Exercises, week 10.

Exercise 1: Let $n \in \mathbb{N}^*$. Let $g : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ be the map sending $k \in \mathbb{Z}$ to $(k \mod n)$. Sow that g is a group surjective group morphism and describe its kernel.

Exercise 2: Let G be a group, let $x \in G$, let $n \in \mathbb{N}$ such that $x^n = e$. Show that $\text{ord}(x)$ divides n.

Exercise 3: Let H be a subgroup of $\mathbb{Z}$. Prove that there exists $n \in \mathbb{N}$ such that $H = n\mathbb{Z}$ (hint: consider the smallest strictly positive number that belongs to H).

Definition 1: Let G be a group. We say that $x \in G$ is a *generator* of G if all elements of G can be written as x^n for some $n \in \mathbb{Z}$. More formally, it is equivalent to say that the group morphism $\alpha : \mathbb{Z} \to G$ that sends n to $\alpha(n) := x^n$ is surjective. If a group has a generator, we call it *cyclic*.

Exercise 4: Determine if the following groups are cyclic

1. $(\mathbb{Z}, +)$
2. $\mathbb{Z}/n\mathbb{Z}$, for $n > 1$.
3. $(\mathbb{Q}, +)$
4. $(\mathbb{Z} \times \mathbb{Z}, +)$

Exercise 5:

1. Prove that 3 is a generator of $\mathbb{Z}/4\mathbb{Z}$.
2. Prove that 3 is a not generator of $\mathbb{Z}/6\mathbb{Z}$.
3. Let $n \in \mathbb{N}$. Prove that 1 is a generator of $\mathbb{Z}/n\mathbb{Z}$.
4. Let $p, k \in \mathbb{N}$ such that $\gcd(p, k) = 1$. Prove that k is a generator of $\mathbb{Z}/p\mathbb{Z}$.

The end of this exercise sheet is a more conceptual exercise, for those interested. We will characterize the subsets of $(\mathbb{R}, +)$, and prove the following:

Theorem 2: Let H be a subgroup of $(\mathbb{R}, +)$. Then H is either dense or of the form $x\mathbb{Z} := \{xk \mid k \in \mathbb{Z}\}$, for some $x \in \mathbb{R}$.

Recall that a subset $S \subseteq \mathbb{R}$ is *dense* if for all $x, y \in \mathbb{R}$ with $x < y$, there exists an $s \in S$ such that $x < s < y$. The prototypical example of dense subset is $\mathbb{Q}$. Recall also that every bounded-below subset of $\mathbb{R}$ has an infimum, i.e. a greatest lower bound. The precise definition is as follows.

Definition 3: Let $S \subseteq \mathbb{R}$ be any *non-empty* subset. Suppose there exists $m \in \mathbb{R}$ such that for all $s \in S$, $m \leq s$, then we define $\inf(S)$ to be the *necessarily unique* (prove it) real number having the following property:

$$\forall x \in \mathbb{R}, (\forall s \in S, x \leq s \Rightarrow x \leq \inf(S)).$$

For instance, if S is finite, then prove that $\inf(S) = \min(S)$.

Exercise 6: Let H be a subgroup of $(\mathbb{R}, +)$.

1. Suppose $H = \{0\}$. Conclude that Theorem 2 is true in that case.

We can therefore assume that H is not the zero group. We define

$$H^+ := \{x \in H \mid 0 < x\}.$$

2. Show that H^+ is not empty. Thus, we consider $h_0 := \inf(H)$.
3. Suppose $h_0 = 0$. Prove that H is dense.
4. Suppose that $h_0 \neq 0$. Prove that $h_0 \in H$, then that $H = h_0\mathbb{Z}$.
5. Prove Theorem 2.