MA2202S Homework 3

Qi Ji (A0167793L)

26th October 2018

As this homework concerns Abelian groups, additive notation will be used throughout. All subgroups are automatically normal.

1

Cauchy's Theorem (finite Abelian groups)**.** Let A be a finite Abelian group of order n. Suppose $p \in \mathbb{N}$ is a prime such that $p \mid n$, then there exists an $v \in A$, $v \neq 0$ such that $p \cdot v = 0$.

Proof. Case of $|A| = 1$ is vacuous. Case where $|A| = 2$ is trivial. Suppose result holds for all groups of size less than n, let A be a Abelian group of order n and let $p \in \mathbb{N}$ be a prime such that $p \mid n$. Let the prime factorisation of n be

$$n = p^e q_1 q_2 \cdots q_r$$

where $q_1, q_2, \ldots, q_r$ are possibly repeated primes of which none are equal to p.

Since we are in the case that $|A| > 1$, take $a \in A \setminus \{ 0 \}$. If the order of a is a multiple of p, then let $\operatorname{ord}(a) = pq'$. By setting $x = q' \cdot a$, we have $p \cdot x = p \cdot (q' \cdot a) = 0$.

In the other case where $p \nmid \operatorname{ord}(a)$, $\operatorname{ord}(a) = \overline{q} \mid q_1 q_2 \cdots q_r$. We generate the cyclic subgroup of a, denoted $\langle a \rangle$. This subgroup is non-trivial as $a \neq 0$, then the quotient group $A / \langle a \rangle$ has size $n/\overline{q}$. Denote that as $p^e \hat{q}$, where $p^e \hat{q}\overline{q} = n$. Since $p^e \hat{q} < n$, use induction hypothesis to find $x + \langle a \rangle \in A / \langle a \rangle$ such that $p \cdot (x + \langle a \rangle) = 0 + \langle a \rangle$ and $x + \langle a \rangle \neq 0 + \langle a \rangle$ or equivalently $x \notin a$.

Then $p \cdot x + \langle a \rangle = p \cdot (x + \langle a \rangle) = 0 + \langle a \rangle$, which shows that $px \in \langle a \rangle$. Let $px = b \in \langle a \rangle$ and $l = \operatorname{ord}(b) \mid \overline{q}$, so in particular $\gcd(p, l) = 1$. Let $c, d \in \mathbb{Z}$ such that $cp + dl = 1$, then

$$\begin{aligned} px &= b \\ &= (cp + dl)b \\ &= cpb + dlb \\ &= pcb \\ p(x - cb) &= 0 \end{aligned}$$

Now $x \neq cb$, because $cb \in \langle a \rangle$ but $x \notin \langle a \rangle$. Setting $v = x - cb$ completes the proof. □

(i)

We proceed via induction on the order of A. Base case when $n = 1$ is vacuously true. Suppose result holds for all finite Abelian groups of order less than n.

Let A have order n and fix a prime divisor p_i of n. Let $p = p_i$ and $e = e_i$.

Set $B = \{ a \in A : p^e \cdot a = 0 \}$.

Claim 0. B is a subgroup of A.

Suppose $b_1, b_2 \in B$, then $p^e b_1 + p^e b_2 = p^e (b_1 + b_2) = 0$, so $b_1 + b_2 \in B$. We are done because B is finite.

Observation 1 (Characterising property)**.** If $p^{e+k} \cdot a = 0$ for some $k \in \mathbb{N}, a \in A$, then $a \in B$.

As $\operatorname{ord}(a) \mid p^{e+k}$, $\operatorname{ord}(a)$ is a power of p, but $\operatorname{ord} a \mid n$ which entails that the power is at most e, hence $p^e \cdot a = 0$.

Claim 2. $B \neq \{ 0 \}$ and $p \mid |B|$.

By Cauchy's theorem, there exist an element of $a \in A$ with order p, so $a \in B$ and B is not trivial. Additionally, by theorem of Lagrange, $\operatorname{ord}(a) = p \mid |B|$.

Claim 3. For any $j \neq i, p_j \nmid |B|$.

Suppose on the contrary that $p_j \mid |B|$, by Cauchy theorem there exists $b \in B, b \neq 0$ such that $p_j \cdot b = 0$. Then we have $\operatorname{ord}(b) \mid p_j$ which implies that $p_j \mid p$ which is absurd.

Now from claim 0, B is a subgroup of A so $|B|$ divides $n = p_1^{e_1} \cdots p_r^{e_r}$. By 2 and 3, $|B| = p^{e'}$ where $1 \leq e' \leq e$ Finally, we claim that $e' = e$, which will complete the proof.

Suppose on the contrary that $e' < e$, then we consider the quotient A/B, which has order $p^{e'-e} \prod_{j \neq i} p_j^{e_j} < n$. By Cauchy theorem, there exists $v + B \in A/B$ such that $v \notin B$ and $p \cdot (v + B) = 0 + B$. Then $p \cdot v \in B$, so by definition of B, there exists $d \in \mathbb{Z}$ such that $p^d \cdot (pv) = 0$ in A, which implies that $p^{d+1} \cdot v = 0$, shows that $v \in B$, a contradiction. □

(ii)

Suppose we have a subgroup $C \subseteq A$ such that $|C| = p_i^{e_i}$, let B_i be B as defined above for p_i. It suffices to show that $C \subseteq B_i$ since both subgroups are of the same size. Let $x \in C$, then $p_i^{e_i} \cdot x = 0$ implying that $\operatorname{ord}(x) \mid p_i^{e_i}$ which shows $x \in B_i$ by observation 1. □

(iii)

Consider the internal sum $B_1 + B_2 + \cdots + B_r$. For any i, consider any $v \in B_i \cap \sum_{j \neq i} B_i$. Then there exists $b_i \in B_i$ for all $i \neq j$ such that

$$v = b_1 + \cdots + b_{i-1} + b_{i+1} + \cdots + b_r$$

letting $\hat{p} = \frac{n}{p_i^{e_i}}$, we see that $\hat{p}$ kills RHS, so $\hat{p}v = 0$ which means that $\operatorname{ord}(v) \mid \hat{p}$. We also have $v \in B_i$ and by characterising property $\operatorname{ord}(v) \mid p_i^{e_i}$. As $\gcd(p_i^{e_i}, \hat{p}) = 1$, $\operatorname{ord}(v) = 1$, so $v = 0$ and the sum is direct.

Given a direct sum, we see that

$$B_1 + B_2 + \cdots + B_r \simeq B_1 \oplus B_2 \oplus \cdots \oplus B_r.$$

The RHS has size $p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} = n$, so the LHS also has the same size. Then as

$$B_1 + B_2 + \cdots + B_r \subseteq A$$

and $|A| = n$, this cardinality argument shows that equality in fact holds. $\square$

(iv)

By Lagrange theorem, $p_1^{f_1} \mid n = p_1^{e_1} \cdots p_r^{e_r}$, which implies that $f_1 \leq e_1$. Let $c \in C$ be arbitrary, then $p_1^{f_1} \cdot c = 0$ which means $c \in B_1$, hence $C \subseteq B_1$. $\square$

(v)

Only one because Sylow p_i-subgroups are unique by (ii).

2

Listing out the invariant factors

- $3 \mid 3 \cdot 3 \cdot 5 \cdot 5$,
- $3 \mid 3 \mid 3 \cdot 5 \cdot 5$,
- $3 \mid 3 \cdot 5 \mid 3 \cdot 5$,
- $5 \mid 3 \cdot 3 \cdot 3 \cdot 5$,
- $3 \cdot 5 \mid 3 \cdot 3 \cdot 5$,
- $3 \cdot 3 \cdot 3 \cdot 5 \cdot 5$.

Which gives the following isomorphism classes

$$\mu_3 \oplus \mu_{225}$$
$$\mu_3 \oplus \mu_3 \oplus \mu_{75}$$
$$\mu_3 \oplus \mu_{15} \oplus \mu_{15}$$
$$\mu_5 \oplus \mu_{135}$$
$$\mu_{15} \oplus \mu_{45}$$
$$\mu_{675}$$

Let A, B be two distinct groups from the list above, let d_A, d_B be the largest invariant factor for A, B respectively. As each invariant factor divides the next, we know that elements in A have order at most d_A, of which one has order exactly d_A, similarly for B. Without loss of generality assume $d_A < d_B$, then it is impossible for A to have an element of order d_B, which shows a structural difference between A and B. $\square$