Lecture 27: Cauchy and pq

Wednesday, December 10, 2014
12:15 PM

Let p and q be primes, $p<q$, $p \nmid q-1$. Let G be a finite group.

$$\left.\begin{array}{l} |G| = pq \\ \exists\, N \trianglelefteq G,\ |N| = q \end{array}\right\} \Rightarrow G \simeq \mathbb{Z}_{pq}.$$

Remark 1. The assumption of existence of N is NOT needed. Using Sylow theorems, one can prove this.

2. Whenever we are asked to show $G \simeq \mathbb{Z}_n$, we need to show that G is cyclic. Since we have proved that a cyclic group of size $\underline{n}$ is isomorphic to $\mathbb{Z}_n$.

3. To show a group of size $\underline{n}$ is cyclic, we have to find an element of order $\underline{n}$.

Pf. Let $e \neq b \in N \Rightarrow o(b) \neq 1$ and $o(b) \mid |N|$ (by Lagrange)

$\Rightarrow o(b) = q$ (as q is prime)

$\Rightarrow |\langle b \rangle| = o(b) = q = |N| \Rightarrow \langle b \rangle = N \trianglelefteq G.$

By Cauchy's theorem, $\exists\, a \in G,\ o(a) = p.$

- If we show that $ab = ba$, then since $\gcd(o(a), o(b)) = 1$,

$$o(ab) = o(a)\,o(b) = pq,$$

which implies G is cyclic. And so $G \simeq \mathbb{Z}_{pq}$.

- $\langle b \rangle \trianglelefteq G \Rightarrow \exists\, i,\ aba^{-1} = b^i,$

$$0 \leq i \leq q-1$$

And $i \neq 0$ as otherwise $aba^{-1} = e \Rightarrow b = a^{-1}a = e$ which is a contradiction.

- $$a b^j a^{-1} = \underbrace{aba^{-1} \cdot aba^{-1} \cdot \ldots \cdot aba^{-1}}_{j \text{ times}} = b^i \cdot \ldots \cdot b^i$$

$$= b^{ij}.$$

- $$a^k b a^{-k} = a^{k-1}(aba^{-1})\,a^{-(k-1)}$$

$$= a^{k-1} b^i a^{-(k-1)}$$

$$= \left(a^{k-1} b a^{-(k-1)}\right)^i$$

$$= b^{(i^k)}$$

repeating

$\Rightarrow \quad b = a^p b a^{-p} = b^{i^p}$

Recall. $g^\ell = g^k \Leftrightarrow \ell \equiv k \pmod{o(g)}$.

$\Rightarrow \quad 1 \equiv i^p \pmod{o(b)} \Rightarrow \quad [i]_q^p = [1]_q$

$\Rightarrow \quad o([i]_q) \mid p \quad$ in $\mathbb{Z}_q^\times$

$\Rightarrow \quad$ either $\quad o([i]_q) = 1 \quad$ or $\quad o([i]_q) = p$.

On the other hand $\quad o([i]_q) \mid |\mathbb{Z}_q^\times| \quad$ by Lagrange

Recall. $\mathbb{Z}_n^\times =$ the group of units

$= \{[a]_n \mid \gcd(a,n)=1\}$

- $|\mathbb{Z}_n^\times| = \varphi(n)$ and $\varphi(q) = q-1$.

Since $p \nmid q-1$, $o([i]_q) = 1 \Rightarrow [i]_q = [1]_q$

$\Rightarrow \quad i = 1 \Rightarrow ab = ba \quad$ and we are done. $\blacksquare$