MAT 302: LECTURE SUMMARY

We began with the following fundamental concept:

Definition (Subgroup)**.** *A subset H of a group G is called a subgroup of G, denoted $H \leq G$, if it is a group under the binary operation of G.*

We came up with several examples of subgroups of $\mathbb{Q}^{\times}$:

(1) $\mathbb{Q}_{>0} = \{\alpha \in \mathbb{Q} \ : \ \alpha > 0\}$ under multiplication.
(2) $\mathbb{Q}^{\times}$
(3) $\{1\}$ (the 'trivial subgroup')
(4) $\{\pm 1\}$
(5) $\{\ldots, \alpha^{-2}, \alpha^{-1}, 1, \alpha, \alpha^2, \ldots\}$ where α is any nonzero rational number

We noted in passing that examples (3) and (4) above were the only finite subgroups of $\mathbb{Q}^{\times}$.

We next came up with examples of subgroups of $\mathbb{Z}$ (under addition):

(1) $\{0\}$ (the trivial subgroup)
(2) $\mathbb{Z}$
(3) the set of all even numbers, which we denoted by $2\mathbb{Z}$
(4) the set of all multiples of 3, which we denoted by $3\mathbb{Z}$

In other words, all the subgroups of $\mathbb{Z}$ we came up with were of the form $n\mathbb{Z}$, for some $n \in \mathbb{N} = \{0, 1, 2, \ldots\}$. The natural question is, are there any others? After taking some time to explore this issue, we proved the following:

Theorem 1. *$H \leq \mathbb{Z}$ if and only if $H = n\mathbb{Z}$ for some $n \in \mathbb{N}$.*

Proof. ($\Longleftarrow$) This is an exercise.

($\Longrightarrow$) We are given $H \leq \mathbb{Z}$. If $H = \{0\}$, we're done. So, we might as well assume that H contains a nonzero element. This implies that H contains at least one positive element. (Why?) Among all positive elements in H, let n be the smallest one. We claim that $H = n\mathbb{Z}$.

Step 1: $n\mathbb{Z} \subseteq H$

> H is a group under addition, which means that it contains both n and $-n$. (Why?) Also H is closed under addition (because it is a group!) from which the claim follows. (Make sure you can explain why.)

Date: February 1st, 2011.

Step 2: $H \subseteq n\mathbb{Z}$

Pick any $h \in H$, and suppose $h \notin n\mathbb{Z}$ (in other words, h isn't a multiple of n). This would mean that h is strictly between two consecutive multiples of n, say, $qn < h < (q+1)n$, which is the same as saying $0 < h - qn < n$. But now we have arrived at a contradiction: on one hand, $h - qn \in H$ (why?), but on the other hand, it is positive and smaller than n. (Why is this a problem?) Therefore, every $h \in H$ is also in $n\mathbb{Z}$.

This concludes the proof.

$\square$