Classification of finite abelian groups - 1

Proposition: If G is a finite abelian group of order n, and p is a prime that divides n, then G has an element of order p.

Proof:

We use induction on n. The key technique is to use the fact that since G is abelian, every subgroup H is normal, so you can look at H and G/H and try to figure out something for G.

Assume "If G is abelian, order k, $p|k \Rightarrow G$ has an elt of order p." holds for all $k < n$.

If $n = 1$, G is the trivial group and the result is true. So suppose every group of order $k < n$ satisfies the condition.

$n=1$ G trivial. $\Rightarrow$ true.

1. Suppose that G has no proper subgroups. Since G is abelian this means that G is cyclic of order p. Thus the result is true in that case.

G has no proper subgroups $\Rightarrow$ every non-trivial elt of G generates $G \Rightarrow G$ has prime order $\Rightarrow G = \mathbb{Z}_p$.
So we have our result in this case.

2. Otherwise let H be a proper subgroup of G. If p divides the order of H, then H has an element of order p since H has fewer elements than G and we can apply the inductive hypothesis.

$|G| = |H|[G:H]$

$p \mid |H|$
$|H| < |G|$ $\Rightarrow$ H has an elt of order p.

$\Rightarrow$ G has an elt of order p.

3. If H does not have order divisible by p, then p divides the order of G/H. By the inductive hypothesis, G/H contains an element of order p.

G/H has order divisible by p
$|G/H| < |G|$ $\Rightarrow$ G/H has an elt of order p.

$\in G/H$

4. Suppose aH is this element of order p. Then $(aH)^p = H$ so a^p is in H (but $a \notin H$.)

$(aH)^p = H \Leftrightarrow a^p \in H$

$a \notin H$

5. Let $b = a^{|H|}$. Since $|H|$ is not divisible by p, we can solve $x|H| + yp = 1$. Thus

$a^p \in H$

$a \notin H$

$$a = b^x (a^p)^y \in b^x H.$$

$a^1 = a^{x|H| + yp} = (a^{|H|})^x (a^p)^y$

$= b^x \underbrace{(a^p)^y}$ $\Rightarrow$

$a \in b^x H$. $a \notin H$ so $b^x \notin H$.

6. If $b = e$ then $a \in H$, but that isn't true. Therefore $b \neq e$. However, $b^p = a^{p|H|} = e$ since $a^p \in H$. Thus b has order p in G.

$b = e \Leftrightarrow a = (a^p)^y \in H$ and that isn't true.

$b \neq e$.

$b^p = a^{p|H|}$ $a^p \in H$

$b^p = e$ $(a^p)^{|H|} = e$.

b has order p.

$(aH)^p = H$ $\underline{a^p \in H}$, $a \notin H$.

$b = a^{|H|}$ $\Rightarrow$ b has order p.

Proposition: Let G be a finite abelian group and let p be a prime number. The following are equivalent:

- every element of G has order p^s for some $s \geq 0$.
- G has order p^n for some $n \geq 1$.

Proof:

Let n be the order of G. If every element of G has order p^s for some $s \geq 0$, then by the previous result n must be a power of p.

If n is order a power of p, then by Lagrange's theorem every element has order a power of p.

if $|G| = p^k$ then if $g \in G$, order$(g) \mid p^k$
so order$(g) = p^i$.

If $o(g) = p^i$ for all g:
Suppose $|G|$ is divisible by q, $q \neq p$.
G has an elt of order q — not true since $o(g) = p^i$.

Classification of finite abelian groups - 2

Proposition: Suppose G is a finite abelian p-group. Let g have maximal order among elements of G. Then there is a subgroup H so that G is the internal direct product of $\langle g \rangle$ and H.

Proof: We will use induction on the order of G. Given g of maximal order, such that $G \neq \langle g \rangle$, the strategy of this proof is to find a subroup of H of order p such that $\langle g \rangle \cap H = \{0\}$ and so that the order of gH in G/H is the same as the order of g in G. Since G/H is of order less than G, by induction there is a subgroup K in G/H so that G/H is the internal product of $\langle gH \rangle$ and K. Then the inverse image of K in G is the subgroup we want.

Goal:

$gH \in G/H$ to have same order as $g \in G$.

G

$|H| = p$ $\quad$ H $\quad$ G/H

$G/H = \langle gH \rangle \times K/H$

$\langle g \rangle \times K$

$|G| = p^n$ if $|G| = p^k$ $k < n$
then result is true.

1. If $n = 1$, then G is cyclic of order p and so we can take H to be the trivial group.

2. Now let $g \in G$ be of maximal order among the elements of G. Say the order of g is p^m.Notice that $a^{p^m} = e$ for any $a \in G$.

3. If g generates G, then G is cyclic and we can take H to be the trivial group.

$\mathbb{Z}_8 \times \mathbb{Z}_4$
$g = (1,0)$

$a\langle g\rangle$

4. Otherwise, choose $a\langle g\rangle$ in $G/\langle g\rangle$ of minimal order greater than 1. This gives an $a \notin \langle g\rangle$. Since the order of a^p is less than the order of a, we must have $a^p \in \langle g\rangle$.

$a\langle g\rangle$ must have order p

$a^p \in \langle g\rangle$ $\quad a \notin \langle g\rangle$,

5. We have $a^p = g^r$ for some r. Since $g^{rp^{m-1}} = a^{p^m r} = e$ we see that g^r is not a generator of $\langle g\rangle$. This means that $p|r$.

$a^p = g^r$

$a^{p^m} = e$ $\qquad (a^p)^{p^{m-1}} = e = (g^r)^{p^{m-1}} = g^{rp^{m-1}}$

$g^K = e \Rightarrow \text{order}(g)|K$ $\qquad p^m \mid rp^{m-1} \Leftrightarrow p|r$.

6. Write $r = ps$ and let $b = g^{-s}a$. Note that $b \notin \langle g\rangle$ since a is not. Also Then $b^p = g^{-ps}a^p = g^{-ps}g^r = e$. Therefore b has order p. Let H be the subgroup generated by b.

$b \neq e$. $\qquad b = g^{-s}a$. $\qquad b \notin \langle g\rangle$ because if

$b^p = g^{-ps}a^p = g^{-ps}g^r = e$. $\qquad g^{-s}a = g^j \Rightarrow a = g^{j+s}$

but $a \notin \langle g\rangle$.

$\mathbb{Z}_8 \times \mathbb{Z}_4$

$g = (1,0)$

$h = (0,2)$

7. H has order p and its intersection with $\langle g \rangle$ is trivial.

$H = \langle b \rangle$ order p

8. Consider gH in G/H. If $(gH)^{p^s} = H$ then $g^{p^s} \in H$, but that can only happen if $g^{p^s} = e$. Therefore the order of gH in G/H is still p^m.

$(gH)^{p^s} = H \Rightarrow g^{p^s} \in H.$

$g^{p^s} \in \langle g \rangle \cap H = \{e\}$

$g^{p^s} = e \Rightarrow p^m \mid p^s.$

order $(gH) = p^m.$

$(\mathbb{Z}_8 \times \mathbb{Z}_4)/H$

$\mathbb{Z}_8 \times \mathbb{Z}_2$

$(1,0)$

9. By induction, there is a subgroup K of G/H so that G/H is the internal direct product of $\langle gH \rangle$ and K, so that

$$G/H \cong \langle gH \rangle \times K.$$

Inductive hypothesis.

10. Let J be the preimage of K in G/H under the canonical homomorphism. J is a subgroup of G that contains H.

$J = \{k \in G \mid kH \in K \subseteq G/H\}$.

$H \subseteq J \subseteq G$. $\quad k_1, k_2 \in J \quad k_1 H \in K \quad k_2 H \in K$

$k_1 k_2 H = (k_1 H)(k_2 H) \in K$

11. $G = \langle g \rangle J$. Because given an element u of G, we have $uH = (zH)(kH)$ where $z \in \langle g \rangle H$ and $k \in J$, so $u = zhkh' = zk'$ for $k' \in J$.

$u \in G$. $\quad uH = (zH)(kH) \quad z \in \langle g \rangle H$

$\langle g \rangle H \times K = J/H \quad k \in J$

$u = zkh = g^i j$

$k \in J$

$h \in H \subseteq J$

$kh \in J$.

12. If $h \in J \cap \langle g \rangle$ then hH is in the intersection of K with $\langle gH \rangle$ in G/H, so $h \in H \cap \langle g \rangle$ and therefore $h = e$.

$h \in \underbrace{\langle g \rangle \cap J} \quad hH \in K \quad G/H = \langle g \rangle H \times K$

$hH \in \langle g \rangle H \quad \Rightarrow h \in H \cap K \cap \langle g \rangle H = H$.

$h = e$ since $H \cap \langle g \rangle = \{e\}$.

13. Consequently G is the product of $\langle g \rangle$ with K.

$J, \langle g \rangle \leq G$

$J \cap \langle g \rangle = \{e\}$

$\langle g \rangle J = G$.

$G \simeq \langle g \rangle \times J$.

$\underset{\langle g \rangle}{\mathbb{Z}_8} \times \underset{J}{\mathbb{Z}_4}$

Corollary: An abelian p-group is isomorphic to a product of cyclic abelian p-groups.

Proof: We prove this by induction on the number of elements in G. If G has p elements, it is cyclic. If G has p^m elements, use the theorem to write $G = \langle g \rangle \times K$ where g has maximal order among the elements of G. Then K is a p-group of order smaller than the order of G, so it is a product of cyclic abelian p-groups.

Classification of finite abelian groups - 3

Theorem: An abelian group G of order nm, where n and m have greatest common divisor one, is isomorphic to the product $G = G_n \times G_m$. where G_n is the subgroup of elements of order dividing n and G_m is the subgroup of elements of order dividing m.

Proof: G_n and G_m are subgroups, and their intersection are the elements consists of elements whose order divides both n and m, and is therefore trivial. Write $am + bn = 1$. Let g be any element of G. Then

$$g = g^{am+bn} = (g^m)^a (g^n)^b.$$

But g^m has order dividing n since $(g^m)^n = e$, and g^n has order dividing m for the same reason. Thus $G_n G_m = G$. Therefore G is the internal direct product of G_n and G_m.

$a, b \in G$ order$(a) \mid n$ order$(b) \mid n$.

$n(a+b) = na + nb = 0$ order$(a+b) \mid n$.

$(ab)^n = a^n b^n$ in abelian group.

$h \in G_n \cap G_m \Rightarrow$ order$(h) \mid n$ and order$(h) \mid m$

$\Rightarrow$ order$(h) = 1$.

$am + bn = 1$.

$g \in G$ $\quad g = g^{am+bn} = (g^m)^a (g^n)^b$

$g^m \in G_n \quad [g^m]^n = e$

$g^n \in G_m \quad [g^n]^m = e$.

$G \cong G_n \times G_m$

Theorem: Any finite abelian group is a product of finite cyclic p groups.

Proof: Let n be the order of G. Write $n = p_1^{e_1} \times \cdots \times p_k^{e_k}$. Then by the previous theorem, G is the product of subgroups G_i consisting of elements of order a power of p_i. Each such subgroup is an abelian p_i group and is therefore a product of cyclic abelian p_i groups as claimed.

$n = p_1^{e_1} [\ _1 \qquad]$

$G = G_{p_1^{e_1}} \times G_{p_2^{e_2}} \times \dots \times G_{p_k^{e_k}}$

$G_{p_i^{e_i}} = \{ g \in G \mid \text{order}(g) = p_i^{r_i} \}.$

$G_{p_i^{e_i}}$ is an abelian p-group.

$G_{p_i^{e_i}} = \langle g_1 \rangle \times H = \langle g_1 \rangle \times \langle g_2 \rangle \times H'$

$=$ product of cyclic p-groups.

finite G = product of cyclic p-groups.

<u>Theorem</u>: If G is a finitely generated abelian group

then

$$G \simeq \mathbb{Z}^k \times G_{tor}$$

$G_{tor} = \{ g \in G \mid \text{order}(g) \text{ is finite} \}$

G_{tor} is a finite abelian gp.