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.

2 Cyclic groups

Definition 1. A group G is called cyclic if $G = \left\{g^k | k \in \mathbb{Z}\right\}$ for some $g \in G$.

We can think of every cyclic group as either $\mathbb{Z}$ or $\mathbb{Z}/n\mathbb{Z}$, the latter denotes the group of integers mod n under addition. There is a more concrete notion called "isomorphism" for treating groups as the same, which will be explored later.

Definition 2. Let G, H be groups. $\varphi : G \mapsto H$ is called an isomorphism if φ is bijective and for all $x, y \in G$, $\varphi(xy) = \varphi(x)\varphi(y)$. G and H are isomorphic if there exists an isomorphism between G, H.

Notation:

- $\mathbb{Z}/n\mathbb{Z}$ is often written as $\mathbb{Z}_n$
- If G, H are isomorphic, we write $G \cong H$.

Theorem 1. Let G, H be cyclic groups of the same order. Then, $G \cong H$

Proof. Let G, H be cyclic groups of the same order. Then, $G = \left\{g^k | k \in \mathbb{Z}\right\}$ and $H = \left\{h^k | k \in \mathbb{Z}\right\}$ for some $g \in G$ and $h \in H$. One can verify that $\varphi : G \mapsto H$ where $\varphi(g) = h$ is an isomorphism. □

Theorem 2. Let $H \subseteq G$ be a subgroup where G is cyclic. Then, H is cyclic.

Proof. Let G be a cyclic group so $G = \left\{g^k | k \in \mathbb{Z}\right\}$ for some $g \in G$ and $H \subseteq G$ be a subgroup. If $H = \{e\}$, we are done. Then, let a be the minimal natural number such that $g^a \neq e \in H$. I claim $H = \left\{(g^a)^k | k \in \mathbb{Z}\right\}$. Let $g^\ell \in H$ for some $\ell \in \mathbb{Z}$. Then, by Euclidean division, $g^\ell = g^{qa+r} = g^{qa}g^r$ for some $q, r \in \mathbb{Z}$ where $0 \leq r < a$, and by closure in $\left\{(g^a)^k | k \in \mathbb{Z}\right\}$, $g^{\ell - qa} = g^r$ so $g^r \in H$. By minimality of a, $r = 0$, so $g^\ell = g^{qa}$. Hence, $H = \left\{(g^a)^k | k \in \mathbb{Z}\right\}$. □

Theorem 3. Let G be an infinite cyclic group. Then, $G \cong \mathbb{Z}$.

Proof. Let G be an infinite cyclic group. Then, $G = \left\{g^k | k \in \mathbb{Z}\right\}$ for some $g \in G$. One can verify that $\varphi : G \mapsto \mathbb{Z}$ such that $\varphi(g) = 1$ is an isomorphism. □

Theorem 4. Let G be a finite cyclic group of order n. Then, $G \cong \mathbb{Z}/n\mathbb{Z}$, for each divisor d of n, there is a unique subgroup of order d in G.

Proof. Let G be a finite cyclic group of order n so $G = \left\{g^k | k \in \mathbb{Z}\right\}$ for some $g \in G$. One can check that $\varphi(g) = 1$ is an isomorphism between G and $\mathbb{Z}/n\mathbb{Z}$. For subgroups, let $d \mid \#G = n$. Observe that $G = \{e, g, \ldots, g^{n-1}\}$ by $\#G = n$. Then, $H = \langle g^{\frac{n}{d}} \rangle$ has order d. Uniqueness and $\#H = d$ is left for the reader to verify. □

Theorem 5. Let $G = \langle g \rangle$ be a finite cyclic group and $\#G = n$, and $k \in \mathbb{N}$. Then, $\#\langle g^k \rangle = \frac{n}{\gcd(k,n)}$

This will be left for the reader to verify. There are some other theorems mentioned in Jacobson 1.5, they are not extremely important in the grand scheme of things and I will leave it to when you guys actually do 322 or if you decide to do 322. You may read about them out of your own interest. Lemma 1 in page 46 of Jacobson can be quite useful out of the topics not covered.

3 Direct products and finitely generated abelian groups

We will just define the (external) direct product and give a very brief overview on the fundamental theorem of finitely generated abelian groups.

Definition 3. Let G, H be groups under $\cdot, \diamond$ as the operations. Then, we define the (external) direct product of G, H as $G \times H = \{(g, h) | g \in G, h \in H\}$ where multiplication is defined entry-wise, i.e.

$$(g, h) \star (g', h') = (g \cdot g', h \diamond h')$$

There is also the internal direct product, but we will very likely not go through this in the reading group.

We will just mention the fundamental theorem of finitely generated abelian groups, but we will not do much with it in this reading group either.

Theorem 6 (Finitely generated abelian groups)**.** Let G be a finitely generated abelian group. Then, G is isomorphic to a unique direct sum of cyclic groups up to order.

4 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

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

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 $\text{lcm}(m, n)$.

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

   Lemma 4.1 (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

   (b) Show that G has prime power order

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

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 $a, b \neq 1$?