Burnside's theorem

is also known as Burnside's p,q theorem. It says that if $p,q \in \mathbb{P}$, $a,b \in \mathbb{N}_0$, then every finite group of order $p^a q^b$ is solvable. In 1904 Burnside proved this theorem using representation theory of finite groups. Proofs avoiding the use of representation theory were published in 1970's.

The goal of this lecture is to present a proof (of course based on the results we met during the course).

Proposition Let G be a finite group, C a conjugacy class of G, $\varphi: G \to GL(d, \mathbb{C})$ an irreducible matrix representation of G over $\mathbb{C}$. Assume $h := |C|$ is relatively prime to d. Then either

$\exists \lambda \in \mathbb{C}^*$ such that $\varphi(g) = \lambda E$ for all $g \in C$

or $\chi_\varphi(g) = 0 \quad \forall g \in C$.

Proof:
- Note that if $\varphi(g) = \lambda E$ for some $g \in C$, then $\varphi(hgh^{-1}) = \varphi(h)(\lambda E)\varphi(h)^{-1} = \lambda E$, so $\varphi(c) = \lambda E \ \forall c \in C$.
- Similarly if $\chi_\varphi(g) = 0$ for some $g \in C$, then $\chi_\varphi(c) = 0$ for all $c \in C$ because characters are constant on conjugacy classes.
- Recall $A := \{\alpha \in \mathbb{C} \mid \exists h \in \mathbb{Z}[x] \text{ monic such that } h(\alpha) = 0\}$ is a subring of $\mathbb{C}$.

We know $\chi_\varphi(g) \in \mathbb{A}$ for every $g \in G$ and $\frac{h}{d}\chi_\varphi(g) \in \mathbb{A}$ for every $g \in C$ (see pages 2,3 in the notes on the degree theorem from April 15)

- We assume $GCD(h,d)=1$, i.e., there are $k, j \in \mathbb{Z}$ such that $kh + jd = 1$. For any $g \in C$ we have $\chi_\varphi(g) \in \mathbb{A}$, $\frac{h}{d}\chi_\varphi(g) \in \mathbb{A}$, hence also

$$k\,h\,\frac{\chi_\varphi(g)}{d} + j\,\chi_\varphi(g) = (kh + jd)\,\frac{\chi_\varphi(g)}{d} = \frac{\chi_\varphi(g)}{d} \in \mathbb{A}$$

- Recall there are $\lambda_1, \lambda_2, \dots, \lambda_d \in \mathbb{C}$ such that $\varphi(g)$ is similar to $\operatorname{diag}(\lambda_1, \dots, \lambda_d)$
(Imagine the Jordan canonical form of $\varphi(g)$ and note that it has to be diagonal since $\varphi(g)^{o(g)} = E$)

- Therefore $|\chi_\varphi(g)| \le |\lambda_1| + |\lambda_2| + \dots + |\lambda_d| \le d$
(observe $\lambda_i^{o(g)} = 1 \;\forall\, 1 \le i \le d$, so $|\lambda_i| = 1$)
We already know this but what is important here:
if $|\chi_\varphi(g)| = d$, then $\lambda_1 = \lambda_2 = \dots = \lambda_d$; then $\varphi(g)$ is similar to $\operatorname{diag}(\lambda, \lambda, \dots, \lambda)$ for some $\lambda \in \mathbb{C}^*$ and therefore $\varphi(g) = \lambda E$ for some $\lambda \in \mathbb{C}^*$

- It is sufficient to prove $\forall g \in C \quad \left|\frac{\chi_\varphi(g)}{d}\right| < 1 \Rightarrow \chi_\varphi(g) = 0$

- Let $n = o(g)$, $\omega = e^{\frac{2\pi i}{n}}$. Note that $\mathbb{Q}[e^{\frac{2\pi i}{n}}] = \mathbb{Q}[\omega]$ is a splitting field of $x^n - 1$, hence $\mathbb{Q} \subseteq \mathbb{Q}[\omega]$ is a Galois extension of fields. Let $g \in C$.

Note $\frac{\chi_\varphi(g)}{d} \in \mathbb{Q}[\omega] \cap \mathbb{A}$ (which is by the way $\mathbb{Z}[\omega]$)

If $\sigma \in Gal(\mathbb{Q}[\omega] | \mathbb{Q}) = Aut(\mathbb{Q}[\omega])$,

then $\sigma\left(\frac{\chi_\varphi(g)}{d}\right) = \sigma\left(\frac{\lambda_1 + \lambda_2 + \dots + \lambda_d}{d}\right) = \frac{\sigma(\lambda_1) + \dots + \sigma(\lambda_d)}{d}$.

If $\left|\frac{\chi_\varphi(g)}{d}\right| < 1$, then $\lambda_1, \lambda_2, \dots, \lambda_d$ are not all equal

hence $\sigma(\lambda_1), \dots, \sigma(\lambda_d)$ are not all equal and since

$\sigma(\lambda_i)^n = \sigma(\lambda_i^n) = 1$, $|\sigma(\lambda_i)| = 1 \quad \forall\, 1 \le i \le d$;

we get $\left|\sigma\left(\frac{\chi_\varphi(g)}{d}\right)\right| < 1$

- Consider $\beta := \prod_{\sigma \in Gal(\mathbb{Q}[\omega]|\mathbb{Q})} \sigma\left(\frac{\chi_\varphi(g)}{d}\right)$ (the product of all Galois conjugates of $\frac{\chi_\varphi(g)}{d}$)

Then: • $\beta \in \mathbb{A}$: if $h\left(\frac{\chi_\varphi(g)}{d}\right) = 0$ for $h \in \mathbb{Z}[x]$ monic,

then also $h\left(\sigma\left(\frac{\chi_\varphi(g)}{d}\right)\right) = 0$ for $\sigma \in Gal(\mathbb{Q}[\omega]|\mathbb{Q})$

• $\beta \in \mathbb{Q}$ since $\sigma(\beta) = \beta$ for every $\sigma \in Gal(\mathbb{Q}[\omega]|\mathbb{Q})$

• so $\beta \in \mathbb{A} \cap \mathbb{Q} = \mathbb{Z}$ (page 1 fact makes from April 15)

- If $\left|\frac{\chi_\varphi(g)}{d}\right| < 1$, then also $|\beta| < 1$.

  The only integer with abs. value < 1 is 0.
  Therefore $\beta = 0$ and also $\chi_\varphi(g) = 0$
  for some (any) $g \in C$ □

Lemma Let G be a finite non-abelian group.
Suppose G has a conjugacy class $C \neq \{1_G\}$
such that $|C| = p^t$, with p prime and $t \geq 0$.
Then G is not simple.

Proof: Assume G is simple and not abelian,
$\varphi_1, \varphi_2, \dots, \varphi_k$ be a complete list of irreducible reps
of G over $\mathbb{C}$ up to equivalence.
Let $\chi_i := \chi_{\varphi_i}$, $d_i := \chi_i(1_G)$ for $1 \leq i \leq k$
Assume φ_1 is the trivial rep of G over $\mathbb{C}$.

- Since G is simple non-abelian, $[G,G] = G$
  and it follows that φ_1 is "the only" rep. of G over $\mathbb{C}$
  of degree 1, that is, $d_2, \dots, d_k \geq 2$.
- For $2 \leq i \leq k$ $\ker \varphi_i \trianglelefteq G$, so either $\ker \varphi_i = 1$ or
  $\ker \varphi_i = G$. The later implies φ_i is equivalent
  to a direct sum of d_i copies of φ_1 which is not possible
  if φ_i is irreducible. Hence $\varphi_2, \dots, \varphi_k$ are all injective

- Consider $\varphi_i : G \to GL(d_i, \mathbb{C})$ for $i \geq 2$ and $Z_i := \{\lambda E_{d_i} \mid \lambda \in \mathbb{C}^*\}$ (we have seen in exercises $Z_i = Z(GL(d_i, \mathbb{C}))$ but it is not needed here)

  Since $Z_i \trianglelefteq GL(d_i, \mathbb{C})$, $\varphi_i^{-1}(Z_i) \trianglelefteq G$.

  Hence either $\varphi_i^{-1}(Z_i) = \{1\}$ or $\varphi_i^{-1}(Z_i) = G$.

  Again, $\varphi_i^{-1}(Z_i) = G$ would imply $G \xhookrightarrow{\varphi_i} Z_i$, but it is not possible, since $Z_i \simeq \mathbb{C}^*$ is commutative

  Therefore, if $\varphi_i(g) \in Z_i$, then $g = 1_G$.

- Now apply the Proposition: If $i \geq 2$, $p \in \mathbb{P}$, $C \neq \{1_G\}$ $|C| = p^t$ and $p \nmid d_i$ then $|C|$ and d_i are coprime, so by the proposition and the previous paragraph, $\chi_i(g) = 0 \ \forall g \in C$

- Let $reg : G \to GL(|G|, \mathbb{C})$ be the regular representation of G over $\mathbb{C}$. We know that reg is equivalent to $\varphi_1 \oplus \underbrace{\varphi_2 \oplus \cdots \oplus \varphi_2}_{d_2} \oplus \cdots \oplus \underbrace{\varphi_k \oplus \cdots \oplus \varphi_k}_{d_k}$

Recall $\chi_{reg}(x) = \begin{cases} |G| & \text{if } x = 1_G \\ 0 & \text{if } x \neq 1_G \end{cases}$

Equivalent reps have equal characters: $\chi_{reg} = \sum_{i=1}^{k} d_i \chi_i$

If $g \neq 1_G$ $\quad 0 = \chi_{reg}(g) = 1 + \sum_{i=2}^{k} d_i \chi_i(g)$

$d_1 \chi_1(g)$

Now assume $1_G \neq g \in C$, where C is a conjugacy class of size p^t, where $p \in \mathbb{P}$, $t \geq 0$ (note $t > 0$ since $Z(G) = 1$)

if d_i is coprime to p, then $\chi_i(g) = 0$ (for $i \geq 2$).

We get $0 = 1 + \sum_{\substack{2 \leq i \leq k \\ p \nmid d_i}} d_i \chi_i(g)$, and

$-1/p = \sum_{\substack{2 \leq i \leq k \\ p \nmid d_i}} \frac{d_i}{p} \chi_i(g)$. On the right hand side, we have an element from A: $\frac{d_i}{p} \in \mathbb{Z} \subseteq A$, $\chi_i(g) \in A$ and A is a subring of $\mathbb{C}$.

The celebrated equation $\mathbb{Q} \cap A = \mathbb{Z}$ gives $-1/p \in \mathbb{Z}$ which is not possible. So if G is simple and non-abelian, the size of a conjugacy class $\{1\} \neq C \subseteq G$ of prime power order does not exist in G $\square$

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

Proof: Assume G is simple non abelian of order $p^a q^b$.

If $b = 0$ then G is a p-group, so it has a nontrivial center. Then G cannot be simple non-abelian.

Similarly $a = 0$ cannot hold.

Let $H \leq G$ be a Sylow-q-subgroup of G.

So $|H| = q^b > 1$. $Z(H) \neq 1$, let $1 \neq g \in Z(H)$

The "normalizer" of g $N_G(g) := \{x \in G \mid xgx^{-1} = g\}$ contains H (because $g \in Z(H)$).

Let $C := \{hgh^{-1} \mid h \in G\}$ be the conjugacy class of G containing g. Then $|C| = [G : N_G(g)]$

$= \frac{|G|}{|N_G(g)|} \mid \frac{|G|}{|H|}$. That is, $|C| = p^{a'}$ for some $0 \leq a' \leq a$. But then C is a conjugacy class $\neq \{1_G\}$ of prime-power size, which is not possible if G is simple non-abelian. $\square$

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

Proof: For given primes p, q consider a group G of smallest posible order of the form $p^a q^b$ which is not solvable.

Then G is not abelian, so by the theorem, G is not simple. Let $1 \neq N \trianglelefteq G$. Then $|N| = p^{a_1} q^{b_1}$, $|G/N| = p^{a_2} q^{b_2}$. The "minimality assumption" on G implies N, G/N are solvable. Since the class of solvable groups is closed under extensions N, G/N solvable $\Rightarrow$ G solvable, a contradiction. □

Remark: Much deeper result on finite groups whose proof uses R.G. is the Feit-Thompson theorem (also odd order theorem):

Every finite group of odd order is solvable.

The original proof published in 1962 was 255 pages long. Since then some simplifications have been done but the proof is still based on theory of characters.

Fully formal proof checked by a computer theorem prover Coq was announced in 2012.