Lecture 27: Cauchy and \( p, q \)

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

\[
|G| = pq \quad \implies \quad G \cong \mathbb{Z}_{pq}.
\]

\( \exists N \trianglelefteq G, |N| = q \) \]

**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 \( G \cong \mathbb{Z}_n \), we need to show that \( G \) is cyclic. Since we have proved that a cyclic group of size \( n \) is isomorphic to \( \mathbb{Z}_n \).

3. To show a group of size \( n \) is cyclic, we have to find an element of order \( n \).

**Pf.** Let \( e \neq b \in N \implies o(b) \neq 1 \) and \( o(b) \mid |N| \)  
(by Lagrange)
\[ o(b) = q \quad (\text{as } q \text{ is prime}) \]

\[ |\langle b \rangle| = o(b) = q = |N| \Rightarrow \langle b \rangle = N \leq G. \]

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

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 \( G \cong \mathbb{Z}_{pq} \).

\( \langle b \rangle \leq G \Rightarrow \exists i, \quad ab^{-1}a = b^i \),

\[ 0 \leq i \leq q-1 \]

And \( i \neq 0 \) as otherwise \( ab^{-1}a = e \Rightarrow b = a^{-1}a = e \)

which is a contradiction.

\[ \underbrace{a b \quad a^{-1} \quad a b \quad a^{-1} \ldots \quad a b \quad a^{-1}}_{j \text{ times}} = b^i \]

\[ a^k b^{-k} a^k = a^{k-1} (a b a^{-1}) a^{-(k-1)} \]

\[ = a^{k-1} b^i a^{-1} \]

\[ = (a^{k-1} b a^{-1})^i \]

\[ = b^i \]

\[ = b \]
repeating \( b = a^p b a^{-p} = b \)

\[
\Rightarrow \quad b = a^p b a^{-p} = b
\]

Recall \( g^l = g^k \iff l \equiv k \mod o(g) \).

\[
\Rightarrow \quad 1 = i^p \mod o(b) \Rightarrow [i]_q^p = [1]_q
\]

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

\[
\Rightarrow \text{ either } o([i]_q) = 1 \text{ or } o([i]_q) = p.
\]

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

Recall \( \mathbb{Z}_n^x = \text{the group of units} \)

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

\[
|\mathbb{Z}_n^x| = \varphi(n) \text{ and } \varphi(q) = q - 1.
\]

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

\[
\Rightarrow i = 1 \Rightarrow ab = ba \text{ and we are done}. \quad \square
\]