# THE FUNDAMENTAL THEOREM OF FINITE ABELIAN GROUPS – PROOF

Theorem: Let *G* be an abelian group such that $|G| = p^n$ for some prime *p*. Then $G = A \oplus Q$ where *A* is a cyclic group of *G* that is of maximal order.

Proof: Let *G* be an abelian group such that $|G| = p^n$ for some prime *p*. We will proceed by induction on *n*. Thus, if $n = 1$, then $|G| = p$, *G* is cyclic, we can let $A = \langle a \rangle$ for any $a \in G$, $G = A$, and we are done. Hence, suppose that $n \neq 1$ and assume the induction hypothesis that the theorem is true for any $m < n$. If there exists $a \in G$ such that $A = \langle a \rangle = G$, then, again, we are done. Thus, suppose *G* is not cyclic and that $a \in G$ such that $A = \langle a \rangle = p^m$ where $p^m$ is the largest order of any cyclic subgroup of *G*. Suppose also that there exists $b \in G - A$ such that $B = \langle b \rangle$, $|B| = |\langle b \rangle| = p^r$ where $p^r \leq p^m$, and $A \cap B = e$. Now consider $G/B$. We have that $|G/B| = \dfrac{|G|}{|B|} = \dfrac{p^n}{p^r} = p^{n-r} \neq 1$. Hence, our induction hypothesis applies and since $A \cap B = \langle a \rangle \cap \langle b \rangle = e$, it follows that for $aB \in G/B$, $|\langle aB \rangle| = |\langle a \rangle| = |A| = p^m$. Thus, using our induction hypothesis, $G/B = \langle aB \rangle \oplus Q/B$ for some subgroup *Q* of *G* such that $B \leq Q \leq G$. We now ask the question is $A \cap Q = e$? If not, then there exists $a^i \in A \cap Q$ such that $a^i \neq e$ and $a^i \notin B$. Hence, $a^i B \in \langle aB \rangle \cap Q/B$ and $a^i B \neq B$. But this contradicts our induction hypothesis that $G/B = \langle aB \rangle \oplus Q/B$ since by definition of a direct sum we must have $\langle aB \rangle \cap Q/B = B$, the identity in $G/B$. Consequently, it must be true that $A \cap Q = e$. Furthermore, since $G/B = \langle aB \rangle \oplus Q/B$, it follows that $G = AQ$, and since $A \cap Q = e$, we now have that $G = A \oplus Q$. Notice also that if $|B| = |\langle b \rangle| = p^r$, then $\left|\left\langle b^{p^{r-1}} \right\rangle\right| = p$ and $A \cap B = \langle a \rangle \cap \left\langle b^{p^{r-1}} \right\rangle = e$. In other words, if *G* has a subgroup of order $p^r$ whose intersection with *A* is *e*, then *G* has a subgroup of order $p$ whose intersection with *A* is *e*.

Now suppose that there exists $b \in G - A$, $A = \langle a \rangle$, such that $\langle a \rangle \cap \langle b \rangle \neq e$ and $|\langle b \rangle| = p^r \leq p^m = |\langle a \rangle|$. In this case, just as we assumed that $p^m$ is the maximum order for any cyclic subgroup of *G*, we may assume that $p^r$ is the minimum order for any cyclic subgroup of *G* that meets the conditions above. In particular, if we consider $b^p$, then $\left|\left\langle b^p \right\rangle\right| = p^{r-1} < p^r = |\langle b \rangle|$ implies that $b^p \notin G - A$, and, hence, $b^p \in A$. Thus, there exists a positive integer *i* such that $b^p = a^i$. Our claim now is that *p* divides *i*, and we'll prove this claim using proof by contradiction. Thus, assume that *p* does not divide *i*. Then it is also true that $p^m$ does not divide $\dfrac{ip^m}{p} = ip^{m-1}$. Hence, $\dfrac{ip^m}{p} = ip^{m-1}$ is not a multiple of $p^m$, and

therefore, $a^{\frac{ip^m}{p}} = a^{ip^{m-1}} \neq e$. But on the other hand, $a^{ip^{m-1}} = (a^i)^{p^{m-1}} = (b^p)^{p^{m-1}} = (b^p)^{p^m/p} = b^{p^m} = (b^{p^r})^{p^m/p^r} = (e)^{p^m/p^r} = e$, and this is a contradiction. Therefore, *p* divides *i*, and so we can write $i = jp$ for some positive integer *j*. Now let $y = a^{-j}b$. If *y* were an element of *A*, then $a^j y = b$ is also an element of *A* contradicting our assumption that $b \notin A$. Thus, $y \notin A$. Furthermore, $y^p = (a^{-j}b)^p = a^{-jp}b^p = a^{-i}a^i = e$. But now since we have found an element $y \notin A$ such that $y^p = e$ for *p* a prime, it follows also that $\langle a \rangle \bigcap \langle y \rangle = e$ and we can now repeat our earlier arguments to conclude that there exists a subgroup *Q* such that $G = A \oplus Q$.

□

Corollary: Since when *G* is an abelian group such that $|G| = p^n$ for some prime *p*, we can write $G = A \oplus Q$ where *A* is a cyclic group of *G* that is of maximal order, it follows that we can do the same with *Q* and then continue until we have *G* written as a direct sum of cyclic *p*-groups.

□

The Fundamental Theorem of Finite Abelian Groups: If *G* is a finite abelian group such that $|G| = p_1^{n_1} p_2^{n_2} \cdot \ldots \cdot p_k^{n_k}$ for primes $p_1^{n_1}, p_2^{n_2}, \ldots, p_k^{n_k}$, then we can write *G* as a direct sum of cyclic *p*-groups using each prime $p_i$ that divides the order of *G*.

Proof: Our last corollary to the Sylow theorems showed that we can write *G* as a direct sum of its Sylow *p*-subgroups, $G = S_{p_1^{n_1}} \oplus S_{p_2^{n_2}} \oplus \ldots \oplus S_{p_k^{n_k}}$. Also, our theorem and corollary above show that each Sylow *p*-subgroup can be written as a direct sum of cyclic *p*-groups. Thus, combining these results, we can also write *G* as a direct sum of cyclic *p*-groups using each prime $p_i$ that divides the order of *G*.

□