Lemma for Fundamental Theorem of Finite Abelian Groups

Lemma 1 (a)**.** *Let G be a finite abelian group with p a prime such that $p\big||G|$, then there exists an element of order p in G.*

We will make extensive use of Theorem 6.14, so before we begin our proof let us recall it now:

> **Theorem 6.14** – Let G be a cyclic group with n elements and generated by a. Let $b \in G$ and let $b = a^s$. Then b generates a cyclic subgroup H of G containing n/d elements, where d is the greatest common divisor of n and s. Also, $\langle a^s\rangle = \langle a^t\rangle$ if and only if $\gcd(s,n) = \gcd(t,n)$.

For our purposes, the first conclusion of the theorem can be rewritten as: if $|a| = n$ then $|a^s| = \dfrac{n}{(n,s)}$.

Proof. We proceed by induction on $|G|$. Suppose $|G| = 2$, then the result immediately follows since the non-identity element in G has order 2. Now, suppose that for all groups of order less than $n+1$, if p is a prime dividing the order of the group then G contains an element of order p (this is called *strong* induction).

Let G be a group of order $n+1$ with $n > 1$ (since taking $n = 1$ was our base case) and suppose that p is a prime such that $p\big||G|$. Since $|G| > 1$ there exists some $a \in G$ with $a \neq e$, and we may consider $\langle a\rangle \leq G$.

If $p\big||\langle a\rangle|$ then $|\langle a\rangle| = pm$ for some $m \in \mathbb{Z}$ (we can in fact take $m \in \mathbb{N}$ since both p and $|\langle a\rangle|$ are known to be positive), and hence by Theorem 6.14, $|a^m| = \dfrac{pm}{(pm,m)} = \dfrac{pm}{m} = p$. Thus, $a^m \in G$ is an element of order p.

Suppose now that $p \nmid |\langle a\rangle|$. Since G is abelian it follows that $\langle a\rangle \lhd G$ and so we may consider the quotient $G_1 = G/\langle a\rangle = \{g\langle a\rangle : g \in G\}$. We have that $p\big||G|$ and $p \nmid |\langle a\rangle|$ therefore, since $|G_1| = |G|/|\langle a\rangle|$ it must be the case that $p\big||G_1|$. In addition, we also have that $|G_1| < |G| = n+1$ and thus there exists some $x\langle a\rangle \in G_1 = G/\langle a\rangle$ of order p by our inductive hypothesis.

By assumption $p \nmid |\langle a\rangle|$ so we clearly have $\gcd(p, |\langle a\rangle|) = 1$ and thus $\langle a^p\rangle = \langle a\rangle$ by Theorem 6.14. Therefore, since $x\langle a\rangle$ has order p it follows $(x\langle a\rangle)^p = e = \langle a\rangle \in G/\langle a\rangle$ and so we see

$$\langle a\rangle = (x\langle a\rangle)^p = x^p\langle a\rangle^p = x^p\langle a^p\rangle = x^p\langle a\rangle$$

which implies $x^p \in \langle a\rangle$.

For notation's sake, we now let $s = |\langle a\rangle|$. Since $x^p \in \langle a\rangle$ we have $x^{ps} = (x^p)^s = e$ which implies $|x|\big|ps$ and so $|x|k = ps$ for some $k \in \mathbb{Z}$ (and again we can actually take $k \in \mathbb{N}$). Using this and the properties of the greatest common divisor we have the following identity:

$$p(|x|, s) = (p|x|, ps) = (p|x|, |x|k) = |x|(p,k).$$

This in conjunction with Theorem 6.14 then gives

$$|x^s| = \frac{|x|}{(|x|,s)} = \frac{p}{(p,k)},$$

so in particular, $|x^s|\big|p$.

It is clear that $(p,k) = 1$ or $(p,k) = p$ since p is a prime, and hence $|x^s| = p$ or $|x^s| = 1$, respectively. Recall from above we know that $|x\langle a\rangle| = p$, $|\langle a\rangle| = s$ and $p \nmid |\langle a\rangle|$, with the last condition implying $(p, |\langle a\rangle|) = 1$. So, applying Theorem 6.14 one last time, we see

$$|x^s\langle a\rangle| = \frac{|x\langle a\rangle|}{(|x\langle a\rangle|, s)} = \frac{p}{(p, |\langle a\rangle|)} = p.$$

If $|x^s| = 1$ then $x^s = e$ and so $x^s\langle a\rangle = \langle a\rangle$; implying $p = |\langle a\rangle|$, which is a contradiction since we assumed $p \nmid |\langle a\rangle|$. Therefore, we must have $|x^s| = p$, so $x^s \in G$ is an element of order p, as desired.

□