Groups — Structures and actions.

G: normal subgroup.
factor group.

Composition factors

A_n: $n \geq 5$ simple.

S_n: non solvable.

structure: subgroups.

Sylow subgps. 3 Sylow thms.

Ex. S_4

A_4

$\langle (12)(34), (13)(24) \rangle$:

$A_4 = C_2^2 : C_3$

$C_2 \times C_2$. — unique smallest normal subgp.

$S_4 / C_2 \times C_2 \cong S_3 \Rightarrow S_4 = C_2^2 : S_3$.

actions: conjugation

coset action — transitive.

G on $[G:H] = \{ Hx \mid x \in G \}$.

Rings

R: subring, ideal — quotient ring.

prime ideal: $ab \in I \Rightarrow a \in I$ or $b \in I$.

fractional fields of ID:

$\left\{ \frac{a}{b} \middle| a, b \in R, b \neq 0 \right\} \longleftarrow R$

b is not a zero divisor.

Chinese Reminder Theorem.

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

If $m_1, m_2, \cdots, m_n$ are pairwise coprime, then the system has a solution. i.e. $\exists\, b$.

Factorizations of elts in a ring:

$R = \mathbb{Z}[\sqrt{-5}] = \{ a + b\sqrt{5} \mid a, b \in \mathbb{Z} \}$.

$6 = 2 \cdot 3 = (1+\sqrt{5})(1-\sqrt{5})$.

$\Rightarrow 2 \mid (1+\sqrt{5})(1-\sqrt{5})$, $(1+\sqrt{5}) \mid 2 \cdot 3$.

UFD $\leftarrow$ PID

ED

Fields

F, char $F = 0$ or p.

- extensions: $F < E$. $\quad E \mid F$.
- polys and algebraic elts.
- degrees of extension.

construction by Ruler – Compasses.

- For $f(x) \in F[x]$, there exists an extension E of F, s.t $f(x)$ has roots in E.

$(\mathbb{F}_p \longrightarrow \mathbb{F}_{p^d})$

$f(x) \in \mathbb{F}_p[x]$. $\mathbb{F}_p[x] / (f(x)) \cong \mathbb{F}_{p^d}$.

$\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$.

- If char $F=0$, each finite extension E of F is simple.

$$E = F(\alpha). \Leftarrow E = \mathbb{Q}(\sqrt{2}, 2^{\frac{1}{3}}, 2^{\frac{1}{5}}, \cdots, 3^{\frac{1}{7}})$$

- Let $F < L < E$ with char $F=0$. E is a splitting field of F.

$$\begin{array}{c} E \\ | \\ L \\ | \\ F \end{array}$$

Then $\mathrm{Gal}(E:L) \triangleleft \mathrm{Gal}(E:F) \Leftrightarrow L$ is a splitting field of F. $(F \triangleleft L)$

<u>Ex.</u> Let $f(x) = x^m - 2 \in \mathbb{Q}[x]$.

Find $\mathrm{Gal}(f)$.

$F = \mathbb{Q} < E =$ splitting field of f. $E = \mathbb{Q}(2^{\frac{1}{m}}, w)$, $w = e^{\frac{2\pi i}{m}}$.

$$\begin{array}{c} E \\ | \\ L \\ | \\ F \end{array}$$

$F < L = \mathbb{Q}(w) < E$.

both normal. (Rmk: If char $F=0$ or F finite, a splitting extension of $F \Leftrightarrow$ normal.)

$\mathrm{Gal}(f) = \mathrm{Gal}(E:F)$.

$\mathrm{Gal}(E:L)$

$E = L(\alpha)$, $\alpha = 2^{\frac{1}{m}}$.

$\rho \in \mathrm{Gal}(E:L)$

$\rho: \alpha \mapsto \alpha w \mapsto \alpha w^2 \mapsto \cdots \mapsto \alpha w^{m-1}$

$\langle \rho \rangle = \mathbb{Z}_m = \mathrm{Gal}(E:L)$

(char $=0$, permute the roots).

$\mathrm{Gal}(L:F)$.

L is the splitting field of $x^m - 1$ over $F = \mathbb{Q}$.

$\mathrm{Gal}(L:F)$ is a permutation group on the set P_m of the m roots of $x^m - 1$, dividing P_m into orbits.

an orbit consists of the primitive roots of $x^d - 1$ with $d \mid m$. $(x^d - 1 \mid x^m - 1)$.

$\mathrm{Gal}(L:F) \cong \mathrm{Aut}(\mathbb{Z}_m)$

order: $\phi(m)$.

[· How to find out the Galois group of a poly ?]

$\mathrm{Gal}(E:F) \triangleright \mathrm{Gal}(E:L)$ $\qquad$ $\mathrm{Gal}(E:F) = \mathrm{Gal}(E:L) : \mathrm{Gal}(L:F)$.

Classify all order 24 groups:

① abelian: 3×8, $3 \times 4 \times 2$, $3 \times 2 \times 2 \times 2$.

② non-abelian: Sylow 2-subgp. order 8.

8, 4×2, $2 \times 2 \times 2$.

D_8 $\quad Q_8 = \langle i, j, k \mid |i| = |j| = |k| = 4 \rangle$

$i \to j \to k \to i$.

(i) $G = G_2 \times G_3 = 3 \times D_8$, $3 \times Q_8$ — nilpotent (all sylow p groups are unique and normal).

$3 \to C_3$.

(ii) $G_2 \lhd G \Rightarrow Q_8 : 3$, $C_2^3 : C_3 \cong (\underline{C_2^2 : C_3}) \times C_2$
$(G_3 \ntriangleleft G)$
$A_4 \times C_2$.

(iii) $G_3 \lhd G \Rightarrow 3:8$. $(3:4) \times 2$. $(3:2) \times 2 \times 2$. $3 : D_8$. $3 : Q_8$.
$(G_2 \ntriangleleft G)$
(two) (unique).

$\langle x \rangle : \langle \rho, \tau \mid |\rho| = 4, |\tau| = 2, \rho^\tau = \rho^{-1} \rangle$.
① $x^\rho = x^{-1}$, $x^\tau = x$.
② $x^\rho = x$, $x^\tau = x^{-1}$. $\Rightarrow D_{24}$.

(iv) S_4.