Solvability of groups of order $p^a q^b$

Our main goal is to prove the celebrated Burnside's theorem (1904) as one of applications of character theory. Some purely group-theoretic proof was found approximately 70 years later.

Theorem (Burnside). Let $|G| = p^{\alpha} q^{\beta}$ where p, q are primes, $\alpha, \beta \geq 0$. Then G is solvable.

When $p = q$ it is already known but for completeness prove

Lemma 1. Any p-group is solvable.

Proof
By induction on the order $|G| = p^{\alpha}$. If $|G| = p$ then G is cyclic.
$|G| = p^{\alpha}, \alpha > 1$ and G then is non-abelian, then its center $Z(G)$ is proper subgroup of G, $G / Z(G)$ is solvable by inductive hypothesis, and $Z(G)$ is solvable, hence G is solvable.

Now we need several facts about characters.

Lemma 2. Let $\varphi : G \to GL(n, \mathbb{C})$ be a representation of a finite group G with the character χ. Then for any $g \in G$, $|\chi(g)| \leq \chi(1) = n.$ Moreover $|\chi(g)| = n.$ if and only if $\varphi(g) = \lambda E, \lambda \in \mathbb{C}^*$.

Proof. $\chi(g) = \sum_{k=1}^{n} \lambda_k, \Rightarrow |\chi(g)| \leq \sum_{k=1}^{n} |\lambda_k| = n$ where λ_k are characterisnic roots of $\varphi(g),$ *so* $\lambda_k^{|g|} = 1$ and equality holds only if $\lambda_1 = \ldots = \lambda_n = \lambda$, say. It means that $\varphi(g) = \lambda E$.

Lemma 3. Let χ be an irreducible complex character of G, K is some conjugate class of G with $(|K|, \chi(1)) = 1$ and $x \in K$. Then $\chi(g) = 0$ *or* $|\chi(g)| = n.$.
Proof. As $|K|, \chi(1)$ are coprime, there are some integers $u, v :$ $u|K| + v\chi(1)) = 1$. Suppose $\chi(g) \neq 0$, then multiply the equality with $\dfrac{\chi(g)}{\chi(1)}$:

$$u, v : \frac{u|K|\chi(x)}{\chi(1)} + v\chi(x) = \frac{\chi(x)}{\chi(1)}.$$

The left side of this equality is an algebraic integer, by lemmas 3 and 5 of the proof of the theorem 4 of previous lecture, so $z = \dfrac{\chi(g)}{\chi(1)}$ is algebraic integer. Therefore, for any automorphism α of the Galois group of the field $\chi(g) = \sum_{k=1}^{n} \lambda_k \in \mathbb{Q}(\sqrt[|G|]{1})$, $\alpha(z)$ - algebraic conjugate of z – is algebraic integer, and if $z_1 = z, \ldots, z_m$ are all algebraic conjugate of z, then all $|z_i| \leq 1,\ i = 1, \ldots, m$. Its norm $N(z) = \prod_{i=1}^{m} z_i$ is invariant under all field automorphisms over Q and hence is both rational and algebraic integer, so $N(z) = 0 or \pm 1$. The case $N(z) = 0$ was excluded, then $N(z) = \pm 1 \Rightarrow |z| = 1 \Rightarrow |\chi(g)| = n$, q.e.d.

Lemma 4. If G has a conjugate class $K \neq \{1\}$ such that $|K| = p^s$, $s \geq 0$ for some prime p, then G is not simple.

Proof. Take some $x \in K$. If $s = 0$, then $x \in Z(G) \triangleleft G$ and G is not simple. Then $s \geq 1$.

Let $\{\chi_1 = 1_G, \ldots, \chi_r\}$ be all irreducible characters of G; we may arrange $\chi_1, \ldots, \chi_r$ so that $p \nmid \chi_j(1),\ 2 \leq j \leq l,\ p \mid \chi_j(1),\ l+1 \leq j \leq r$.

For $2 \leq j \leq l, (p^s, \chi_j(1)) = 1 \Rightarrow \quad \chi(x) = 0 \ or\ |\chi(x)| = n$, by lemms 3. But $|\chi_j(x)| = n$ means (by lemma 2) that $x \in Z(G) \triangleleft G$, so G is not simple. It remains that $\chi_j(x) = 0 \ \ for\ j = 1, \ldots, l$.

Now $\chi_j(x) = pm_j \ \ for\ j = l+1, \ldots, r$.

By the orthogonality relation, we get

$$0 = 1 + \sum_{j=l+1}^{r} \chi_j(1)\chi_j(x) = 1 + \sum_{j=l+1}^{r} pm_j\chi_j(x). \ (*)$$

The number $\beta = \sum_{j=l+1}^{r} m_j\chi_j(x)$ is algebraic integer; from (*) we have $\beta = -\frac{1}{p}$ both rational integer fnd not integer. This contradiction proves that G is not simple. Q.e.d.

Proof of the theorem. We can use induction on $|G| = p^\alpha q^\beta$. It is sufficient to prove that G is not simple: if $\exists N,\ 1 < N \triangleleft G$ then $N \triangleleft G,\ G/N$ are solvable by inductive hypothesis hence G is solvable.

Let $P \in Syl_p(G)$ and $x \in Z(P) \Rightarrow C_G(x) \geq P \Rightarrow |K| = \frac{|G|}{|C_G(x)|} = q^c,\ c \leq b$, where K is the conjugate class containing x. By lemma 4, G is not simple, and the theorem is proved.