4.3 Burnside's theorem

Lemma 1: $L/\mathbb{Q}$ finite Galois with $L \subset \overline{\mathbb{Q}}$

$\mathcal{O}_L = \mathbb{Z}^{int} \cap L$ (integers of L)

Then $N_{L/\mathbb{Q}}(\mathcal{O}_L) \subset \mathbb{Z}$

proof: Consider $\alpha \in \mathcal{O}_L$. Its min. pol. $f = \sum c_i T^i$ over $\mathbb{Q}$ is in $\mathbb{Z}[T]$ by Prop. 4.1.1. Thus

$$N_{L/\mathbb{Q}}(\alpha) = (\pm c_0)^d \in \mathbb{Z}$$

where $d = [L:\mathbb{Q}(\alpha)] = \frac{[L:\mathbb{Q}]}{\deg f}$. □

Lemma 2: $\lambda_1 - \lambda_n \in \mathbb{C}$ roots of unity

If $a = \frac{1}{n}(\lambda_1 + - + \lambda_n) \in \mathbb{Z}^{int}$,

then either $a = 0$ or $a = \lambda_1 = -- = \lambda_n$.

proof: · If $\lambda_i \neq \lambda_j$ for some $i \neq j$, then

$$|a| < \frac{1}{n} \sum_{i=1}^{n} |\lambda_i| = 1$$

· We have $\lambda_1 - \lambda_n \in \mathbb{Q}(\zeta_r)$ for some $r \geq 1$.

Let $G = \mathrm{Gal}(\mathbb{Q}(\zeta_r)/\mathbb{Q})$ and $\sigma \in G$.

Then

$$\sigma(a) = \frac{1}{n}(\sigma(\lambda_1) + - + \sigma(\lambda_n))$$

roots of unity

and $\sigma(\lambda_i) \neq \sigma(\lambda_j)$. Thus also $|\sigma(a)| < 1$.

- Therefore

$$\underbrace{|N_{\mathbb{Q}(\zeta_r)/\mathbb{Q}}(a)|}_{\in \mathbb{Z} \text{ by Lemma 1}} = \prod_{\sigma \in G} |\sigma(a)| < 1$$

$$\Rightarrow N_{\mathbb{Q}(\zeta_r)/\mathbb{Q}}(a) = 0$$

$$\Rightarrow a = 0.$$ $\square$

G finite group

$K = \mathbb{C}$

Prop 3: V irred. G-repr. with character χ
C conj. cl. of G
$g \in C$
If $\gcd(\#C, \dim V) = 1$, then either $\chi(g) = 0$
or g acts as a scalar on V.

proof: - Let $d = \dim V$ and $\rho_V(g) \sim \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_d \end{pmatrix} = A(g)$.

Then - $\chi(g) = \lambda_1 + \dots + \lambda_d \in \mathbb{Z}^{\text{int}}$;

- $\frac{\#C}{d} \chi(g) \in \mathbb{Z}^{\text{int}}$, by Lemma 4.2.3.

- If $\gcd(\#C, d) = 1$, then $a \cdot \#C + b \cdot d = 1$

for some $a, b \in \mathbb{Z}$. Thus

$$\frac{1}{d}(\lambda_1 + \dots + \lambda_d) = \frac{\chi(g)}{d} = a \cdot \underbrace{\frac{\#C}{d} \cdot \chi(g)}_{\in \mathbb{Z}^{int}} + b \cdot \underbrace{\chi(g)}_{\in \mathbb{Z}^{int}} \in \mathbb{Z}^{int}$$

- By Lemma 2, either $\chi(g) = 0$ or $\lambda_1 = \dots = \lambda_d$. $\square$

Prop. 4: If G is simple, then none of its conj. cl. can be of order p^k with p prime and $k > 0$.

proof: - Let C be a conj. cl. of G. Assume that $\#C = p^k$ with p prime and $k > 0$. In part., $C \neq \{e\}$.

- By column orthogonality (Prop. 2.2.9),

$$\sum_{\chi \text{ simple}} \chi(C) \cdot \underbrace{\overline{\chi(e)}}_{= \dim \chi \in \mathbb{Z}_{>0}} = 0$$

- Define $X = \{\chi \text{ simple} \mid p \mid \chi(e)\}$

$Y = \{\chi \text{ simple} \mid p \nmid \chi(e) \ \& \ \chi \neq \chi_{triv}\}$

Claim: $\chi(C) \neq 0$ for some $\chi \in Y$.

proof: For $\chi \in X$, $\underbrace{\frac{1}{p}\overline{\chi(e)}}_{\in \mathbb{Z}_{>0}} \cdot \underbrace{\chi(C)}_{\in \mathbb{Z}^{int}} \in \mathbb{Z}^{int}$

Thus
$$a = \sum_{\chi \in X} \frac{1}{p} \chi(C) \cdot \overline{\chi(e)} \in \mathbb{Z}^{int}.$$

$$\Rightarrow a \neq -\frac{1}{p} \in \mathbb{Q} - \mathbb{Z}$$

$$0 = \sum_{\chi \text{ simple}} \chi(C) \cdot \overline{\chi(e)}$$

$$= \underbrace{\chi_{\text{triv}}(C) \cdot \overline{\chi_{\text{triv}}(e)}}_{=1 \cdot 1 = 1} + \underbrace{\sum_{\chi \in X} \chi(C) \cdot \overline{\chi(e)}}_{= p \cdot a} + \sum_{\chi \in Y} \chi(C) \overline{\chi(e)}$$

$$= \underbrace{1 + p \cdot a}_{\neq 0} + \sum_{\chi \in Y} \chi(C) \cdot \underbrace{\overline{\chi(e)}}_{\in \mathbb{Z}_{>0}}$$

Thus $\chi(C) \neq 0$ for some $\chi \in Y$. ↯

- Let $\chi \in Y$ with $\chi(C) \neq 0$, $g \in C$ and V an irred. G-repr. with char. χ.

  Since $p \nmid \overline{\chi(e)}$, $\gcd(\underbrace{\#C}_{= p^k}, \underbrace{\dim V}_{= \chi(e)}) = 1$.

  Since $\chi(g) \neq 0$, Prop. 3 implies that g acts as a scalar on V.

- Let $g_V(g) \sim \begin{pmatrix} \lambda & \\ & \ddots & \\ & & \lambda \end{pmatrix}$ and $g_V(h) \sim \begin{pmatrix} \mu & \\ & \ddots & \\ & & \mu \end{pmatrix}$ for $g, h \in C$. Then $\lambda = \frac{\chi(g)}{\dim V} = \frac{\chi(h)}{\dim V} = \mu$.

- Define $H = \langle g h^{-1} \mid g, h \in C \rangle$.

  Then $H \trianglelefteq G$ since for all $a \in G$,

$$a g h^{-1} a^{-1} = \underbrace{a g a^{-1}}_{\in C} (\underbrace{a h a^{-1}}_{\in C})^{-1} = \tilde{g} \tilde{h}^{-1} \in H$$

- Since V is not trivial ($\chi \in Y$), $H \neq G$.
  Since $\# C = p^k > 1$, $H \neq \{e\}$. Thus
  G is not simple. ↯

$\square$

<u>Thm 5:</u> (Burnside)

If $\# G = p^k q^e$ with p, q prime, $k, e \geq 0$, then G is solvable.

<u>proof</u>: · Assume that there exists a group G of order $p^k q^e$ that is <u>not</u> solvable. Assume that $\# G = p^k q^e$ is minimal. Then G is simple (since one of its subquotients is not solvable and of order $p^{k'} q^{e'} \mid \# G$)

- In particular, $Z(G) = \{e\}$, and by Prop. 4, for every conj. cl. $C \neq \{e\}$ of G, $p \cdot q \mid \# C$. But

$$\# G = 1 + \sum_{C \neq \{e\}} \# C$$

divisible by pq

cannot be divisible by neither p nor q.
Thus $\# G = p^0 q^0$, but $G = \{e\}$ is solvable. ↯

$\square$

<u>Rem:</u> A_5 is <u>not</u> solvable and has $\# A_5 = 2^2 \cdot 3^1 \cdot 5^1$ elements. Thus Burnside's thm. does not extend to 3 primes.