1 Problem of the Week

There are weekly problems assigned which will be discussed in reading groups. A solution will also be given in the reading group. You are not expected to necessarily complete them, but it will be very useful to look through it and have some ideas about how you might go about solving the problem even if you are very unsure.

Weekly Problem 1. Let G be a finite abelian group where the number of solutions to the equation $x^n = e$ is at most n for all $n \in \mathbb{N}$. Prove that G is cyclic.

You may use the following hint:

Lemma 1.1. $\sum_{d|n} \varphi(d) = n$ where φ denotes the euler-totient function.

Proof. Let $\#G = n$. For every $d|n$, let A_d be the set of elements of order d. Then, A_d can have at most $\varphi(d)$ elements as that is the number of generators for a cyclic subgroup of order d. Also, every $x \in G$ is contained in some A_d so then $n = \sum_{d|n} \#A_d \leq \sum_{d|n} \varphi(d) = n$ and $\#A_d = \varphi(d)$ must hold for all $d \mid n$. Then, $\#A_n = \varphi(n)$ gives an element of order n in G. □

2 Exercises

These are exercises which will be worked through in the reading group. You are more than welcome to try them beforehand, but you are not expected to. Solutions will be posted after the reading section.

1. Prove Lemma 1.1

   Proof. Let G be a cyclic group of order n. Every element in G generates a cyclic subgroup of order dividing n and there are $\varphi(d)$ generators for each unique cyclic subgroup of order d, so summing up the generators gives $\#G = n$. There is no undercounting since we know every element must generate some cyclic subgroup, and no overcounting since every element generates the unique subgroup of its corresponding order. □

2. Show that any finitely generated subgroup of $(\mathbb{Q}, +)$ is cyclic.

   Proof. See my Math 220 Practice Finals 3 Q4 answer here. □

3. Let G be an abelian group such that there is an element of order m and an element of order n. Prove that G has an element of order $\text{lcm}(m, n)$.

   Proof. Let g be an element of order m and h be an element of order n. Then, if $\gcd(m, n) = 1$, we are done as gh is an element of order $mn = \text{lcm}(m, n)$. Now assume that $\gcd(m, n) \neq 1$. Write

   $$m = p_1^{d_1} p_2^{d_2} \dots p_r^{d_r}$$
   $$n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$$

Then, let $M = \{i | d_i \geq e_i\}$ and $N = \{i | d_i < e_i\}$. Now let $m' = \prod_{i \in M} p^{d_i}$ and $n' = \prod_{i \in N} p^{e_i}$. By construction, we have that $\gcd(m'n') = 1$ and also $m'n' = \text{lcm}(m, n)$ so then $g^{m/m'} h^{n/n'}$ has order $m'n' = \text{lcm}(m, n)$ □

4. Here is a lemma that you may use (we will prove it a couple of reading sessions later):

Lemma 2.1 (Cauchy's theorem)**.** Let G be a finite group and p be a prime such that $p \mid \#G$. Then, G has an element of order p

Let G be a finite abelian group such that $H_0 \neq \{e\}$ is the unique subgroup of G that is contained in every subgroup $\neq \{e\}$ in G.

(a) Show that H_0 is cyclic of prime order

Proof. Let G be a finite abelian group and suppose $H_0 \neq \{e\}$ is a subgroup that is contained in every subgroup of G. Assume H_0 does not have prime order, so H_0 has order pm for p is a prime and $m \neq 1$. Then, by Cauchy's theorem we have a subgroup of order p contained in H_0 but $p < pm$ so it is a strict containment, contradicting H_0 being contained in every subgroup of G. It follows that H_0 must be cyclic of prime order generated by some h_0. □

(b) Show that G has prime power order

Proof. Assume for the sake of contradiction that it is not, so $G = p^k m$ where $p \nmid m$. Notice $m = qr$ for some prime q and some $r \in \mathbb{N}$, and by Cauchy's theorem we have a subgroup of order q, call it Q, and p, q are coprime so $H_0 \cap Q = \{e\}$ which implies $H_0 \nsubseteq Q$, a contradiction. Hence, G is of prime power order. Observe that H_0 is a unique subgroup of order p in G. □

(c) (Bonus) Show that G is cyclic (this question requires knowing quotient groups)

Proof. Let $h \in G$ have maximal order p^m. If $m = 1$, G is cyclic as H_0 is the unique subgroup of order p and every element will be in H_0 since their order is less than or equal to p. Hence, assume $m \neq 1$. Observe that $h^{p^{m-1}}$ must then have order p so $H_0 = \langle h^{p^{m-1}} \rangle$ by uniqueness of H_0. I claim $G = \langle h \rangle$. Assume for the sake of contradiction that G is not. Then, consider $G/\langle h \rangle$, which has p power order. By Cauchy's theorem, we have an element $g\langle h \rangle$ of order p in $G/\langle h \rangle$. It follows that $g^p = h^r$ for some $r \in \mathbb{N}$. Now, observe that by p^m being the maximal order in G, $e = (g^p)^{p^{m-1}} = (h^j)^{p^{m-1}} = h^{jp^{m-1}}$. By assumption, $\#h = p^m$ so $p \mid j$. Then,

$$\begin{aligned} g^p &= h^{pn} \\ g^p h^{-pn} &= e \\ (gh^{-n})^p &= e \end{aligned}$$

So $\#\langle gh^{-n} \rangle = p$ and from uniqueness of H_0, $\langle gh^{-n} \rangle = H_0 \subseteq \langle h \rangle$ but this implies $g \in \langle h \rangle$, a contradiction. Hence, we have that $G = \langle h \rangle$ and G is cyclic as required. □

5. Let $n \in \mathbb{N}$ and assume $n \geq 2$. When can $\mathbb{Z}_n$ be decomposed into $\mathbb{Z}_a \times \mathbb{Z}_b$ where $a, b \neq 1$?

   Whenever $n \neq p^k$ for $k \in \mathbb{N}$, p is prime. It is obvious that $\mathbb{Z}_p$ cannot be decomposed further. We will just prove $\mathbb{Z}_{p^2} \ncong \mathbb{Z}_p \times \mathbb{Z}_p$ as the other cases are the exact same.

   Proof. $\mathbb{Z}_{p^2}$ is cyclic of order p^2 so there is an element g of order p^2. Now let $h \in \mathbb{Z}_p \times \mathbb{Z}_p$ so $h = (s, t)$. s, t both have order 1 or p so $h^p = (s^p, t^p) = e$ and thus h has at most order p. It follows that they cannot be isomorphic. □