Group representations 1

Burnside's p,q - theorem

May 17, 2021

Burnside's theorem

Theorem

Let $p, q \in \mathbb{P}$, $a, b \in \mathbb{N}_0$. Then every finite group of order $p^a q^b$ is solvable.

Burnside's theorem

Theorem

Let $p, q \in \mathbb{P}$, $a, b \in \mathbb{N}_0$. Then every finite group of order $p^a q^b$ is solvable.

Remark

This theorem was proved by William Burnside in 1904 using the representation theory of groups. Proofs avoiding representation theory of groups were published in 1970's.

The key proposition

Proposition

Let G be a finite group, $C \subseteq G$ a conjugacy class of G, $\psi\colon G \to \mathrm{GL}(d, \mathbb{C})$ an irreducible matrix representation of G over $\mathbb{C}$.

The key proposition

Proposition

Let G be a finite group, $C \subseteq G$ a conjugacy class of G, $\psi\colon G \to \mathrm{GL}(d,\mathbb{C})$ an irreducible matrix representation of G over $\mathbb{C}$. Assume $h := |C|$ is coprime to d. Then either $\chi_\psi(C) = 0$ or there exists $\lambda \in \mathbb{C}^*$ such that $\psi(g) = \lambda E$ for every $g \in C$.

Remark

Note that if $\psi(g) = \lambda E$, then for every $x \in G$ we have $\psi(xgx^{-1}) = \psi(x)(\lambda E)\psi(x)^{-1} = \lambda E$.

In the proof we will denote $K = \mathbb{Q}[e^{\frac{2\pi \mathrm{i}}{|G|}}]$ and $\mathbb{Z}_K$ is the ring of all algebraic integers in K. Recall that $\chi_\psi(h) \in \mathbb{Z}_K$ for every $h \in G$. We will also need the fact that $\lambda_C^\psi := \frac{h}{d}\chi_\psi(g)$, where $g \in C$, is an element from $\mathbb{Z}_K$.

proof of the proposition, part 1

The assumption $\mathrm{GCD}(d, h) = 1$ gives there exist $k, j \in \mathbb{Z}$ such that $kh + jd = 1$.
Recall (from the last lecture) that for every $g \in C$ we have

$$\chi_\psi(g) \in \mathbb{Z}_K, \frac{h}{d}\chi_\psi(g) \in \mathbb{Z}_K\,.$$

It follows that $k\frac{h}{d}\chi_\psi(g) + j\chi_\psi(g) = \frac{kh+jd}{d}\chi_\psi(g) = \frac{\chi_\psi(g)}{d} \in \mathbb{Z}_K$.
Recall that every element of $\mathrm{GL}(d, \mathbb{C})$ of finite order is diagonalizable. For every $g \in G$ the matrix $\psi(g)$ is similar to $\mathrm{diag}(\lambda_1, \ldots, \lambda_d)$, therefore

$$|\chi_\psi(g)| = |\sum_{i=1}^{d} \lambda_i| \leq \sum_{i=1}^{d} |\lambda_i| = d$$

Note that the equality occurs if and only if
$\lambda_1 = \lambda_2 = \cdots = \lambda_d = \lambda$ and in this case $\psi(g) = \lambda E$.
Therefore our proposition can be stated as: If $g \in C$ satisfies $|\frac{\chi_\psi(g)}{d}| < 1$, then $\chi_\psi(g) = 0$.

proof of the proposition, part 2

Note that $\mathbb{Q} \subseteq K$ is a Galois extension, let Γ be its Galois group.
Note that for every $\gamma \in \Gamma$, $\gamma(\frac{\chi_\psi(g)}{d}) \in \mathbb{Z}_K$ for every $g \in C$.
We claim $|\frac{\chi_\psi(g)}{d}| < 1 \Rightarrow |\gamma(\frac{\chi_\psi(g)}{d})| < 1$ for every $\gamma \in \Gamma$.
Recall that $\chi_\psi(g) = \lambda_1 + \cdots + \lambda_d$, where $\lambda_i^{o(g)} = 1$ for every $1 \leq i \leq d$, so in particular, $\lambda_i \in K$. So $\gamma(\lambda_i)$ is defined for every $\gamma \in \Gamma$ and since $\gamma(\lambda_i)^{o(g)} = 1$, we get $|\gamma(\lambda_i)| = 1$.
Now if $|\frac{\chi_\psi(g)}{d}| < 1$, then there are i, j such that $\lambda_i \neq \lambda_j$, hence also $\gamma(\lambda_i) \neq \gamma(\lambda_j)$ and also

$$|\gamma(\frac{\chi_\psi(g)}{d})| = \frac{|\sum_{i=1}^{d} \gamma(\lambda_i))|}{d} < 1$$

proof of the proposition, part 3

Consider $\beta := \prod_{\gamma \in \Gamma} \gamma(\frac{\chi_\psi(g)}{d})$. Note that

- $\beta \in \mathbb{Z}_K$: This follows from $\frac{\chi_\psi(g)}{d} \in \mathbb{Z}_K$, $\gamma(\mathbb{Z}_K) \subseteq \mathbb{Z}_K$ for every $\gamma \in \Gamma$ and $\mathbb{Z}_K$ is a subring of K.
- $\beta \in \mathbb{Q}$: Since $\gamma(\beta) = \beta$ for every $\gamma \in \Gamma$
- If $|\frac{\chi_\psi(g)}{d}| < 1$, then $|\beta| < 1$.

Since $\mathbb{Z}_K \cap \mathbb{Q} = \mathbb{Z}$ we get that $\beta \in \mathbb{Z}$. The only integer with absolute value < 1 is zero. This proves what we want: If $|\frac{\chi_\psi(g)}{d}| < 1$ then $\chi_\psi(g) = 0$.

Which groups are not simple

Lemma

Let G be a finite group which is not abelian. Suppose that $C \subseteq G$ is a conjugacy class of G, $C \neq \{1_G\}$ and $|C| = p^t$ for some $p \in \mathbb{P}$ and $t \in \mathbb{N}_0$. Then G is not simple.

proof: Assume G is a finite simple group which is not abelian, let $\psi_1, \ldots, \psi_k$ be a complete list of irreducible matrix representations of G over $\mathbb{C}$.
We write $\chi_i := \chi_{\psi_i}$ and let $d_i := \chi_i(1_G)$ be the degree of ψ_i.
Further we assume that ψ_1 is the trivial representation of G over $\mathbb{C}$, that is, $\psi_1(g) = (1) \in \mathrm{GL}(1, \mathbb{C})$ for every $g \in G$.
Observe that every simple non-abelian group is perfect, that is $[G, G] = G$. It follows that G has only one matrix representation of degree one, namely ψ_1. It follows $d_2, \ldots, d_k \geq 2$.

proof of the lemma, part 2

Since G is simple, $\operatorname{Ker} \psi_i$ is either $\{1_G\}$ or G. If $\operatorname{Ker} \psi_i = G$, then $\psi_i(g) = E$ for every $g \in G$ and ψ_i is equivalent to a direct sum of d_i copies of the trivial representation. For $i \geq 2$ is $d_i \geq 2$ and such a representation is not irreducible. Thus we get
ψ_i is injective for every $i \geq 2$.

proof of the lemma, part 3

For $2 \leq i \leq k$ let $Z_i := \{\lambda E_{d_i} \mid \lambda \in \mathbb{C}^*\} \leq \mathrm{GL}(d_i, \mathbb{C})$.
Note that Z_i is a normal subgroup of $\mathrm{GL}(d_i, \mathbb{C})$, hence $\psi_i^{-1}(Z_i)$ is a normal subgroup of G. Since we assume G simple, the only possibilities for $\psi_i^{-1}(Z_i)$ are $\{1_G\}$ and G.
Recall for $i \geq 2$ we know ψ_i is injective. Therefore $\psi_i^{-1}(Z_i) = G$ implies that ψ_i is an embedding of G into a commutative group Z_i. This is not possible - we assume G not abelian.
The important conclusion is that for $i \geq 2$ the matrix $\psi_i(g)$ is not in Z_i unless $g = 1$.
At this point we may apply the Proposition. If $i \geq 2$, $C \neq \{1_G\}$ is a conjugacy class of size p^t, $p \in \mathbb{P}$ and $t \in \mathbb{N}_0$ and $p \nmid d_i$, then $\chi_i(g) = 0$ for every $g \in C$.

proof of the lemma, part 4

For every $1 \leq i \leq k$ let $\varphi_i \in \mathrm{Rep}_{\mathbb{C}}(G)$ be the representation corresponding to the matrix representation ψ_i. We know how the decomposition of the regular representation looks like:

$$\mathrm{reg}_{\mathbb{C}}(G) \simeq \varphi_1 \oplus \overbrace{\varphi_2 \oplus \cdots \oplus \varphi_2}^{d_2} \oplus \cdots \oplus \overbrace{\varphi_k \oplus \cdots \oplus \varphi_k}^{d_k}.$$

We also computed character of the regular representation

$$\chi_{\mathrm{reg}_{\mathbb{C}}(G)}(1_G) = |G|, \chi_{\mathrm{reg}_{\mathbb{C}}}(g) = 0, g \neq 1_G$$

Again we write χ_{reg} instead of $\chi_{\mathrm{reg}_{\mathbb{C}}(G)}$

proof of the lemma, part 5

Assume $\{1_G\} \neq C$ is a conjugacy class of size p^t for some $p \in \mathbb{P}$ and some $t \in \mathbb{N}_0$. Let $g \in C$. Recall we know $\chi_i(g) = 0$ if $i \geq 2$ and $p \nmid d_i$.
Since equivalent representations have equal characters we get

$$\chi_{\text{reg}} = \sum_{i=1}^{k} d_i \chi_i$$

Evaluating these functions in $g \in C$ gives
$0 = 1 + \sum_{2 \leq i \leq k, p | d_i} d_i \chi_i(g)$. Therefore

$$-\frac{1}{p} = \sum_{2 \leq i \leq k, p | d_i} \frac{d_i}{p} \chi_i(g)\,.$$

The element on the RHS of the last equality is in $\mathbb{Z}_K$ while the element on the LHS of this equality is in $\mathbb{Q}$. Again $\mathbb{Q} \cap \mathbb{Z}_K = \mathbb{Z}$ gives $\frac{-1}{p} \in \mathbb{Z}$ which is not possible.

Burnside's theorem

Theorem

Let $p, q \in \mathbb{P}$, $a, b \in \mathbb{N}_0$ and let G be a finite group of order $p^a q^b$. Then G is not simple unless it is cyclic of prime order.

Proof.

Recall that an abelian group is simple if and only if it is a group of prime order. Assume G simple and not commutative, $|G| = p^a q^b$. Recall that any p-group has a non-trivial center, so necessarily $p \neq q$ and $a, b > 0$.
Let H be a Sylow q-subgoup of G. That is, $H \leq G$, $|H| = q^b > 1$. Since $Z(H) \neq 1$ there exists $1 \neq h \in Z(H)$. Let C be the conjugacy class containing h. Then

$$|C| = \frac{|G|}{|\{g \in G \mid ghg^{-1} = h\}|}.$$

Since $h \in Z(H)$, $H \subseteq \{g \in G \mid ghg^{-1} = h\}$, so the order of the stabilizer $\{g \in G \mid ghg^{-1} = h\}$ is a multiple of q^b. It follows that $|C| = p^{a'}$ for some $0 \leq a' \leq a$.

Promised p, q - theorem

Theorem

Let $p, q \in \mathbb{P}$, $a, b \in \mathbb{N}_0$. Then every finite group of order $p^a q^b$ is solvable.

Proof.

Assume there are primes p, q such that there exists a group of order $p^a q^b$ which is not solvable. Let G be such a group of smallest possible order.
Since every abelian group is solvable, G is not abelian. By the previous theorem G is not simple, so it contains a nontrivial normal subgroup N. Since the order of G is as small as possible N and G/N have to be solvable (note if $|G| = p^a q^b$, then $|N| = p^{a_1} q^{b_1}$ and $|G/N| = p^{a-a_1} q^{b-b_1}$).
But the class of solvable groups is closed under extensions, so if N and G/N are solvable, G is solvable as well. $\square$

End

Thanks for your attention.