Q: Let G be a group of order pq, where p and q are distinct primes. prove that G is ~~ab~~ abelian.

=> Solution:

Let, p = 3, q = 5, so, pq = 3 * 5 = 15.

consider Group of order 15 set is

G = {0, 1, 2, ... 14}.

Closure: if a, b ∈ G then a+b ∈ G

Let a = 7 ∈ G, b = 4 ∈ G; a+b = 7+4 = 11 ∈ G

condition satisfy.

Associative: if a, b, c ∈ G then a+(b+c) = (a+b)+c

Let, a = 1 ∈ G, b = 5, c = 6 ∈ G.

1+(5+6) = (1+5)+6

Identity element: The identity is 0, since ~~Let~~ so, Let a = 5. a+e = e+a = a

5+0 = 0+5 = 5.

condition is passed.

Inverse: if $a \in G$ the $a' + a = e$.

Let $a = 6$, $a' = -6$ so, $6 + -6$
$= 6 + 9 = 15 \% 15 = 0$.

commutativit: If $a \in G$, $b \in G$ then.

$a + b = b + a$ Let ~~a~~ $a = 3$, $b = 7$

so, $3 + 7 = 7 + 3 = 10 \in G$.

Since there all ~~proerty~~ properties of abelin is statify so G is abelian.

Q) If G is a group of order p^2 (where p is prime), then G is abelian if and only if it has $p+1$ subgroups of order p.

Solution: Let $p=3$ (so $|G|=9$)

There are only two

For any prime p:

If $G \cong \mathbb{Z}_{p^2}$ (cyclic of order p^2) → it has exactly 1 subgroup of order p.

If $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$ (like the 2D grid example above) → it has exactly $p+1$ subgroups of order p.

So, Every group of order p^2 is abelian.

The number of order-p subgroups tells you which abelian group it is

→ 1 subgroup → cyclic ($\mathbb{Z}_{p^2}$)

→ $p+1$ subgroups → not cyclic but still abelian ($\mathbb{Z}_p \times \mathbb{Z}_p$).

CamScanner

That's why the statement holds. The proof really just boils down to the fact there are only two abelian groups of order p^2.

Q) Let G be a finite group and H be a proper subgroup of G. Prove that the union of all conjugates of H cannot be equal to G.

Solution:

Q) Let G be a group and N be a normal subgroup of G. If G/N is cyclic and N is cyclic, prove that G is abelian.

$\Rightarrow$ given: G is a group, $N \trianglelefteq G$

$\rightarrow$ G/N is cyclic.

$\rightarrow$ N is cyclic.

Since G/N is cyclic, let gN be a generator of G/N.

That is, $G/N = \langle gN \rangle$, so every coset is of the form $g^k N$ for some $k \in \mathbb{Z}$.

Since N is cyclic let $N = \langle x \rangle$ for some $x \in N$.

Every element of G can be written as $g^k x^t$ for some integers k, t.

pick any $a \in G$. Then $aN = g^k N$ for some k, so $a = g^k n$ for some $n \in N$.

But $n = x^t$ for some t, since $N = \langle x \rangle$, Thus $a = g^k x^t$.

we want to show $ab = ba$ for all $a, b \in G$.

write $a = g^k x^t$, $b = g^m x^s$.

Since N is normal, $gxg^{-1} \in N$.

So $gxg^{-1} = x^r$ for some integer r.

Similarly $g^{-1}xg = x^q$ for some integer q.

But from $gxg^{-1} = x^r$, multiply on left by g^{-1} and right by g:

$x = g^{-1}x^r g = (g^{-1}xg)^r$

But $g^{-1}xg = x^q$, so $x = (x^q)^r = x^{qr}$

Thus $x^{qr-1} = 1$, so $qr \equiv r \pmod{|x|}$

(if $|x|$ finite; similar mod 0 if infinite order)

So r and q are multiplicative inverses modulo the order.

we have $gxg^{-1} = x^r$.
then $gx^t g^{-1} = (gxg^{-1})^t = (x^r)^t = x^{rt}$.
similarly, $g^{-1}x^t g = x^{qt}$.
Let $a = g^k x^t$, $b = g^m x^s$.
First, $ab = g^k x^t g^m x^s$.
we know that $g^m x^t = x^{r^m t} g^m$. Let's ~~check that~~

Lemma: $g^m x^t = x^{r^m t} g^m$, where r is from $gxg^{-1} = x^r$.
proof by induction on m
Base $m=1$: $gx^t = (gxg^{-1})^t g = (x^r)^t g = x^{rt} g$. so true for $m=1$
Assume $g^{m-1} x^t = x^{r^{m-1} t} g^{m-1}$
Then $g^m x^t = g(g^{m-1} x^t) = g(x^{r^{m-1}t} g^{m-1})$
Now $gx^{r \cdot m-1 t} = x^{r \cdot r^{m-1} t} g = x^{r^m t} g$.
so $g^m x^t = x^{r^m t} g g^{m-1} = x^{r^m t} g^m$. QED.
similarly, $x^s g^m = g^m (g^{-m} x^s g^m) = g^m x^{q^m s}$.
but maybe easier.

we can also find $x^s g^m = g^m x^{q^m s}$ from $g^{-m} x^s g^m = x^{q^m s}$ (since $g^{-1} x g = x^q$).

Now,

$ab = g^k x^t g^m x^s$.

using lemma: $x^t g^m = g^m x^{q^m t}$ - wait, check

we have $g^m x^t = x^{r^m t} g^m$

Replace t by dummy: $g^m X = X^{r^m} g^m$ for $X \in N$.

so x^t becomes $(x^t)^{r^m} = x^{r^m t}$. yes

From $g^m x^t = x^{r^m t} g^m$.

conjugate by g^{-m}: $x^t = g^{-m} x^{r^m t} g^m$.

so, $x^t g^m = g^{-m} x^{r^m t} g^m g^m$

Let ~~$x = g = gx$~~ $xg = gx^q$, so $x^t g = g x^{qt}$

similarly, $x^t g^m = g^m x^{q^m t}$ by induction.

Base $m=1$: $x^t g = g x^{qt}$.

Assume $x^t g^{m-1} = g^{m-1} x^{q^{m-1}t}$.

Then, $x^t g^m = (x^t g^{m-1}) g = g^{m-1} x^{q^{m-1}t} g$.

Now $x^{q^{m-1}t} g = g x^{q \cdot q^{m-1} t} = g x^{q^m t}$.

So $x^t g^m = g^{m-1} g x^{q^m t} = g^m x^{q^m t}$.

~~ab~~ So, $ab = g^k (x^t g^m) x^s = g^k (g^m x^{q^m t}) x^s$

$= g^{k+m} x^{q^m t + s}$.

$ba = g^m x^s g^k x^t$.

First, $x^s g^k = g^k x^{q^k s}$ (by above lemma w/ $m=k$)

So, $ba = g^m (x^s g^k) x^t = g^m g^k x^{q^k s} x^t$

$= g^{m+k} x^{q^k s + t}$.

We have:

$ab = g^{k+m} x^{q^m t + s}$

$ba = g^{k+m} x^{q^k s + t}$.

Since g^{k+m} is the same in both, for $ab = ba$ we need: $x^{q^m t + s} = x^{q^k s + t}$

That is, $q^m t + s \equiv q^k s + t \pmod{|x|}$ (mod order of x)

we want this to hold for all integers k, m, s, t.

In particular, take $k=0$, $m=1$;

Then $a = x^t$, $b = gx^s$.

compute $ab = x^t g x^s = (g x^{qt}) x^s = g x^{qt+s}$.

$ba = (gx^s) x^t = g x^{s+t}$.

Equality $ab = ba$ means $g x^{qt+s} = g x^{s+t}$,

so $x^{qt+s} = x^{s+t}$, so $x^{(q-1)t} = 1$ for all t.

Thus $q=1$.

Similarly, take $k=1$, $m=0$. we'd find $r=1$.

$q=1$ means $g^{-1} x g = x$, so $gx = xg$.

Similarly $r=1$ means $g x g^{-1} = x$, same conclusion.

so g commates with x, hence g

commutes with all elements of N.

since g commutes with all of N, and G/N is cyclic generated by gN, and N is cyclic generated by x, every element is $g^k x^t$, and these commute.

$(g^k x^t)(g^m x^s) = g^{k+m} x^{t+s}$

$(g^m x^s)(g^k x^t) = g^{m+k} x^{s+t}$, same.

so G is abelian.