Cyclic Groups

$$G = < a >= \begin{cases} a^n \quad if \quad (.) \quad ex: \; U(10) =< 3 \geq \{3^n \; n\epsilon Z\} = \{3^0, 3^1 3^2 3^3\} \\ na \quad if \quad (+) \quad ex: \; Z_4 =< 1 >= \{n1 : n\epsilon Z\} = \{0, 1, 2, 3\} \end{cases}$$

Properties of a Cyclic Groups

	Properties	Examples
1.	$\lvert a\rvert = \infty \Rightarrow a^i = a^j \Leftrightarrow i = j$	ex: $In\ (Z, +)\ \forall\ 0 \neq a \in Z: \lvert a\rvert = \infty$ So for $2^3 = 2^j \Leftrightarrow j = 3$
2.	$\lvert a\rvert = n, then$ $< a >= \begin{cases} \{e, a, \dots, a^{n-1}\}\ for\ (.) \\ \{e, 2a, \dots, (n-1)a\}\ for\ (+) \end{cases}$	$ex1$: $(U(10), .), \lvert 9\rvert = 2, then$ $< 9 >= \{e, a^1\} = \{1, 9\}$ $ex2$: $(Z_6, +)\ \lvert 2\rvert = 3\ then$ $< 2 >= \{e, a, 2a\} = \{0, 2, 4\}$
3.	$\lvert a\rvert = n \Rightarrow a^i = a^j \Leftrightarrow n \mid i - j$	$(Z_6, +)\ \lvert 2\rvert = 3$, $2(2) = 4, 20(2) = 4$ $then\ 3 \mid 2 - 20$
4.	$\lvert a\rvert = \lvert < a > \rvert$	$(Z_6, +)\ \lvert 2\rvert = 3\ then$ $< 2 >= \{e, a, 2a\} = \{0, 2, 4\}$ $\lvert < 2 > \rvert = 3$
5.	$\lvert a\rvert = n\ and\ a^k = e \Rightarrow \lvert a\rvert \mid k$	$(Z_6, +)\ \lvert 2\rvert = 3\ then$ $6(2) = 0, 12(2) = 0$ $\Rightarrow 3 \mid 6, 3 \mid 12$
6.	$Let\ \lvert a\rvert = n, then < a^k >=< a^{gcd(n,k)} >$ And $\lvert a^k\rvert = \frac{n}{gcd(n,k)}$	$\lvert a\rvert = 30,$ $then < a^{26} >=< a^2 >$ $since\ gcd(30, 26) = 2$ And $\lvert a^{26}\rvert = \frac{30}{2} = 15$
7.	$Let\ \lvert a\rvert = n, then < a^i >=< a^j > \Leftrightarrow gcd(n, i) = gcd(n, j)$ And $\lvert a^i\rvert = \lvert a^j\rvert \Leftrightarrow gcd(n, i) = gcd(n, j)$	From ex.6 above, $\lvert a\rvert = 30,$ $then < a^{26} >=< a^2 > \Leftrightarrow$ $gcd(30, 26) = gcd(30, 2) = 2$ And $\lvert a^{26}\rvert = \lvert a^2\rvert = \frac{30}{2} = 15$

	Properties	Examples
8.	$Let\ \|a\| = n, < a > = < a^j > \Leftrightarrow gcd(n,j) = 1$ And $\|a\ \ \| = \|< a^j >\| \Leftrightarrow gcd(n,j) = 1$	$(U(10),.), \|9\| = 2, then$ $< 9 > = \{1,9\}$ $gcd(2,3) = 1 \Rightarrow < 9^3 \geq < 9 >$ $< 9^3 > = \{9^{3^0}, 9^{3^1}\} = \{1,9\}$ $\|9\ \ \| = \|< 9^3 >\|$ $gcd(2,5) = 1 \Rightarrow < 9^5 > = < 9 >$
9.	k is a generator of $Z_n \Leftrightarrow gcd(n,k) = 1$	$Find\ the\ all\ generators\ of\ Z_{10}?$ $Z_{10} = < 1 > = < 3 > = < 7 > = < 9 >$
10.	Every subgroup of a cyclic group is cyclic	Clearly
11.	$\|G\| = n, \forall H \leq G, \|H\| \mid \|G\|$	Lagrange's Theorem
12.	$\|G\| = \|< a >\| = n, for\ each\ divisor\ k\|n$ $G\ \ has\ a\ subgroup\ H\ s.t. \|H\| = k$ $and \quad H = < a^{n/k} >$	$U(10) = < 3 >, \|U(10)\| = 4, 2\|4$ $so\ \exists\ a\ subgroup\ H\ of\ order\ 2$ $and\ H = < 3^{4/2} > = < 9 > = \{1,9\}$
13.	Special Case of 12 for $G = Z_n$: $\|Z_n\| = \|< 1 >\| = n\ , for\ each\ divisor\ k\|n,$ $Z_n\ \ has\ a\ subgroup\ H\ s.t. \|H\| = k$ $and \quad H = < n/_k >$	$\|Z_{10}\| = \|< 1 >\| = 10$ $as\ 2\|10, \ \ and \ \ 5\|10$ $\exists\ a\ subgroup\ H\ of\ order\ 2$ $which$ is $H = < 10/_2 > = < 5 > = \{0,5\}$ $\exists\ a\ subgroup\ K\ of\ order\ 5$ $which$ is $K = < 10/_5 > = < 2 > = \{0,2,4,6,8\}$
14.	$\phi(n) = \|U(n)\|$ $= number\ of\ +ve\ integers$ $less\ than\ n\ and\ relatively\ prime\ to\ n.$	$\phi(10) = \|U(10)\| = 4$
15.	$\|G\| = \|< a >\| = n\ if\ d \mid n,\ \ then$ $the\ number\ of\ elements\ of\ order\ d$ $= \phi(d)$	*Ex*: Find the number of elements of order 9 in Z_{70}, Z_{5056}? $= \phi(9)$=6
16.	$For\ arbitrary\ group\ G\ , \|G\| = n,$ $the\ number\ of\ elements\ of\ order\ d$ $is\ \ divisible\ by\ \phi(d)$	