AlgebraNotes01
Subgroups, Cyclic Groups

Exercise 1. Suppose that G is a group and g is a fixed element of G. Then $H = \{h | hg = gh\}$ is a subgroup of G.

Exercise 2. Suppose that G is a group; show that $H = \{h | hx = xh, \forall x \in G\}$ is a subgroup of G. [Note this is called the commutator subgroup of G.] Also show that H is abelian.

Exercise 3. Suppose that G is an abelian group and H and K are both subgroups of G. Then $HK = \{hk | h \in H, k \in K\}$ is a subgroup of G. What about the case where G is not abelian.

Theorem 1.1. Suppose that G is a group and $g \in G$. Then $H = \{g^n | n \in \mathbb{Z}\}$ is a subgroup of G.

Definition. If the subgroup H of theorem 1.1 is all of G then G is said to be a cyclic group and g is called a generator of G.

Theorem 1.2. If G is a cyclic group then G is abelian.

Theorem 1.3. If G is a finite cyclic group with generator g which contains n elements and m is a number that is relatively prime with n then g^m is also a generator of G.

[Hint: recall the number theory theorem that says that if c is the GCD of the integers x and y then there exists integers a and b so that $ax + by = c$.]

Theorem 1.4. If G is a cyclic group and H is a subgroup of G then H is cyclic.

Exercise 4. Let n be a positive integer. Define the relation $\sim$ on the integers $\mathbb{Z}$ by $x \sim y$ if and only if $n|(y - x)$ (i.e. n divides $y - x$).

a. Prove that $\sim$ is an equivalence relation on $\mathbb{Z}$.

We denote the set of equivalence classes by $\mathbb{Z}_n$. For $[x]_n, [y]_n \in \mathbb{Z}_n$ (where $[x]_n$ denotes the equivalence class containing x), define $+_n$ by $[x]_n +_n [y]_n = [x + y]_n$.

b. Prove that $+_n$ is well defined.

c. Prove that $(\mathbb{Z}_n, +_n)$ is a group. [Helpful hint: write the addition table for $\mathbb{Z}_n$.]

Theorem 1.5. If G is a cyclic group then either G is isomorphic to $(\mathbb{Z}, +)$ or to $(\mathbb{Z}_n, +_n)$ for some integer n.

Exercise 5. Repeat exercise 4 with multiplication instead of addition. [Caution: this has a monkeywrench - at least one step is not possible.]