Chapter 4. Burnside's $p^a q^b$-Theorem

Notation

G finite group
$C_i = [g_i]$ $(1 \leq i \leq r)$: conj. classes of G
$\hat{C}_i$ $(1 \leq i \leq r)$: class sums
ω_i $(1 \leq i \leq r)$: central character of $\mathbb{C}G$.
$\mathrm{Irr}(G) = \{\chi_1, \dots, \chi_r\}$, $r = |C(G)|$; $n_i := \chi_i(1)$
m_{jkl} $(1 \leq j,k,l \leq r)$: class mult. constants

1. Algebraic integers and character values.

Recap on algebraic integers (See Commutative Algebra)

* An element $b \in \mathbb{C}$ is called an algebraic integer iff it is integral over $\mathbb{Z}$, i.e. $\exists f \in \mathbb{Z}[X]$ monic s.t. $f(b) = 0$.

* If $b \in \mathbb{Q}$ is integral over $\mathbb{Z}$, then $b \in \mathbb{Z}$.

* If $A \subseteq \mathbb{C}$ is a subring, then $\{b \in \mathbb{C} \mid b \text{ integral over } A\}$ is a subring of $\mathbb{C}$

* In particular $\mathcal{O} := \{b \in \mathbb{C} \mid b \text{ algebraic integer}\}$ is a subring of $\mathbb{C}$, so that sums and products of algebraic integers are algebraic integers.

Lemma 4.1: Character values are algebraic integers.

Proof: Let χ be a character of G, and let $g \in G$. Set $n := \deg(\chi)$.

$\overset{\text{Prop 2.1(b)}}{\Longrightarrow}$ $\chi(g) = \varepsilon_1 + \dots + \varepsilon_n$ with ε_i $o(g)$-th root of unity $\forall\ 1 \leq i \leq n$.

But then ε_i is a zero of $X^m - 1 \in \mathbb{Z}[X]$, where $m := o(g)$. $\forall\ 1 \leq i \leq n$.

$\Rightarrow$ $\varepsilon_1, \dots, \varepsilon_n$ are algebraic integers.

$\Rightarrow$ so is $\chi(g)$ as a sum of alg. integers. #

30. Mai 2017

Theorem 4.2 [Integrality Theorem]

The values of the central characters of G are algebraic integers.

Proof: Cor. 3.13 $\Rightarrow$ $\omega_i(\hat{C}_j)\,\omega_i(\hat{C}_k) = \sum_{l=1}^{r} m_{jkl}\, \omega_i(\hat{C}_l)$

$\forall\ 1 \leq i, j, k \leq r$.

For $1 \leq i,k \leq r$ set: $W_i = (\omega_i(\hat{C}_1), \ldots, \omega_i(\hat{C}_r))^t$

$M_k := (m_{jkl})_{\substack{1 \leq j \leq r \\ 1 \leq l \leq r}}$

so that $M_k W_i = \omega_i(\hat{C}_k) W_i$

Now as $\omega_i(1) = 1$ certainly $\omega_i \neq 0$, therefore W_i is an eigenvector of M_k with eigenvalue $\omega_i(\hat{C}_k)$

$\Rightarrow$ $\omega_i(\hat{C}_k)$ is a zero of $f := \det(M_k - X I_r)$

But the class mult. csts $m_{jkl} \in \mathbb{Z}$ by def^n $\Rightarrow f \in \mathbb{Z}[X]$

Hence $\omega_i(\hat{C}_k)$ is an algebraic integer.

#

Corollary 4.3:

$\frac{|C_j|}{n_i} \chi_i(g_j)$ is an algebraic integer.

Proof: Apply Prop. 3.15 (a). #

Corollary 4.4:

$\chi(1) \mid |G| \quad \forall \chi \in \mathrm{Irr}(G)$.

Proof: Let $\chi_i \in \mathrm{Irr}(G) = \{\chi_1, \ldots, \chi_r\}$. We have

$$\frac{|G|}{n_i} = \frac{|G|}{n_i} \langle \chi_i, \chi_i \rangle \overset{\text{orthog. of chars}}{=} \frac{1}{n_i} \sum_{j=1}^{r} |C_j| \chi_i(g_j) \chi_i(g_j^{-1})$$

$$= \sum_{j=1}^{r} \frac{|C_j|}{n_i} \chi_i(g_j) \chi_i(g_j^{-1})$$

$$= \sum_{j=1}^{r} \underbrace{\omega_i(\hat{C}_j)}_{\substack{\text{alg. int} \\ \text{by 4.2}}} \cdot \underbrace{\chi_i(g_j^{-1})}_{\substack{\text{alg. int.} \\ \text{by 4.1}}}$$

$$\Rightarrow \frac{|G|}{n_i} \in \mathbb{Q} \text{ is an algebraic integer}$$

$$\Rightarrow \frac{|G|}{n_i} \in \mathbb{Z} \qquad \Rightarrow \qquad n_i \mid |G| \,. \qquad \#$$

<u>Example 8:</u> $G = GL_3(\mathbb{F}_2)$ is a simple group with $|G| = (2^3-1)(2^3-2)(2^3-2^2) = 168$
$= 2^3 \cdot 3 \cdot 7$.

G has 6 conjugacy classes (without proof here)

<u>Question:</u> can we compute $\chi(1)$ $\forall \chi \in \mathrm{Irr}(G)$?

<u>Solution:</u> (1) G simple non-abelian $\Rightarrow [G,G] = G$

$\Rightarrow \chi(1) \geq 2 \quad \forall \chi \in \mathrm{Irr}(G) \setminus \{1_G\}$

[Übung] (2) Exercise 18(c) Sheet 5:

G simple $\Rightarrow \chi(1) \neq 2 \quad \forall \chi \in \mathrm{Irr}(G)$

(3) Set $n_i := \chi_i(1) \quad \forall 1 \leq i \leq 6$.

$\Rightarrow 168 = n_1^2 + n_2^2 + n_3^2 + n_4^2 + n_5^2 + n_6^2$

(1)+(2) $\Rightarrow$ the possibilities are

$$\left.\begin{array}{cccccc} 1 & 2 & 4 & 5 & 6 & \cancel{9} \\ 1 & 2 & 3 & 3 & 8 & \cancel{9} \\ 1 & 2 & \cancel{5} & \cancel{5} & 7 & 8 \end{array}\right\} \; 9, 5 \nmid |G|$$

$$\left.\begin{array}{cccccc} 1 & \cancel{2} & 4 & 7 & 7 & 7 \end{array}\right\} \; \text{not possible by (2)}$$

$$\begin{array}{cccccc} 1 & 3 & 3 & 6 & 7 & 8 \end{array}$$

<u>Important current research topic:</u> find further arithmetic properties of the degrees of the irreducible characters.

E.g. the following conjecture is of particular interest:

Conjecture 4.5 [McKay, 1972] Status: open!

Let G be a finite group, $p \in \mathbb{P}$, and $P \in \mathrm{Syl}_p(G)$. Then

$$|\{\chi \in \mathrm{Irr}(G) \mid p \nmid \chi(1)\}| = |\{\chi \in \mathrm{Irr}(N_G(P)) \mid p \nmid \chi(1)\}|.$$

Note: Proved for soluble groups by Okuyama-Wajima.

Example 9:

$G = S_4$. Then $|\mathrm{Irr}(G)| = 5$ by Ex. 6.
with $\chi_1(1) = 1$, $\chi_2(1) = 1$, $\chi_3(1) = 2$, $\chi_4(1) = \chi_5(1) = 3$

(a) $p = 2$ yields $P \cong D_8$ with $N_G(P) = P$
By the Exercises $|\mathrm{Irr}(D_8)| = 5$ with character degrees $1, 1, 1, 1, 2$

(b) $p = 3$ yields $P \cong A_3$ with $N_G(P) \cong S_3$
Ex. 5 $\Rightarrow$ $|\mathrm{Irr}(S_3)| = 3$ with char. degrees $1, 1, 2$

$\Rightarrow$ The McKay Conjecture holds in both cases.

2. Burnside's vanishing theorem.

Definition 4.6: Let χ be a character of G. Then the centre of χ is $Z(\chi) := \{g \in G \mid |\chi(g)| = \chi(1)\}$

Example 15: $G = S_3$ has char. table by Ex. 5.

χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

$\Rightarrow$ $Z(\chi_1) = Z(\chi_2) = G$
$Z(\chi_3) = \{1_G\}$

Proposition 4.8 Let χ be a character of G. Then

(a) $Z(\chi) \trianglelefteq G$.

(b) $\chi|_{Z(\chi)} = \chi(1)\lambda$ for some linear character $\lambda \in \mathrm{Irr}(Z(\chi))$.

(c) $Z(\chi)/\ker(\chi)$ is a cyclic group

(d) $\chi \in \mathrm{Irr}(G) \Rightarrow Z(\chi)/\ker(\chi) = Z(G/\ker(\chi))$

Proof: Let ρ be a representation affording χ and set $n := \chi(1)$.

(a) Let $g \in Z(\chi)$: • Prop 2.2(h) $\Rightarrow$ $\chi(g) = \varepsilon_1 + \cdots + \varepsilon_n$ with $\varepsilon_1, \ldots, \varepsilon_n$ $o(g)$-th roots of unity

• (H): $|\chi(g)| = n$

So only possibility is that $\varepsilon_1 = \cdots = \varepsilon_n =: \varepsilon(g)$

$\Rightarrow \rho(g) = \varepsilon(g)\,\mathrm{Id}_V$

• Now if $g, h \in Z(\chi)$, then $\rho_V(gh^{-1}) = \rho_V(g)\rho_V(h)^{-1}$

$= \varepsilon(g)\varepsilon(h)^{-1}\mathrm{Id}_V$ (scalar matrix)

$\Rightarrow gh^{-1} \in Z(\chi)$

$\Rightarrow Z(\chi) \leq G$.

• Finally if $g \in Z(\chi)$ and $h \in G$, then

$$\rho_V(hgh^{-1}) = \rho_V(h)\varepsilon(g)\,\mathrm{Id}_V\,\rho_V(h)^{-1}$$
$$= \varepsilon(g)\,\mathrm{Id}_V = \rho_V(g) \quad \Rightarrow Z(\chi) \trianglelefteq G.$$

(b) The map $\lambda : Z(\chi) \longrightarrow \mathbb{C}^\times$, $g \mapsto \varepsilon(g)$ is a grp homomorphism

hence a linear character of $Z(\chi)$.

Moreover, clearly $\chi|_{Z(\chi)} = \chi(1)\lambda$ as claimed.

(c) By the 1st iso. theorem $\underset{Z(\chi)/\ker(\chi)}{\overset{\parallel}{Z(\chi)/\ker(\lambda)}} \cong \underbrace{\mathrm{Im}(\lambda)}_{\leq \mathbb{C}^\times}$.

Hence $Z(\chi)/\ker(\chi)$ is cyclic since it is a finite subgrp of $\mathbb{C}^\times$.

(d) By (a) $\forall g \in Z(\chi)$, $\rho_V(g) = \varepsilon(g)\, Id_V$ scalar matrix

$$\Rightarrow \rho_V(Z(\chi)) \leq Z(\rho_V(G))$$

Again by the 1st Iso theorem:

$$Z(\chi)/\ker(\chi) \cong \rho_V(Z(\chi)) \leq Z(\rho_V(G)) \cong Z(G/\ker\rho_V) = Z(G/\ker(\chi))$$

On the other hand, if $g\ker(\chi) \in Z(G/\ker(\chi))$, then by Schur's Lemma $\rho_V(g) = \varphi\, Id_V$ for some $\varphi \in \mathbb{C}^\times$

$$\Rightarrow g \in Z(\chi) \Rightarrow Z(G/\ker(\chi)) \leq Z(\chi)/\ker(\chi)$$

Corollary 4.9 $\bigcap_{\chi \in Irr(G)} Z(\chi) = Z(G)$

Proof: Exercise See Ex. Sheet 5

Remark: one can prove that $\chi(1) \mid |G : Z(\chi)| \ \forall \chi \in Irr(G)$

Remarks on field extensions: Let $m \geq 1$ be an integer and let φ_m be a primitive m-th root of unity in $\mathbb{C}$. Then:

- $L := \mathbb{Q}(\varphi_m)$ is the splitting field of $X^m - 1$, hence $L/\mathbb{Q}$ is a Galois extension.
- For $\sigma \in Gal(L/\mathbb{Q})$ we must have $\sigma(\varphi_m) = \varphi_m^k$ for some $k \in \mathbb{Z}$ with $\gcd(k, m) = 1$

- this defines an isomorphism

$$\mathrm{Gal}(L/\mathbb{Q}) \xrightarrow{\cong} (\mathbb{Z}/m\mathbb{Z})^\times$$

$\Rightarrow$ $\mathrm{Gal}(L/\mathbb{Q})$ is an abelian group.

Theorem 4.10 [Burnside]

Let $\chi \in \mathrm{Irr}(G)$ with $\chi(1) =: n$, and let C be a conjugacy class of G with $\gcd(n, |C|) = 1$. Let $g \in C$.
Then either $\chi(g) = 0$,
or $g \in Z(\chi)$ (i.e. $|\chi(g)| = n$).

<u>Proof</u>: $\gcd(n, |C|) = 1 \Rightarrow \exists u, v \in \mathbb{Z}$ s.t. $un + v|C| = 1$

Set $\alpha := \frac{1}{n}\chi(g) = \underbrace{\underset{\in \mathbb{Z}}{u}\underset{\text{alg. int.}}{\chi(g)} + \underset{\in \mathbb{Z}}{v}\underbrace{\frac{|C|}{n}\chi(g)}_{\text{alg. int. by §1}}}_{\Rightarrow \alpha \text{ algebraic integer.}}$

- If $g \in Z(\chi)$ we are done ✓
- Else $|\chi(g)| < n \Rightarrow |\alpha| < 1$.

Let $m = o(g)$. Since $\chi(g)$ is a sum of m-th roots of unity
$\Rightarrow \chi(g) \in \mathbb{Q}(\zeta_m)$

Therefore if $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$, we have

$\sigma(\chi(g))$ = sum of n m-th roots of unity

$\Rightarrow |\sigma(\chi(g))| \leq n$

$\Rightarrow |\sigma(\alpha)| \leq 1$

$\Rightarrow \left| \prod_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})} \sigma(\alpha) \right| < 1$ as $|\mathrm{Id}(\alpha)| = |\alpha| < 1$.

but this is the norm of the algebraic integer α
i.e. the constant term of the min. polynomial of α in
$\mathbb{Q}(\alpha)/\mathbb{Q}$ $\Rightarrow \alpha = 0 \Rightarrow \chi(g) = 0$. #

Corollary 4.11: In the situation of Thm 4.10 with
1. $\chi(1) = n > 1$
2. $C \neq \{1\}$
3. G is simple

Then $\chi(g) = 0$.

Proof: $\chi(g) \neq 0 \overset{\text{Thm 4.10}}{\Longrightarrow} g \in Z(\chi) \Rightarrow Z(\chi) \neq 1$

But $Z(\chi) \underset{\text{Prop 4.8(a)}}{\trianglelefteq} G$ and G is simple $\Rightarrow Z(\chi) = G$

So Prop 4.8(b) $\Rightarrow \chi$ is a sum of linear characters with $n > 1$ terms

$\Rightarrow \chi$ reducible ↯

#

Exercise 4.12: Let G be a finite cyclic group.
Let $S := \{g \in G \mid \langle g \rangle = G\}$. (set of generators).
If $\chi(g) \neq 0 \ \forall g \in S$, then

$$\sum_{g \in S} |\chi(g)|^2 \geq |S| .$$

Theorem 4.13 (Burnside's Vanishing Theorem).

Let $\chi \in \mathrm{Irr}(G)$ with $\chi(1) > 1$. Then $\exists g \in G$ with $\chi(g) = 0$.

Proof: Define an equivalence relation on G as follows:
For $g_1, g_2 \in G$: $g_1 \sim g_2 \iff \langle g_1 \rangle = \langle g_2 \rangle$
(Clear: reflexiv, symmetric, transitive.)

Assume now that $\chi(g) \neq 0 \ \forall g \in G$.
Let $Z \leq G$ be a cyclic subgrp and let $S := \{g \in Z \mid \langle g \rangle = Z\}$

moreover: S is an equiv class of $\sim$

Restricting χ to Z, Ex 4.12 $\Rightarrow \sum_{g \in S} |\chi(g)|^2 \geq |S|$

Letting Z running over all cyclic subgrps of G, we get:

$$\sum_{g\in G} |\chi(g)|^2 = \sum_{S\in G/\sim} \sum_{g\in S} |\chi(g)|^2 \geq |G| \quad \text{and since } \{1\}\in G/\sim$$

$$\sum_{g\in G\setminus\{1\}} |\chi(g)|^2 \geq |G| - 1$$

$$\Rightarrow \quad |G| = \sum_{g\in G} \chi(g)\overline{\chi(g)} \geq |G| - 1 + \underbrace{\chi(1)^2}_{>1} > |G| \quad ⚡$$

#

A stronger result whose proof requires the classification of finite simple groups is the following:

<u>[Malle - Navarro - Olsson, 2000]</u> Let $\chi \in \mathrm{Irr}(G)$ with $\chi(1) > 1$. Then $\exists g \in G$ of prime power order s.t. $\chi(g) = 0$.

3. Burnside's $p^a q^b$ - Theorem

We now see one of the most famous application of Character Theory to the structure of finite simple groups: the proof of Burnside's $p^a q^b$-Thm.

<u>Example 10:</u>

In the Einf. in die Algebra we have seen that:

(a) G finite group with $|G| = p^2$ for some prime $p \in \mathbb{P}$ $\Rightarrow$ G is abelian.

Here is another proof using character theory:

Let $\chi \in \mathrm{Irr}(G)$ $\underset{\text{Cor 4.4}}{\Rightarrow}$ $\chi(1) \mid |G|$ $\Rightarrow$ $\chi(1) \in \{1, p, p^2\}$

But then $p^2 = |G| = \sum_{\chi\in\mathrm{Irr}(G)} \chi(1)^2 = \underbrace{1_G(1)^2}_{=1} + \sum_{\substack{\chi\in\mathrm{Irr}(G)\\ \chi\neq 1_G}} \chi(1)^2$

$\Rightarrow$ any $\chi \in \mathrm{Irr}(G)\setminus\{1_G\}$ is linear

$\overset{\text{Cor. 3.6}}{\Rightarrow}$ G abelian #

(b) G p-group ($p \in \mathbb{P}$) $\Rightarrow$ G soluble group

There is another proof using character theory:

Induction on $|G|$: • if $|G| = p$, $|G| = p^2$ ✓ ((a))

• So assume $p^n = |G| \geq p^3$.

$\chi(1) \in \{1, p, p^2, p^3, \dots\}$ $\forall \chi \in \mathrm{Irr}(G)$.

As $\sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2 = 1 + \underbrace{\sum_{\substack{\chi \in \mathrm{Irr}(G) \\ \chi \neq 1_G}} \chi(1)^2}_{\vdots\, p^n - 1} = p^n$

there are at least p linear characters in $\mathrm{Irr}(G)$

$\overset{3.6}{\Longrightarrow} [G,G] < G \Longrightarrow [G,G]$ soluble by induction hyp. and so is $G/[G,G]$

$\Longrightarrow$ G is soluble (Sandwich principle)

Theorem 4.14: Let G be a finite non-abelian simple group, and let $C \in C(G)$ be a conjugacy class of prime power order,
(Burnside)
i.e. $|C| = p^a$ for some $p \in \mathbb{P}$ and some $a \in \mathbb{N}_0$.
Then $C = \{1\}$.

Proof: Assume $C \neq \{1\}$, and let $g \in C$ ($g \neq 1$)

Let $\chi \in \mathrm{Irr}(G) \setminus \{1_G\}$.

As G is simple non-abelian $[G,G] = G \overset{\text{Cor 3.6}}{\Longrightarrow} \chi(1) > 1$

$\Longrightarrow$ either $p \mid \chi(1)$ or $\underbrace{(\chi(1), |C|) = 1}$

$\Downarrow$ Cor 4.11

$\chi(g) = 0$

2^{nd} Orth. Relations yield

$$0 = 1 + \sum_{\chi \in \mathrm{Irr}(G) \setminus \{1_G\}} \chi(g)\chi(1)$$

$$= 1 + \sum_{\substack{\chi \in \mathrm{Irr}(G) \setminus \{1_G\} \\ \chi(g) \neq 0}} \chi(g)\underbrace{\chi(1)}_{p \mid \chi(1)}$$

So either the sum is $\emptyset$ and $0 = 1$ ↯

or $-\frac{1}{p} = \sum_{\substack{\chi \in \mathrm{Irr}(G) \setminus \{1_G\} \\ \chi(g) \neq 0}} \chi(g)\frac{\chi(1)}{p}$ algebraic integer by Lemma 4.1 ↯ #

Theorem 4.15 [Burnside's p^aq^b-Theorem, "simple" version]

Let $p, q \in \mathbb{P}$, and let $a, b \in \mathbb{N}_0$ with $a+b \geq 2$.
If G is a group of order $p^a q^b$, then G is not simple.

Proof:

- 1st assume that either $a=0$, or $b=0$, then G is a q-group or a p-group (resp.) with ~~$|G| \geq$~~ q^2 (resp p^2) $\mid |G|$
  $\overset{\text{Ex 1(b)}}{\Longrightarrow}$ G is soluble $\Rightarrow \exists \{1\} \neq N \ntrianglelefteq G$ with $|G:N| = q$, resp. p.
  $\Rightarrow$ G not simple.
- Now assume that $a \geq 1$, $b \geq 1$. Let $Q \in Syl_q(G)$ $(|Q| = q^b)$. Because Q is a q-group, $Z(Q) \neq \{1\}$ so let $g \in Z(Q) \setminus \{1\}$.
  Then $Q \leq C_G(g) \overset{\text{class eq.}}{\Longrightarrow} |[g]| = |G : C_G(g)| = p^r$ for some $r \leq a$.
  If G were simple, then G would be non-abelian as $a+b \geq 2$
  $\overset{\text{Thm 4.14}}{\Longrightarrow}$ $[g] = \{1\}$ $(\Rightarrow g \in Z(G))$ $\lightning$ $g \neq 1$.

#

Corollary 4.16: Every group of order $p^a q^b$ is soluble.

Proof: Induction on $a+b$:

- Clear if $a+b \leq 1$
- Assume $a+b \geq 2$ and let G be a finite grp s.t. $|G| = p^a q^b$
  Burnside $\Rightarrow \exists \{1\} \neq H \ntrianglelefteq G$
  and both $|H|, |G/H| \lneq p^a q^b$
  $\Rightarrow H, G/H$ soluble by the induction hypothesis
  $\Rightarrow$ G is soluble as well by the sandwich principle. #