10/26/2018
Fr

Recall We used group actions and counting arguments (e.g. the class equation) to prove

(5.4.2) If $|G| = p^n$, p prime, then $|Z(G)| > 1$

(5.4.3) If $|G| = p^2$, p prime, then $G \cong \mathbb{Z}_{p^2}$ or $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$

(5.4.6) Cauchy Theorem: If $p \mid |G|$, p prime, then G has an element of order p.

Today: Sylow theorems and applications

Def Let G be a finite group, p prime, n = largest integer such that $p^n \mid |G|$. A subgroup H of G s.t. $|H| = p^n$ is called the p-Sylow subgroup.

1st Sylow theorem Suppose G is a finite group, p a prime and $p^k \mid |G|$ $(k \in \mathbb{N})$. Then G has a subgroup H with $|H| = p^k$. In particular p-Sylow subgroups exist.

2nd Sylow theorem Any two p-Sylow subgroups of a finite group G are conjugate: if $P, Q < G$ are two p-Sylow subgroups, then $\exists\, a \in G$ s.t. $c_a(P) := aPa^{-1} = Q$.

In particular, all p-Sylow subgroups of G are isomorphic.

3d Sylow theorem Let G be a finite group, p prime, $p \mid |G|$, n = largest integer s.t. $p^n \mid |G|$, k = # of p-Sylow subgroups of G. Then $k \mid (|G|/p^n)$ and $k \equiv 1 \bmod p$.

Example 5.4.12 (Classification of groups of order $p \cdot q$, p, q primes, $1 < q < p$)

Let G be a group with $|G| = pq$

(i) If $q \nmid (p-1)$ then G is cyclic, hence $G \simeq \mathbb{Z}_{pq}$.

(ii) If $q \mid (p-1)$ then either $G \simeq \mathbb{Z}_{pq}$ or G is isomorphic to the semi-direct product $\mathbb{Z}_p \rtimes \mathbb{Z}_q$

Proof Since $|G| = pq$ and p, q are primes, Cauchy's theorem $\Rightarrow$ G has elements of order p and of order q.

$\Rightarrow$ $\exists$ subgroups P, Q of G with $P \simeq \mathbb{Z}_p$, $Q \simeq \mathbb{Z}_q$.

Note $P \cap Q$ is a subgroup of P and of Q.

$|P \cap Q| \mid p$ and $|P \cap Q| \mid q$. $\Rightarrow$ $|P \cap Q| \mid \gcd(p,q) = 1$

$\Rightarrow$ $|P \cap Q| = 1$ $\Rightarrow$ $P \cap Q = \{e\}$.

Let n = # of p-Sylow subgroups of G

3rd Sylow theorem $\Rightarrow$ $n \mid \frac{pq}{p} = q$ and $n \equiv 1 \bmod p$.

Since $n \mid q$, $n = 1$ or q. Suppose $n = q$.

Then $q \equiv 1 \bmod p$, i.e. $p \mid (q-1)$! But $q < p$: Impossible.

$\Rightarrow$ $n = 1$.

$\Rightarrow$ There is only one p-Sylow subgroup of G.

On the other hand, $\forall x \in G$ xPx^{-1} is also a p-Sylow subgroup. $\Rightarrow$ $xPx^{-1} = P$ $\forall x \in G$.

$\therefore$ P is normal in G.

Now $P = \langle a \rangle$, $Q = \langle b \rangle$ for some $a, b \in G$.

Since P is normal in G, $bab^{-1} \in \langle a \rangle$. $\Rightarrow$

$bab^{-1} = a^m$ for some $m \in \mathbb{Z}_0$

$\Rightarrow$ $PQ = \{ a^k b^l \mid k, l \in \mathbb{Z} \}$ is a subgroup of G

Consider $f : P \times Q \to G$ $f(a^k, b^l) = a^k b^l$

$a^k b^l = a^{k'} b^{l'} \Rightarrow a^{k-k'} = b^{l'-l} \in \langle a \rangle \cap \langle b \rangle = \{e\}$

$\Rightarrow$ $a^k = a^{k'}$, $b^l = b^{l'}$.

$\Rightarrow$ f is injective

Since $|P \times Q| = |P||Q| = pq = |G|$, f is onto hence a bijection.

Conclusion $G \cong P \rtimes Q \cong \mathbb{Z}_p \rtimes \mathbb{Z}_q$.

Note In general there is an action of $\mathbb{Z}_q$ on $\mathbb{Z}_p$ by isomorphisms, ie a homomorphism

$$\varphi : \mathbb{Z}_q \longrightarrow \mathrm{Aut}(\mathbb{Z}_p).$$

If φ is the trivial map, ie $\varphi([k]) = \mathrm{Id}_{\mathbb{Z}_p} \ \forall [k] \in \mathbb{Z}_q$

Then $G \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$ (Chinese remainder Thm)

So remains to prove: if $q \nmid (p-1)$ then

$\varphi([k]) = \mathrm{id}_{\mathbb{Z}_p} \ \forall [k] \in \mathbb{Z}_q$.

Claim $\mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_p^{\times}$, hence $|\mathrm{Aut}(\mathbb{Z}_p)| = p-1$.

Assume the claim for the moment.

$\ker(\varphi : \mathbb{Z}_q \to \mathrm{Aut}(\mathbb{Z}_p))$ is a subgroup of $\mathbb{Z}_q$

hence $|\ker\varphi| \mid q = |\mathbb{Z}_q|$. Two possibilities:

(i) $|\ker\varphi| = 1$. and (ii) $|\ker\varphi| = q$.

In case (i) $\varphi : \mathbb{Z}_q \to \mathrm{Aut}(\mathbb{Z}_p)$ is 1-1.

$\Rightarrow \varphi(\mathbb{Z}_q)$ is a subgroup of $\mathrm{Aut}(\mathbb{Z}_p)$ with q elements.

$\Rightarrow q \mid |\mathrm{Aut}(\mathbb{Z}_p)| = p-1$ (claim)

So φ is 1-1 only if $q \mid p-1$.

So if $q \nmid p-1$, $|\ker\varphi| \neq 1 \Rightarrow \ker\varphi = \mathbb{Z}_q \Rightarrow \varphi([k]) = \mathrm{Id}_{\mathbb{Z}_p} \ \forall [k] \in \mathbb{Z}_q$

$\Rightarrow G \cong \mathbb{Z}_{pq}$.

Proof of claim Suppose $f : \mathbb{Z}_p \to \mathbb{Z}_p$ is an isomorphism.

Then $f([n]) = f(\underbrace{[1]+\cdots+[1]}_{n}) = \underbrace{f([1])+\cdots+f([1])}_{n} = [n]\,f([1])$.

$f([1]) \neq [0]$ (for otherwise $f([n]) = [n][0] = [0]$ for all $[n]$, hence cannot be an isomorphism)

$\Rightarrow f([1]) = [a]$ for some unit $[a]$ of $\mathbb{Z}_p$.

and $f([n]) = [n][a] = [a][n]$ for <u>all</u> $[n] \in \mathbb{Z}_p$.

This gives us a map $\varphi : Aut(\mathbb{Z}_p) \to \mathbb{Z}_p^\times$

$\varphi(f) = f([1])$.

We need to prove: φ is an isomorphism.

$\varphi(f \circ g) = (f \circ g)([1]) = f(g([1])) = g([1]) \cdot f([1])$

$= \varphi(g) \cdot \varphi(f) = \varphi(f) \cdot \varphi(g)$ since $\mathbb{Z}_p^\times$ is abelian

φ is <u>onto</u> since $\forall [a] \in \mathbb{Z}_p^\times$

$R_{[a]}([n]) = [n][a]$ is an isomorphism.

(with the inverse $R_{[a]^{-1}}$)

φ is 1-1 since $\ker \varphi = \{ f \in Aut(\mathbb{Z}_p) \mid f([1]) = [1] \}$

and $\varphi([1]) = [1] \Rightarrow f([n]) = [n][1] = [n] \quad \forall [n] \in \mathbb{Z}_p$

i.e. $f = id(\mathbb{Z}_p)$