L : L^G] \leq |G|$" by assuming $G = \{\sigma_1, ..., \sigma_n\}$ and $a_1, ..., a_{n+1}$ being linearly independent element in L over L^G to get contradiction. Please carry out the proof.

Problem 5.20.2. What is the Galois group of the following polynomial?

(a) $f_1(X) = X^3 - X - 1$ over $\mathbb{Q}$

(b) $f_2(X) = X^3 - 10$ over $\mathbb{Q}$

(c) $f_3(X) = X^3 - 10$ over $\mathbb{Q}\left(\sqrt{2}\right)$

(d) $f_4(X) = X^3 - 10$ over $\mathbb{Q}\left(\sqrt{-3}\right)$

(e) $f_5(X) = X^3 - X - 1$ over $\mathbb{Q}\left(\sqrt{-23}\right)$

Problem 5.20.3. Find the Galois group over $\mathbb{Q}$ of the following polynomials.

(a) $X^3 + X + 1$

(b) $X^3 + 2X + 1$

(c) $X^3 - X - 1$

(d) $X^3 + X^2 - 2X - 1$

Problem 5.20.4. Let $k = \mathbb{C}(t)$ be the field of rational function in one variable. Find the Galois group over k of the following polynomials:

(a) $X^3 - X + t$

(b) $X^3 - 2tX + t$

(c) $X^3 + t^2X - t^3$

5.21

Problem 5.21.1. Find the Galois group of $x^4 - 2$ over $\mathbb{Q}$. Find all subgroups of this group and all corresponding intermediate fields between its splitting field and $\mathbb{Q}$.

Problem 5.21.2. Let $(F) \neq 2, 3$ and $f(x) = x^4 + px^2 + qx + r$ be an irreducible separable polynomial in $F[x]$ with roots being $\alpha_1, \alpha_2, \alpha_3, \alpha_4$. Let $L = F(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ and $G = \mathrm{Gal}(L/F) \leq S_4$.
Set $\beta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4, \beta_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4, \beta_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3$.

(a) Show that

$$L^{G \cap V} = F(\beta_1, \beta_2, \beta_3)$$

and

$$\mathrm{Gal}(F(\beta_1, \beta_2, \beta_3)/F) \simeq G/(G \cap V)$$

where $V = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$.

(b) Show that there exists i such that $\beta_i \in F$ if and only if $G \leq D_8$.

(c) Let $h(x) = (x-\beta_1)(x-\beta_2)(x-\beta_3) \in F[x]$ with the discriminant being D. Show that

(1) if $h(x)$ is irreducible and $D \notin F^2$, then $G \simeq S_4$

(2) if $h(x)$ is irreducible and $D \in F^2$, then $G \simeq A_4$

(3) if $h(x)$ splits completely in $F[x]$, then $G \simeq V$

(4) if $h(x)$ have one root in F. Then

(i) if $f(x)$ is irreducible over $F(\beta_1, \beta_2, \beta_3)$, them $G \leq D_8$;

(ii) if $f(x)$ is reducible over $F(\beta_1, \beta_2, \beta_3)$, them $G \leq C_4$.

Problem 5.21.3. Let $f(x) = x^4 + ax^2 + b$ be an irreducible polynomial over $\mathbb{Q}$, with roots $\pm\alpha, \pm\beta$, and splitting field K.

(a) Show that $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to subgroup of D_8 (the non-abelian group of order 8 other than the quaternion group), and thus is isomorphic to one of the following:

(i) $\mathbb{Z}/4\mathbb{Z}$ (ii)$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (iii) D_8.

(b) Show that the first case happens if and only if

$$\frac{\alpha}{\beta} - \frac{\beta}{\alpha} \in \mathbb{Q}$$

Case (ii) happens if and only if $\alpha\beta \in \mathbb{Q}$ or $\alpha^2 - \beta^2 \in \mathbb{Q}$. Case (iii) happens otherwise. (Actually, in (ii), the case $\alpha^2 - \beta^2 \in \mathbb{Q}$ cannot occur. It corresponds to a subgroup of $D_8 \subset S_4$ which is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, but is not transitive on $\{1,2,3,4\}$).

(c) Find the splitting field K in $\mathbb{C}$ of the polynoimal

$$x^4 - 4x^2 - 1$$

Determine the Galois group of this splitting field over $\mathbb{Q}$, and describe fully the lattices of subgroups of the Galois group.

5.22

Problem 5.22.1. For any prime $p \leq 5$. let $m, n_1, ..., n_{p-2} \in \mathbb{Z}$ such that $m > 0$ is even and $n_1, ..., n_{p-2}$ are even with $n_1 < n_2 < \cdots < n_{p-2}$. (If $p = 2$, then we assume $m > 2$.) Consider

$$g(x) = (x^2 + m)(x - n_1)(x - n_2)\cdots(x - n_{p-2})$$

and $f(x) = g(x) - 2 \in \mathbb{Z}[x]$.

(a) Show that f is irreducible in $\mathbb{Z}[x]$.

(b) Show that the Galois group is isomorphic to S_p.

Problem 5.22.2. Let $f(x) \in \mathbb{Q}[x]$ be a polynomial of degree n, and let K be a splitting field of f over $\mathbb{Q}$. Suppose that $\mathrm{Gal}(K/\mathbb{Q})$ is the symmetric group S_n with $n > 2$.

(a) Show that f is irreducible over $\mathbb{Q}$.

(b) If α is a root of f, show that the only automorphism of $\mathbb{Q}(\alpha)$ is identity.

(c) If $n \geq 4$, show that $\alpha^n \notin \mathbb{Q}$

Problem 5.22.3. A polynomial $f(x)$ is said to be **reciprocal** if whenever α is root, then $1/\alpha$ is also a root. We suppose that f has coefficients in a subfield $k \subset \mathbb{R} \subset \mathbb{C}$. If f is irreducible over k, and has a nonreal root of absolute value 1, show that f is reciprocal of even degree.

5.23

Problem 5.23.1.

(a) Show that

$$[\mathbb{Q}(\zeta_n + \frac{1}{\zeta_n}) : \mathbb{Q}] = \frac{\phi(n)}{2}$$

(b) Find Φ_8, Φ_9.

(c) Show that $x^{16} + 1$ is irreducible in $\mathbb{Q}[x]$ and is reducible in $(\mathbb{Z}/7\mathbb{Z})[x]$ as a product of 4 quartic polynomials.

Problem 5.23.2.

(a) Let k be a field of characteristic $\not| 2n$, for some odd integer $n \geq 1$, and let ζ be a primitive n-th root of unity, in k. Show that k also contains a primitive $2n$-th root of unity.

(b) Let k be a finite extension of the rationals. Show that there is only a finite number of roots of unity in k.

Problem 5.23.3.

(a) Determine which roots of unity lie in the following fields:
$\mathbb{Q}(i), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{-5})$.

(b) For which integers m does a primitive m-th root of unity have degree 2 over $\mathbb{Q}$?

Problem 5.23.4.

(a) Let a be a non-zero integer, p a prime, n a positive integer, and $p \nmid n$. Prove that $p|\Phi_n(a)$ if and only if a has period n in $(\mathbb{Z}/p\mathbb{Z})^*$.

(b) Again assume $p \nmid n$. Prove that $p|\Phi_n(a)$ for some $a \in \mathbb{Z}$ if and only if $p = 1 \mod n$. Deduce from this that there are infinitely many primes $= 1 \mod n$, a special case of Dirichlet's theorem for the existence of primes in an arithmetic progression.

5.24

Problem 5.24.1. Show the theorem or corollary in below:

(a) (Artin) Let G be a monoid and K a field. Let $\chi_1, ..., \chi_n$ be distinct characters of G in K. Then they are linearly independent over K.

(b) Let $\alpha_1, ..., \alpha_n$ be distinct non-zero elements of a field K. If $a_1, ..., a_n$ are elements of K such that for all integers $\nu \geq 0$ we have

$$a_1\alpha_1^\nu + \cdots + a_n\alpha_n^\nu = 0$$

then $a_i = 0$ for all i.

(c) Let E be a finite separable extension of k, and let $\sigma_1, ..., \sigma_n$ be the distinct embeddings of E into k^a over k. Let $w_1, ..., w_n$ be elements of E. Then the vectors

$$\begin{aligned} \zeta_1 &= (\sigma_1 w_1, ..., \sigma_1 w_n) \\ &\vdots \\ \zeta_n &= (\sigma_n w_1, ..., \sigma_n w_n) \end{aligned}$$

are linearly independent over k^a if $w_1, ..., w_n$ form a basis of E over k.

Problem 5.24.2. Let ζ be a primitive n-th root of unity. Let $K = \mathbb{Q}(\zeta)$.

(a) If $n = p^r (r \geq 1)$ is a prime power, show that $N_{K/\mathbb{Q}}(1 - \zeta) = p$

(b) If n is composite (divisible by at least two primes) then $N_{K/\mathbb{Q}}(1 - \zeta) = 1$

5.25

Problem 5.25.1. Let k be a field of characteristic $\neq 2$. Let $c \in k, c \notin k^2$. Let $F = k(\sqrt{c})$. Let $\alpha = a + b\sqrt{c}$ with $a, b \in k$ and not both $a, b = 0$. Let $E = F(\sqrt{\alpha})$. Prove that the following conditions are equivalent.

(1) E is Galois over k.

(2) $E = F(\sqrt{\alpha'})$, where $\alpha' = a - b\sqrt{c}$.

(3) Either $\alpha\alpha' = a^2 - cb^2 \in k^2$ or $c\alpha\alpha' \in k^2$

Show that when these conditions are satisfied, then E is cyclic over k of degree 4 if and only if $c\alpha\alpha' \in k^2$.

Problem 5.25.2. Let k be a field of characteristic $\neq 2, 3$. Let $f(x), g(x) = x^2 - c$ be irreducible polynomials over k, of degree 3 and 2 respectively. Let D be the discriminant of f. Assume that

$$[k(D^{1/2}) : k] = 2 \text{ and } k(D^{1/2}) \neq k(c^{1/2})$$

Let α be a root of f and β a root of g in an algebraic closure. Prove:

(a) The splitting field of fg over k has degree 12.

(b) Let $\gamma = \alpha + \beta$. Then $[k(\gamma) : k] = 6$.

Problem 5.25.3.

(a) Let K be cyclic over k of degree 4, and of characteristic $\neq 2$. Let $G_{K/k} = \langle\sigma\rangle$. Let E be the unique subfield of K of degree 2 over k. Since $[K : E] = 2$, there exists $\alpha \in K$ such that $\alpha^2 = \gamma \in E$ and $K = E(\alpha)$. Prove that there exists $z \in E$ such that

$$z\sigma z = -1,\ \sigma\alpha = z\alpha,\ z^2 = \sigma\gamma/\gamma$$

(b) Conversely, let E be a quadratic extension of k and let $G_{E/k} = \langle\tau\rangle$. Let $z \in E$ be an element such that $z\tau z = -1$. Prove that there exists $\gamma \in E$ such that $z^2 = \tau\gamma/\gamma$. Then $E = k(\gamma)$. Let $\alpha^2 = \gamma$, and let $K = k(\alpha)$. Show that K is Galois, cyclic of degree 4 over k. Let σ be an extension of τ to K. Show that σ is an automorphism of K which generates $G_{K/k}$, satisfying $\sigma^2\alpha = -\alpha$ and $\sigma\alpha = \pm z\alpha$. Replacing z by $-z$ originally if necessary, one can then have $\sigma\alpha = z\alpha$.

5.26

No Homework! P

5.27

Problem 5.27.1. Let p be a prime. Show that any solvable subgroup of S_p of order divisible by p is contained in the normalizer of a p-Sylow subgroup of S_p. Conclude that an irreducible polynomial $f(x) \in \mathbb{Q}[x]$ of degree p is solvable by radical if and only if its Galois group is contained in the normalizer of a p-Sylow subgroup of S_p.

Problem 5.27.2. Let k be a field of characteristic 0. Assume that for each finite extension E of k, the index $(E^* : E^{*n})$ is finite for every positive integer n. Show that for each positive integer n, there exists only a finite number of abelian extensions of k of degree n.

Problem 5.27.3. Let $a \neq 0, \pm 1$ be a square-free integer. For each prime number p, let K_p be the splitting field of the polynomial $x^p - a$ over $\mathbb{Q}$. Show that $[K_p : \mathbb{Q}] = p(p-1)$. For each square-free integer $m > 0$, let

$$K_m = \prod_{p|m} K_p$$

be the compositum of all subfield K_p for $p|m$. Let $d_m = [K_m : \mathbb{Q}]$ be the degree of K_m over $\mathbb{Q}$. Show that if m is odd then $d_m = \prod_{p|m} d_p$, and if m is even, $m = 2n$ then $d_{2n} = d_n$ or $2d_n$ according as $\sqrt{a}$ is or is not in the field of m-roots of unity $\mathbb{Q}(\zeta_m)$.

5.28

Problem 5.28.1. Show that if $f(x) = x^n + px + q$, then its discriminant is

$$D = (-1)^{\frac{n(n-1)}{2}} n^n q^{n-1} + (-1)^{\frac{(n-2)(n-1)}{2}} p^n (n-1)^{n-1}$$

Problem 5.28.2. Let $f(x) = x^5 - x - 1 \in \mathbb{Q}[x]$. Determine the Galois group of $f(x)$ over $\mathbb{Q}$.