Groups of Order pq

Xuanang (Shawn) Chen

November 2020

Abstract

The classification of groups of order pq is the a very useful trick which could easily be applied to lots of problems. In fact, a direct corollary of it is that if groups of order n is unique, then $(n, \phi(n)) = 1$.

Indeed, one can use Sylow Theorem to solve it, but it's too brutal and advanced. Here I'll present two very elementary proofs.

Theorem 1. *Groups of order pq is unique (cyclic) up to isomorphism if and only if* $p \nmid (q-1)$*, where* $p < q$ *are both primes.*

This is the main theorem of this paper which will be proved later. We first need some lemma.

Lemma 1. *For any finite group* G*, if* p *is the smallest prime that divides* $|G|$*, and* K *is a subgroup of* G *such that* $|G : K| = p$*, then* K *is a normal subgroup of* G.

Proof. Consider G acts on the left cosets of K by left multiplication. It induces a homormorphism $\phi : G \to Sym(G : K)$.
Consider $ker(\phi) \trianglelefteq G$. Note that $ker(\phi) \trianglelefteq K$. By Isomorphism Theorem , we have

$$G/_{ker(\phi)} \cong im(\phi) \leq Sym(G : K)$$

We have $|G : ker(\phi)| = |G : K||K/_{ker(\phi)}| = p|K/_{ker(\phi)}|$. So $p \mid |G : ker(\phi)|$. Hence $p \mid im(\phi)$.
On the one hand, the prime factors in $im(\phi)$ are no more than p as it's a subgroup of $Sym(G : K)$. On the other hand, the prime factors in $im(\phi)$ are no less than p since $G/_{ker(\phi)} \cong im(\phi)$. So $|im(\phi)| = p$. Thus, $ker(\phi) = K$. So $K \trianglelefteq G$ $\square$

Lemma 2. $x^d \equiv 1 \pmod q$ *has exactly* d *in-congruent solutions when* $d|(q-1)$ *for prime* q

Proof. Firstly, in $\mathbb{Z}_p$, the equation $x^d - 1 \equiv 0 \pmod q$ has at most d solution, while $x^{q-1} - 1 \equiv 0 \pmod q$ has exactly $q - 1$ solutions.
Since $d|(q-1)$, we can factorize $x^{q-1} = x^d P(x)$, where polynomial $P(x)$ has degree $(q - 1 - d)$, which has at most $(q - d - 1)$ solutions.
Thus, $P(x)$ and $x^d - 1$ must have maximun number of solutions so that $(q - d - 1) + d = (q - 1)$ can hold. So $x^d - 1 \equiv 0 \pmod q$ has exactly d solutions. $\square$

Lemma 3. *Let* G *be a finite group and* p *is a prime dividing its order. Then* $n_p \equiv -1 \mod p$*, where* n_p *denotes the number of elements of order* p.

Proof. Consider a subset $X \subseteq G^p$ defined by $X = \{(g_1, g_2, \ldots, g_p) \in G^p : g_1 g_2 \cdots g_p = e\}$. Since $|G^p| = |G|^p$, and $|X| = |G|^{p-1}$. Let $H = C_p = \langle \xi \rangle$, consider the action of H on X by

$$\xi \star (g_1, g_2, \ldots, g_p) = (g_2, g_3, \ldots, g_p, g_1)$$

This is an action, indeed, if $g_1 g_2 \cdots g_p = e$, then $g_2 g_3 \cdots g_p g_1 = g_1^{-1} e g_1 = e$. For any element $x \in X$, by Orbit-Stabilizer Theorem, $p = |H| = |H_x||H \star x|$. Since p is prime, every orbit has to have either size 1 or size p, also the orbits sum to $|X| = |G|^{p-1}$ which is divisible by p. So the number of size 1 orbits must be divisible by p, thus at least 2. All such orbits of size 1 must be in the form $(g, g, \ldots, p)$. In particular, apart from $(e, e, \ldots, e)$, there's a bijection between an element of order p such a tuple. Therefore, $n_p \equiv -1 \mod p$ $\square$

Lemma 4. *$(p-1) \mid n_p$, where p, n_p are the same definition in lemma 1.*

Proof. Consider the subgroups $S_1, S_2, \ldots$ of order p in group G. We must have $S_i \cap S_j = e$ for $i \neq j$. The result follows. ☐

We first prove the easy direction of Theorem 1, which only requires lemma 2 and a proper counterexample.

Proposition 1. *For groups of order pq, if $p|(q-1)$, then the group cannot be determined.*

Proof. By lemma 2, $l^p - 1 \equiv 0 \pmod q$ has exactly p solutions. In particular, it has a solution $t \neq 1$.
Consider the group representation $< h, k | h^p = k^q = e, h^{-1}kh = k^t$
(a) It's a group of order pq. To prove this, firstly notice that we can write equivalent of each element as $h^i k^j, 0 \leq i < p, 0 \leq j < q$. If $h^a k^b = h^c k^d$, then $h^{a-c} = k^{d-b} \Rightarrow p \mid (a-c)q \Rightarrow p \mid (a-c)$. Similarly $b \equiv d \pmod q$. So these pq elements are distinct.
(b) It's non-abelian. Recall that $t^p - 1 \equiv 0 \pmod q$
$(hk)(h^p k) = h^{p+1}k^{t^p+1} = h^{p+1}k^2$,$(h^p k)(hk) = h^{p+1}k^{t+1}$. Since $t \neq 1$, we are done. ☐

The other direction should use lemma 1, lemma 2 and lemma 3. See proposition 2.

Proposition 2. *For groups of order pq, if $p \nmid (q-1)$, then the group must be unique up to isomorphism (i.e. cyclic).*

Proof. By lemma 3, there exists subgroup H, K such that $|H| = q$, $H =< h >$ and $|K| = p, K =< k >$.
By lemma 1, we know H is normal in G. so $k^{-1}hk = h^l$ for some l.
We must have $h = k^{-p}hk^p = k^{-(p-1)}h^l k^{p-1} = k^{-(p-2)}(k^{-1}hk)^l k^{p-2} = k^{-(p-1)}h^{l^2}k^= \ldots = k^{l^p}$.
Thus, $l^p \equiv 1 \pmod q$. Since $p \nmid (q-1)$, we must have $l = 1$. This is because by Bezout Theorem, $(\exists x, y)xp + y(q-1) = 1$, so $l = l^{xp+y(q-1)} \equiv (l^p)^x (l^{(q-1)})^y \equiv 1 \pmod q$.
So the group must be abelian, hence cyclic. ☐

What about lemma 4? Well, when I first start approaching proposition 2, I used another fairly surprising way, which is about counting the order of elements.

Proof. By lemma 3&4, we can write $n_p = k_1 p - 1$, $n_q = k_2(q-1)$ for some $k_1, k_2 \in \mathbb{Z}$.
Suppose the group is not cyclic. Then each element has order 1,p or q. Thus

$$1 + k_1 p - 1 + k_2(q-1) \equiv 0 \pmod p$$

So $p \mid k_2$ as $p \nmid q-1$. Clearly $k_2 \neq 0$, so $k_2 = p, k_1 = 1$
Similarly, if we write $n_p = k_3(p-1), n_q = k_4 q - 1$, we have $q \mid k_3$. So $k_3 = q$.
Now $n_p = pq - q = p - 1 \to q = 1$, which is a contradiction. ☐

Combine Proposition 1 and Proposition 2, Theorem 1 is proved. We now show a direct corollary of Theorem 1.

Corollary 1. *For a group G with order n, if G is unique, then* $\gcd(n, \phi(n)) = 1$.

Proof. Firstly, n must be square-free. Otherwise, Write $n = p^\alpha m$, $C_p \times C_p \times \ldots \times C_m$ is not isomorphic to C_n
So write $n = p_1 p_2 \ldots p_m$. If $\gcd(n, \phi(n)) \geq 1$, we must have $p_i \mid (p_j - 1)$ for some i, j.
By the above construction of non-abelian group (call it H of order $p_i p_j$ in the proof of proposition 1, we know $H \times C_{\frac{n}{p_i p_j}}$ is not isomorphic to C_n ☐