§1 Cyclic Groups

§1.1 Cyclic Subgroup

Let $g \in (G, \circ)$. Notation: $< g >= \{g^n : n \in \mathbb{Z}\}$
Let $g \in (G, +)$. Notation: $< g >= \{ng : n \in \mathbb{Z}\}$

§1.2 Examples

$5 \in \mathbb{Z}$. $< 5 >= \{\dots, -10, -5, 0, 5, \dots\}$
$2 \in \mathbb{Z}$. $< 2 >= \{\text{even integers}\}$
$5 \in \mathbb{Z}_{10}$. $< 5 >= \{0, 5\}$
$6 \in \mathbb{Z}_{10}$. $< 6 >= \{6, 2, 8, 4, 0\}$
$2 \in \mathbb{Z}_{10}$. $< 2 >= \{2, 4, 6, 8, 0\}$
$3 \in \mathbb{Z}_{10}$. $< 3 >= \{3, 6, 9, 2, 5, 8, 1, 4, 7, 0\}$
Note: $< 1 >=< 3 >=< 7 >=< 9 >= \mathbb{Z}_{10}$. These capture the whole group.

Theorem 4.3 - Let G be a group. Let $x \in G$, then $< x >$ is a subgroup of G. Another way of thinking about it: $< x >$ is the smallest subgroup containing x.

Definition / Notation: $< x >$ is the cyclic subgroup generated by x. If $G =< x >$, then G is a cyclic group and x is a generator of G.
Detecting whether or not a subset is a subgroup.
Criteria
(0) Identity element.
(1) Inverse of each element is inside.
(2) Two elements inside, their product is inside.

§1.3 Proof

(0) $x^0 \in< x >$ so $e \in< x >$.
(1) If $g \in< x >$ then $g = x^m$ for some $m \in \mathbb{Z}$. $g^{-1} = x^{-m}$ because $x^{-m} * x^m = x^0 = e$. Therefore $g^{-1} \in< x >$
(2) Let $g, k \in< x >$, then $g = x^m$ and $k = x^n$ for some $m, n \in \mathbb{Z}$so $g \circ h = x^m \circ x^n = x^{m+n} \in< x >$.
Note: Finite groups are really complicated.
The order of x in G equals the smallest $n > 0$ such that $x^n = e$. If $x^n \neq e$ for all $n > 0$ we declare x in G to have infinite order.
Definition / Notation: $|x|$ represents the order of x.

§1.4 Examples

In $\mathbb{Z}_{10}$: $|5| = 2$, $|3| = 10$, $|0| = 1$
3 in $\mathbb{Z}$ has infinite order. All x in Z have infinite order except the identity element.
$2 \in \mathbb{R}^*$. $< 2 >= \{2^n : n \in \mathbb{Z}\} = \{\dots, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, \dots\}$. Infinite order.

Theorem 4.9 - Every cyclic group is abelian (commutative).

§1.5 Proof

Suppose G $=< x >$. For each $g, k \in G$ there exist $m, n \in \mathbb{Z}$ such that $g = x^m$ and $k = x^n$
$g \circ k = x^m * x^n = x^{m+n} = x^{n+m} = x^n + x^m = k \circ g$

§1.6 Practice

$\mathbb{Q}_8$. Quaternians. I'm not sure what the "8" is for.
$< i >= \{1, i, -1, -i\}$
$< -i >= \{1, -i, -1, i\}$
$< 1 >= \{1\}$
$< -1 >= \{-1, 1\}$
$< j >= \{1, j, -1, -j\}$
Note to self: Groups are not necessarily commutative, but cyclic groups are always commutative. Review: Abelian.

§1.7 The group of units modulo n

$U_n = \{m : 1 \leq m < n, \gcd(m, n) = 1\}$
Binary operation: Multiply elements of U_n by computing remainder of xy modulo n.

§1.8 Examples

$U_{10} = \{1, 3, 7, 9\}$
Cayley Table: Can't make the table fast enough. Notes: each element appears once per row.
Changin to U_{15} :
$U_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}$
$U_8 = \{1, 3, 5, 7\}$
$< 1 >= \{1\}$
$< 3 >= \{1, 3\}$
$< 5 >= \{1, 5\}$
$< 7 >= \{1, 7\}$
U_8 is not cyclic. It is commutative because the cayley table is symmetric across $y = -x$.
Remember: U_n is abelian because xy mod n equals yx mod n ((because multiplication in integers is commutative)).
$U_3 = \{1, 2\}$. Is it cyclic. Yes because $< 2 >$ generates it. $< 2 >= \{1, 2\}$
$U_4 = \{1, 3\} =< 3 >$
$U_5 = \{1, 2, 3, 4\} =< 2 >= \{1, 2, 4, 3\} = \{2^0, 2^1, 2^2, 2^3\}$