On Number of Elements of Prime Order

Xuanang Chen

January 2021

Abstract

In this article, we are talking about the number of elements of order p in a group. If the group is finite, is easy to get the answer once we find the proper group action. However, if the group is infinite, the approach is completely different and way harder. Proposition 3 is a special case, while proposition 4 is a generalized result.

Proposition 1. *In a finite group, $n_p \equiv -1 \pmod p$, where p is a prime dividing the order of the group, and n_p is the number of elements of order p.*

It is covered by my another article. See lemma 3 here.

Proposition 2. *In a (possibly infinite) group G, the number of elements of order 2 n_2 cannot be 2.*

Proof. If we have two distinct elements of order 2, say x and y. If x, y commute, then the order of xy is 2. If not, then the order of $x^{-1}yx$ is 2. Either way, there's a third element of order 2. □

Proposition 3. *In a (possibly infinite) group G, if n_2 is not* 0 *or infinite, then n_2 is odd.*

This is an improvement of proposition 2, but the process to fill the gap is not as easy as it was thought to be.

Proof. We prove inductively. Suppose $a_1, a_2, ..., a_n$ are elements of order 2 in G, where n is odd. If there's another element b which also has order 2, We shall show that we can find another c has order 2. Thus, there cannot be even number involutions.
Suppose we cannot find such c. For each i, (i) When $a_ib = ba_i$, $(a_ib)^2 = e$.
(a) If $a_ib \neq a_j$ for any j, let $c = a_ib$, a contradiction.
(b) If $a_ib = a_j$ for some j, then $a_jb = a_i$, $ba_j = a_jb$.
So we know that we can pair a_i with a_j which commutes with b.
(ii) When $a_ib \neq ba_i$, $(ba_ib)^2 = e$
(a) If $ba_ib \neq a_j$ for any j, let $c = ba_ib$, a contradiction.
(b) If $ba_ib = a_j$ for some j, then $ba_jb = a_i$, and $ba_j \neq a_jb$.
So we know that we can pair up a_i with a_j which are not commutes with b.
However, n is odd, so there must be some element that pair to itself. If $a_ib = a_i$ when $a_ib = ba_i$, then $b = e$, contradiction. If $ba_ib = a_i$ when $a_ib \neq ba_i$, then there's a contradiction as $ba_ib = a_i \Rightarrow a_ib = ba_i$.
So the inductive step is done. □

Proposition 4 will generalize proposition 3. The method is, again, completely different. We need some lemma.

Lemma 1. *Let G be a (possibly infinite) group, and H, K be its subgroups of finite index. Then $H \cap K$ is of finite index.*

Proof. We have $[G : H \cap K] = [G : H][H : H \cap K] = [G : H][HK : K] \leq [G : H][G : K]$.
The first equality is trivial. As for the second equality, although the normality of H, K is not assumed so that HK is not necessarily a group, the index still makes sense as it's some left cosets of K, and it is derived from the group action: H transitively acts on $HK : K$, and uses orbit-stabilizer theorem. The last inequality is obvious. □

To prove the final result, we must use commutator group.

Definition 1. *The commutator of a and b is $aba^{-1}b^{-1}$. The commutator group, $[G, G]$, is defined by all finite products of cummutators in G.*

We only need a weak form of the following lemma, but I would not bother write whole lemma to make it complete.

Lemma 2. $[G, G] \trianglelefteq G$. *For* $N \trianglelefteq G$, ${}^{\mathbb{G}}/_{\mathbb{N}}$ *is abelian if and only if* $C \subseteq N$

Proof. The first statement is trivial if we notice that $g^{-1}x_1x_2...x_ng = (g^{-1}x_1g)(g^{-1}x_2g)...(g^{-1}x_ng)$.
($\Leftarrow$) For $C \subseteq N$, We have $(ab)(ab)^{-1} \in N \Rightarrow abN = baN \Rightarrow (aN)(bN) = (bN)(aN)$
($\Rightarrow$) The direct inverse argument. □

Lemma 3. *If the center* $\mathbb{Z}(G)$ *has finite, then* $[G, G]$ *is finite.*

This proof is not hard, but it's just too complicated to be included in this paper. I do not come up with it of my own, and it is attributed to Schur. The proof is, a little tricky and is not a proof that you can benefit a lot, at least for elementary group theory. So I shall just quote it. For a detailed proof, see here

Proposition 4. *The number of elements of order p in a (possibly infinite) group,* n_p, *if non-zero and finite, must satisfy* $n_p \equiv -1 \pmod{p}$.

Proof. In a group G, if the number of elements of order p is non-zero and finite, we just need to look at H which is generated by the elements of order p. If H is finite, we are done by proposition 1.
Every conjugate of an element of order p is of order p. Thus, the orbit of conjugation action on x is finite, so centralizer of x is of finite index by orbit-stabilizer theorem. Here $ord(x) = p$. By lemma 1, we know that $\cap C(x)$ is of finite index, where x are elements of order p. Moreover, since H is generated by these elements, $\cap C(x)$ is the centralizer of any element in H. So the center, $\mathbb{Z}(H) = \cap C(x)$, has finite index.
By lemma 3, the commutator group $[H, H]$ is finite. By lemma 2, we also know that ${}^{H}/_{[H,H]}$ is abelian. It's sufficient to show that ${}^{H}/_{[H,H]}$ is finite.
Since ${}^{H}/_{[H,H]}$ is abelian, and is generated by finite elements of finite order, it must be finite as we can write it in a fixed form. Thus, $|H| = |H : [H, H]||[H, H]|$ is finite. Applying proposition 1, we are done. □