Cyclic Groups

Definition 1 (Cyclic Group). *A group is called cyclic if it can be generated by a single element.*

Example 1 (C_n). The group $C_n = \mathrm{Sym}(\{1, 2, \ldots, \mathrm{n}\}, \mathrm{s})$, where

$$s = \{(1, 2), \ldots, (i, i + 1), \ldots, (1, n), (n, 1)\}$$

is the permutation group on $\{1, 2, \ldots, n\}$ generated by s. Indeed, for any $1 \le k \le n$, there is a unique symmetry which takes 1 to k, namely the permutation which takes i to $i+k-1$ if $i+k-1 \le n$ and to $i+k+n-1$ if $i+k-1 > n$. But this permutation is s^{k-1}. Since f is a symmetry iff $fsf^{-1} = s$, this also shows that the centralizer of s is C_n. Since $C_n = \{1 = s^0, s, s^2, \ldots, s^{n-1}\}$, the order of C_n is n. The permutation s permutes $1, 2, \ldots, n$ cyclically and is called an n-cycle.

Example 2 (C_∞). The integers $\mathbb{Z}$ under ordinary addition are a cyclic group, being generated by 1 or -1. Via the regular representation, it is isomorphic to the permutation group C_∞ generated by $s = \{(i, i + 1) | i \in \mathbb{Z}\}$. Moreover, as in the previous example, $C_\infty = \mathrm{Sym}(\mathbb{Z}, \mathrm{s})$.

If $(G, \cdot)$ is a group and a is any element of G, the mapping $\phi : \mathbb{Z} \to G$ defined by $\phi(n) = a^n$ is a homomorphism of the additive group of integers into G. Since the image of ϕ is $< a >$, the mapping ϕ is surjective iff $G =< a >$. Assume that $G =< a >$. Now there are two possibilities:

(a) ϕ is injective: This case arises iff $a^k = a^m \implies k = m$ or, equivalently, $a^n = 1 \implies n = 0$. In this case, $\phi : (\mathbb{Z}, +) \xrightarrow{\sim} (G, \cdot)$.

(b) ϕ is not injective: In this case, there is a integer $k \neq 0$ such that $a^k = 0$. The set of all such k, namely $\phi^{-1}(1)$, is a subgroup of $\mathbb{Z}$. In n is the smallest such $k > 0$, then $a^k = 1 \implies n|k$ in virtue of the following Lemma.

Lemma 1. *Every subgroup of $(\mathbb{Z}, +)$ is cyclic. More, precisely, if I is a non-zero subgroup of $(\mathbb{Z}, +)$, then I is generated by the smallest integer n in I, i.e, $I = n\mathbb{Z} = \{kn|k \in \mathbb{Z}\}$.*

Proof. Suppose that $I \neq 0$ and let n be the smallest positive integer in I. If $m \in I$ we have, by the division algorithm, $m = kn + r$ with $0 \le r < n$. But then, $r = m - kn \in I$ which implies $r = 0$. $\square$

We therefore have $a^k = a^m \iff n|k - m$. In particular, $|G| = n$ and $\phi^{-1}(a^k) = k + n\mathbb{Z} = \{k+mn|m \in \mathbb{Z}\}$. If we let $\mathbb{Z}/n\mathbb{Z}$ denote the collection of sets of the form $k+n\mathbb{Z}$, i.e., the integers mod n, the mapping $\phi' : \mathbb{Z}/n\mathbb{Z} \to G$ defined by $\phi'(k + n\mathbb{Z}) = a^k$ is bijective. Morover, there is a unique group structure on $\mathbb{Z}/n\mathbb{Z}$ such that ϕ' is an isomorphism, namely $(k+n\mathbb{Z})+(m+n\mathbb{Z}) = (k+m)+n\mathbb{Z}$. This is the additive group of integers mod n. Applying, this to $G = C_n$, we get an isomorphism of $(\mathbb{Z}/n\mathbb{Z}, +)$ with C_n.

We thus obtain the following result:

Theorem 2. *Every infinite cyclic group is isomorphic to C_∞ and every finite group of order n is isomorphic to C_n.*

Definition 2 (Order of an Element in a Group). *The order of an element a in a group is the order of the cyclic group it generates. It is denoted by $o(a)$.*

Thus $o(a) = \infty$ iff $a^n = 1 \implies n = 0$ or, in additive notation, $na = 0 \implies n = 0$. We have $o(a) = n < \infty$ iff $a^n = 1$ and $a^k \neq 1$ if $1 \le k < n$ or, in additive notation, $na = 0$ and $ka \neq 0$ if $1 \le k < n$.

We now look at the set of subgroups of a cyclic group. The set of subgroups of any group G are partially orderd by inclusion. Moreover, with respect to this partial order, every pair of subgroups H, K of G have a greatest lower bound (glb), namely $H \cap K$, and a least upper bound (lub), namely $< H \cup K >$. Such a partially ordered set is called a lattice. We denote the lattice of subgroups of G by $\mathcal{L}(G)$. If we replace $\subseteq$ by $\supseteq$ we get a lattice $\mathcal{L}_{\text{opp}}(G)$ in which $\text{glb}(H,K) =< H \cup K >$ and $\text{lub}(H,K) = H \cap K$.

The natural numbers are partially ordered by the divisbility relation $|$ where $k|m$ means $\exists n \in \mathbb{N}$ with $m = nk$. The greatest lower bound of two natural numbers m, n is their greatest common divisor $\gcd(m,n)$ and their least upper bound is their least common multiple lcm(m,n). Note that $\gcd(0,0)$ does not exist if greatest is with respect the usual ordering of $\mathbb{N}$. Since $n|m \iff n\mathbb{Z} \supseteq m\mathbb{Z}$, we see that the mapping $n \mapsto n\mathbb{Z}$ is an isomorphism of the lattice $(\mathbb{N}, |)$ with the lattice $\mathcal{L}_{\text{opp}}(\mathbb{Z}, +)$. In particular, we have $d = \gcd(m,n) \iff d\mathbb{Z} = m\mathbb{Z} + n\mathbb{Z}$ and $\ell = \text{lcm(m,n)} \iff \ell\mathbb{Z} = \text{m}\mathbb{Z} \cap \text{n}\mathbb{Z}$.

Theorem 3. *Let $(G, \cdot)$ be a finite cyclic group of order n generated by a and let $\phi : \mathbb{Z} \to G$ be the homomorphism defined by $\phi(k) = a^k$. Then, the mapping $H \mapsto \phi^{-1}(H)$ is an isomorphism of the lattice of subgroups of G with the lattice of subgroups of $(\mathbb{Z}, +)$ which contain $n\mathbb{Z}$.*

Proof. Since $\phi(\phi^{-1}(H)) = H$ it sufices to prove that $I = \phi^{-1}(\phi(I)$ for every subgroup of $\mathbb{Z}$ which contains $n\mathbb{Z}$. For such a subgroup we have $I = d\mathbb{Z}$ with $d|n$ and $\phi(I) =< a^d >$. Hence $\phi^{-1}(\phi(I) = d + n\mathbb{Z} = d\mathbb{Z} = I$. □

Corollary 4. *If $(G, \cdot)$ is a cyclic group of order n and generated by a, the the mapping $d \mapsto < a^d >$ is an isomorphism of the lattice of divisors of n with the lattice $\mathcal{L}_{\text{opp}}(G)$. In H is a subgroup of G and d is the smallest positive integer with $a^d \in H$ then $H =< a^d >$.*

Corollary 5. *If G is a finite cyclic group and $d|n$ there is a unique subgroup H of G of order d. If $G =< a >$ then $H =< a^{n/d} >$.*

This follows from the fact that d is the order of $a^{n/d}$.

September 1, 1998