Group representations 1

Elementary results on finite groups proved via representation theory

May 18, 2021

Every group of order p^2 is abelian

Proposition

If $p \in \mathbb{P}$, then every group of order p^2 is commutative.

Outline of a standard proof: If G is a group such that $G/Z(G)$ is cyclic, then G has to be abelian. If G is a group of order p^2 and not abelian, then $(|G/Z(G)| = p$ and hence $G/Z(G)$ is cyclic. Then G has to be abelian.

A proof via complex representations of G

The proof using complex representations of finite groups can look like this: Assume G is not abelian, let $\varphi_1, \ldots, \varphi_k \in \mathrm{Rep}_{\mathbb{C}}(G)$ be a list of all different complex irreducible representations of G up to equivalence. Since G is not trivial, $k > 1$. If d_i is the degree of φ_i, then, because of the degree theorem, $d_i \in \{1, p, p^2\}$. On the other hand, $\sum_{i=1}^{k} d_i^2 = |G| = p^2$. So $k > 1$ implies $d_i \in \{1\}$, for every i. It follows that G has no irreducible representation over $\mathbb{C}$ of degree > 1, hence G is abelian.

Groups of order pq

Proposition

Every group of order pq, where $p < q$ are primes and $q \not\equiv 1 \mod p$ is commutative.

Outline of the standard proof: Let G be a group of order pq, P its Sylow p-subgroup and Q its Sylow q-subgroup. Since $(q+1)(q-1)+1 = q^2 > pq$, Q has to be normal. Since $P \cap Q = 1$, G is a semidirect product of P and Q. Such a product can be costructed from P, Q and a homomorphism $f\colon P \to \mathrm{Aut}(Q)$. Now $P \simeq \mathbb{Z}_p, Q \simeq \mathbb{Z}_q$, $\mathrm{Aut}(Q) \simeq \mathbb{Z}_{q-1}$. Hence either f is trivial or $p = |\mathrm{Im}\ f|$ divides $q - 1 = |\mathrm{Aut}(Q)|$. The latter is not possible because of the assumption $q \not\equiv 1 \mod p$, so f is trivial. That is, the semidirect product is actually a product and $G = P \times Q$ is commutative.

Proof using complex representations

As in the first exercise we consider $\varphi_1, \ldots, \varphi_k \in \mathrm{Rep}_{\mathbb{C}}(G)$ a complete list of all different irreducible representations of G over $\mathbb{C}$ up to equivalence. If d_i is the degree of φ_i, then $d_i \in \{1, p, q, pq\}$ by the degree theorem. Since $\sum_{i=1}^{k} d_i^2 = |G| = pq$, each d_i has to be either 1 or p. Assume G is not commutative, so $[G, G] \neq 1$. The number of degree 1 representations in the list is G is $[G : [G, G]]$. Note that $[G : [G, G]]$ cannot be 1, since in this case $1 + (k-1)p^2 = pq$ cannot hold for any $k \in \mathbb{N}$. Similarly, $[G : [G, G]]$ cannot be q, since $q + (k-q)p^2 = pq$ implies $q(1 - p^2) = p(q - kp)$ where the left hand side is a product of two numbers coprime to p. Finally, if $[G : [G, G]] = p$, then $p + (k-p)p^2 = pq$ implies $1 + kp - p^2 = q$ and hence $p|(q-1)$.

Every finite p-group has nontrivial center

Proposition

Proof: *The classical argument is easy: Consider G as $G = \dot\bigcup_{i=1}^{k} C_i$, the union of conjugacy classes of G. Size of each C_i is either 1 (in this case $C_i \subseteq Z(G)$) or divisible by p. Then $|G| = \sum_{i=1}^{k} |C_i|$ shows that there exists i such that $C_i \neq \{1_G\}$ and $|C_i| = 1$.*

A proof using modular representations of groups, part 1

First let us show that every finite p-group is solvable: If $\varphi_1, \ldots, \varphi_k \in \mathrm{Rep}_{\mathbb{C}}(G)$ is a complete list of all different irreducible representations of G up to equivalence, d_i is the degree of φ_i. The trivial representation is of degree 1 and if $d_i > 1$, then $p | d_i$. From $\sum_{i=1}^{k} d_i^2 = |G| = p^l$ we see that there exists a nontrivial representation of degree 1. The kernel of this representation contains $[G, G]$, since the image of this representation is abelian. Thus for every finite p-group G, $[G, G] \neq G$ holds. Then every finite p-group is solvable.

A proof using modular representations of groups, part 2

Now we can prove that every finite p-group has a nontrivial center in a rather bizarre way. Assume there exists a finite p-group with trivial center. Let G be such a group of the smallest possible order. Since G is solvable, it has a normal subgroup N with $[G : N] = p$. Note that $1 \neq Z(N)$ and $Z(N)$ is a characteristic subgroup of N (this means that $\alpha(Z(N)) \subseteq Z(N)$ for every $\alpha \in \mathrm{Aut}(N)$). Let S be the socle of $Z(N)$, that is, $S = \{g \in Z(N) \mid g^p = 1\}$. Then S is a characteristic subgroup of N and as a group, $S \simeq \mathbb{Z}_p^t$ for some $t \in \mathbb{N}$.

A proof using modular representations of groups, part 3

Now consider a group homomorphism $\varphi\colon G \to \mathrm{Aut}(S)$ given by $\varphi(g)\colon s \mapsto gsg^{-1}$. Since S has a natural vector space structure over the field $\mathbb{F}_p$, we can consider S as an $\mathbb{F}_p$-vector space. Moreover, $\mathrm{Aut}(S) = \mathrm{Aut}_{\mathbb{F}_p}(S)$. So $\varphi \in \mathrm{Rep}_{\mathbb{F}_p}(G)$. Note that $N \subseteq \mathrm{Ker}\ \varphi$. So either $\mathrm{Ker}\ \varphi = N$ or $\mathrm{Ker}\ \varphi = G$. If $\mathrm{Ker}\ \varphi = G$ holds, then $S \subseteq Z(G)$. Which is not possible. Assume $\mathrm{Ker}\ \varphi = N$. Let $\pi\colon G \to G/N$ be the canonical projection and let $\psi\colon G/N \to \mathrm{Aut}_{\mathbb{F}_p}(S)$ be the homomorphism such that $\varphi = \psi\pi$. So ψ is a representation of $G/N \simeq \mathbb{Z}_p$ over the field $\mathbb{F}_p$.

A proof using modular representations of groups, part 4

Now use the connection between $\mathrm{Rep}_{\mathbb{F}_p}(G/N)$ and $\mathbb{F}_p(G/N)\text{-}\mathrm{Mod}$ and the fact that $\mathbb{F}_p(G/N) \simeq \mathbb{F}_p[x]/(x^p - 1)$ as $\mathbb{F}_p$-algebras. The ring $R = \mathbb{F}_p[x]/(x^p - 1)$ is local, so every simple R-module is isomorphic to R/m, where m is the maximal ideal of R. Note that for every $\bar{r} \in R/m$ the relation $\bar{r} = x\bar{r}$ holds, since $m = (x - 1)/(x^p - 1)$. Moreover, the ring is artinian, so every finitely generated R-module is artinian and, in particular, contains a simple submodule. When translated to $\mathrm{Rep}_{\mathbb{F}_p}(G/N)$ we get that every irreducible representation of G/N over $\mathbb{F}_p$ is trivial and that every representation of G/N finite degree contains an invariant subspace on which the action of G/N is trivial. Apply this to ψ: There exists $s \in S$ such that $|\langle s\rangle| = p$ and $\psi(gN)(s) = s$ for every $g \in G$. Then $[\varphi(g)](s) = [\psi(gN)](s) = s$, so $gsg^{-1} = s$. Then $s \in Z(G)$ a contradiction again.