Classification of Finite Abelian Groups

Here are some notes for what we did in class. We assume the order of G is a prime power and we want to express it as the direct product of cyclic groups. In these notes we'll first do a special case that illustrates the general ideas and then the general case.

But first, some general stuff. Let G be an Abelian group and A a subgroup of G. Then we have the map $\phi : G \to G/A$ where we write $\phi(x) = \overline{x}$. The standard example is when G is the integers (positive, negative and zero) and A is the multiples of three (positive, negative and zero). Since ϕ is a homomorphism we have $\overline{x+x} = \phi(x+x) = \phi(x) + \phi(x) = \overline{x} + \overline{x}$. Further $\overline{x+x+x} = \phi(x+x+x) = \phi(x) + \phi(x) + \phi(x) = \overline{x} + \overline{x} + \overline{x}$. More generally, for any positive integer s we have

$$\overline{sx} = s\overline{x}$$

(Here sg is a shorthand for $g + \ldots + g$, with s terms.) For example, take $s = 5$ and $x = 2$ in the standard example. So $5 \cdot 2 = 2+2+2+2+2 = 10$ and we are saying $\overline{10} = \overline{2} + \overline{2} + \overline{2} + \overline{2} + \overline{2}$. Of course, both are $\overline{1}$.

A second thing. When is $\overline{x} = \overline{0}$? This occurs exactly when x is in the kernel of ϕ which happens exactly when $x \in A$. (Going back to the cosets, it is saying that the coset $x + A$ is equal to the coset $0 + A$ exactly when $x \in A$. In the example $\overline{x} = \overline{0}$ exactly when x is a multiple of three.) That is,

$$\overline{x} = \overline{0} \text{ if and only if } x \in A$$

OK, on to finite Abelian groups.

`Special Case:` $o(G) = p^3$, No x has $o(x) = p^3$, Some x has $o(x) = p^2$.
Theorem: In this case $G \cong Z_{p^2} \times Z_p$.
Proof: Take $x_1 \in G$ with $o(x_1) = p^2$ and set $A_1 = \{ix_1 : 0 \leq i < p^2\}$. A_1 is a subgroup with p^2 elements so G/A_1 is a group with $p^3/p^2 = p$ elements. Take $y_2 \notin A_1$. Then $\overline{y_2} \neq \overline{0}$. (Notation: For $z \in G$ we write $\overline{z}$ for the coset containing z, so that $\overline{z} \in G/A_1$.) As $o(G/A_1) = p$, $o(\overline{y_2}) = p$ so $\overline{0} = p\overline{y_2} = \overline{py_2}$ so $py_2 \in A_1$ so $py_2 = ix_1$ for some $0 \leq i < p^2$.

As no element of G has order p^3 we must have $0 = p^2 y_2$. Thus $0 = p^2 y_2 = pix_1$. As $o(x_1) = p^2$ this implies $p^2 | pi$ so that $p|i$ so we can write $i = pj$ with $0 \leq j < p$. That is: $py_2 = pjx_1$. *Now set* $x_2 = y_2 - jx_1$. Then $px_2 = py_2 - pjx_1 = 0$. Further $x_2 \notin A_1$ since if it were $y_2 = x_2 + jx_1$ would be in A, which it isn't. Set $A_2 = \{jx_2 : 0 \leq j < p\}$. Now $A_1 \cap A_2$ is a subgroup of A_2 but not equal to A_2 since $x_2 \notin A_1$ and hence $A_1 \cap A_2 = \{0\}$. Hence $A_1 + A_2$ has all distinct sums. This gives p^3 sums which thus is all of

G. That is, every $g \in G$ is uniquely expressible as $ix_1 + jx_2$ where $0 \leq i < p^2$ and $0 \leq j < p$. Thus $G \cong Z_{p^2} \times Z_p$, mapping $ix_1 + jx_2$ to (i, j).
`General Case:` $o(G) = p^w$.
Take $x_1 \in G$ with maximal order, say $o(x_1) = p^{a_1}$. If $a_1 = w$ then $G \cong Z_{p^w}$ and done so assume $a_1 < w$. Set $A_1 = \{ix_1 : 0 \leq i < p^{a_1}\}$.

Now $o(G/A_1) = p^{w-a_1}$. By induction on w we can write

$$G/A_1 \cong Z_{p^{a_2}} \times \cdots \times Z_{p^{a_s}}$$

That is, there exist elements $\overline{y_2} \ldots, \overline{y_s} \in G/A_1$ so that

1. $o(\overline{y_i}) = p^{a_i}$
2. Every $\overline{y} \in G/A_1$ is uniquely expressible as

$$\overline{y} = b_2\overline{y_2} + \ldots + b_s\overline{y_s}$$

where $0 \leq b_j < p^{a_j}$ for $2 \leq j \leq s$.

Further as $o(x_1)$ was maximal, $p^{a_1}y = 0$ for all $y \in G$ and hence $\overline{p^{a_1}y} = \overline{0}$ for all y and hence $a_2, \ldots, a_s \leq a_1$. Taking $i = 2$, we have $o(\overline{y_2}) = p^{a_2}$ so $\overline{p^{a_2}y_2} = \overline{0}$ so $p^{a_2}y_2 \in A_1$ so $p^{a_2}y_2 = ix_1$. Multiplying both sides by $p^{a_1-a_2}$ gives $0 = ip^{a_1-a_2}x_1$ which implies $p^{a_1} | ip^{a_1-a_2}$ which implies $p^{a_2} | i$ so that $i = p^{a_2}j$ for some integer j. That is: $p^{a_2}y_2 = p^{a_2}jx_1$. Setting $x_2 = y - jx_1$ we have $p^{a_2}x_2 = 0$ and $\overline{x_2} = \overline{y_2}$. Similarly we find $x_3, \ldots, x_s$. That is, we now have element $\overline{x_2} \ldots, \overline{x_s} \in G/A_1$ so that

1. $o(\overline{x_i}) = p^{a_i}$
2. $o(x_i) = p^{a_i}$.
3. Every $\overline{y} \in G/A_1$ is uniquely expressible as

$$\overline{y} = b_2\overline{x_2} + \ldots + b_s\overline{x_s}$$

where $0 \leq b_j < p^{a_j}$ for $2 \leq j \leq s$.

Now we claim that every $g \in G$ is uniquely expressible as

$$g = b_1x_1 + b_2x_2 + \ldots + b_sx_s$$

where $0 \leq b_j < p^{a_j}$ for $1 \leq j \leq s$. First the expression: As $\overline{g} \in G/A_1$ we can write

$$\overline{g} = b_2\overline{y_2} + \ldots + b_s\overline{y_s}$$

where $0 \leq b_j < p^{a_j}$ for $2 \leq j \leq s$. Thus $\overline{g - (b_2y_2 + \ldots + b_sy_s)} = \overline{0}$ so $g - (b_2y_2 + \ldots + b_sy_s) \in A_1$ so $g - (b_2y_2 + \ldots + b_sy_s) = b_1y_1$ for some $0 \leq b_1 < p^{a_1}$. Second the uniqueness: We need only show 0 has a unique expression. Suppose $0 = b_1y_1 + \ldots + b_sy_s$. Then $\overline{0} = b_2\overline{y_2} + \ldots + b_s\overline{y_s}$ so all $b_2, \ldots, b_s = 0$. Then $0 = b_1y_1$ so $b_1 = 0$.

Therefore we have an isomorphism of G to $Z_{p^{a_1}} \times \cdots Z_{p^{a_s}}$, sending $g = b_1x_1 + b_2x_2 + \ldots + b_sx_s$ into $(b_1, \ldots, b_s)$.