Remark: If G is finite, then every element of G must be of finite order

Def: A group G is called a cyclic group, if $G = \langle g \rangle$ for a suitable element $g \in G$. This element g is then called a generator of G.

Examples: a) $(\mathbb{Z}, +, 0)$ is cyclic with generators 1 and -1.

b) $\mathbb{Z}_7 = \{0,1,2,3,4,5,6\}$ is cyclic, and it turns out, that every element of $G = (\mathbb{Z}_7, +, 0)$ is a generator, not only 1 and $6 = -1$.

c) $\mathbb{Z}_7^{\times} = \{1,2,3,4,5,6\}$ with multiplication and identity 1. Here it turns out that 3 and 5 are elements of order 6 and thus generators of $\mathbb{Z}_7$

One aspect of cyclic groups is clear and results from the fact that powers of the same element always commute:

Observation: G cyclic $\Longrightarrow$ G Abelian.

Prop. Every subgroup of a cyclic group is again cyclic.

Proof. Let G be a cyclic group with generator $g \in G$, and let $H \leq G$. If $H = \{e\}$ then there is nothing to show, as $\{e\}$ is a cyclic group. Otherwise, there exists a nonzero $k \in \mathbb{Z}$ such that $g^k \in H$. Moreover, we may assume that k is positive and smallest possible. Defining $K = \langle g^k \rangle$, we have clearly $K \subseteq H$ and we wish to show that $H \subseteq K$. Let $x \in H$ be arbitrary. Then there exists $l \in \mathbb{Z}$ such that $x = g^l$ because G is cyclic. We have $l = q \cdot k + r$ where $q \in \mathbb{Z}$ and $0 \leq r < k$ and this leads to $x = g^l = (g^k)^q \cdot g^r$. From $x \in H$ and $g^k \in H$ we conclude that $g^r \in H$ which forces $r = 0$ because of the minimality of k. This way we see $x = (g^k)^q \in K$, and this finishes the proof. $\square$

Lemma. Let G be a group and $g \in G$ with $|g| = m$. For any $k \in \mathbb{Z}$ we have $|g^k| = \frac{m}{\gcd(k,m)}$.

Proof: We first observe that

$$(g^k)^{\frac{m}{\gcd(k,m)}} = g^{\frac{k \cdot m}{\gcd(k,m)}} = (g^m)^{\frac{k}{\gcd(k,m)}} = e$$

$\frac{k}{\gcd(k,m)} \in \mathbb{Z}$

For this reason $|g^k| \le \frac{m}{\gcd(k,m)}$.

In order to proceed we need another helping lemma.

Lemma: Let G be a group and $g \in G$ with $|g| = m$. If $g^k = e$, then $m \mid k$.

proof: By definition m is the smallest positive integer such that $g^m = e$. We write $k = q \cdot m + b$ with $0 \le b < m$ and compute $e = g^k = (g^m)^q \cdot g^b = g^b$, which forces by minimality $b = 0$. Hence $m \mid k$. $\square$

Continuation of previous proof.

Assume, the order of g^k is t, ie $|g^k| = t$. Then $g^{kt} = e$, and by the above lemma $m \mid kt$, ie we have $kt = q \cdot m$ for some $q \in \mathbb{Z}$. Let $d = \gcd(k,m)$ and divide both sides by d to arrive at

$$\frac{k}{d} t = q \cdot \frac{m}{d} \quad \text{where } \gcd\left(\frac{k}{d}, \frac{m}{d}\right) = 1.$$

But this immediately shows $\frac{m}{d} \mid t$. Together with the above observation that $(g^k)^{\frac{m}{d}} = e$ we have $|g^k| = \frac{m}{d}$ as desired.

<u>Lemma</u> Let G be an infinite cyclic group with generator g. For all k, n there holds $\langle g^k \rangle \subseteq \langle g^n \rangle \Leftrightarrow n \mid k$.

<u>proof</u>: Let $\langle g^k \rangle \subseteq \langle g^n \rangle$, then $g^k \in \langle g^n \rangle$ and hence $g^k = g^{n \cdot \ell}$ for some $\ell \in \mathbb{Z}$. As the mapping $\mathbb{Z} \to G$, $t \to g^t$ is bijective, this yields $k = n \cdot \ell$ and hence $n \mid k$. The converse is obvious.

<u>Corollary</u>: An infinite cyclic group has 2 generators. (exactly!)

<u>Prop</u> Let G be a finite cyclic group with generator $g \in G$ of order m

a) For each positive divisor $k \mid m$ there exists exactly one subgroup H of G with $|H| = k$, namely $\langle g^{\frac{m}{k}} \rangle$

b) The order of any subgroup of G must be a divisor of m

c) $\langle g^i \rangle \subseteq \langle g^j \rangle \Leftrightarrow \gcd(j, m) \mid i$

d) g^i is a generator of $G \Leftrightarrow \gcd(i, m) = 1$.

proof. a) Let $k \mid m$ be positive and set $t := \frac{m}{k}$. Then by all what we have seen so far, we have $|g^t| = \frac{m}{t} = k$ so $\langle g^t \rangle$ is a subgroup that we desire.

For the uniqueness let H be a subgroup of order k. We know, that H is cyclic, so there is $i \in \mathbb{Z}$ with $H = \langle g^i \rangle$ and of course $|g^i| = k$. Together with $|g^i| = \frac{m}{\gcd(m,i)}$ this shows that $\frac{m}{\gcd(m,i)} = k$ and hence $\gcd(m,i) = \frac{m}{k} = t$. Accordingly $t \mid m$ and $t \mid i$ which leads to $\langle g^i \rangle \subseteq \langle g^t \rangle$ and hence $H = \langle g^t \rangle$ as they both have k elements.

b) Any subgroup of G is cyclic. If $H \leq G$ we have $H = \langle g^i \rangle$ for some i and we conclude $|H| = |g^i| = \frac{m}{\gcd(m,i)}$ which is a divisor of m.

c) Assume $\langle g^i \rangle \subseteq \langle g^j \rangle$. Then $|g^i|$ is a divisor of $|g^j|$ and hence $\frac{m}{\gcd(m,i)} \mid \frac{m}{\gcd(m,j)}$ which is equivalent with $\gcd(m,j) \mid \gcd(m,i)$ which implies $\gcd(m,j) \mid i$.

Going backwards we see that $\gcd(m,j) \mid i$ implies $|g^i| \mid |g^j|$. The cyclic group $\langle g^j \rangle$ contains a unique subgroup of order $|g^i|$ and this is the unique subgroup $\langle g^i \rangle$ of G. Hence $\langle g^i \rangle \subseteq \langle g^j \rangle$

d) We apply (c) to $\langle g^i \rangle = G = \langle g^1 \rangle$

and obtain $\gcd(m,i) \mid 1$ which means $\gcd(m,i) = 1$.

Example: Inspection of $\mathbb{Z}_{12}$:

a) generators are $1, 5, 7, 11$.

b) There exist subgroups of order $1, 2, 3, 4, 6, 12$ these are generated by $12, 6, 4, 3, 2, 1$ in turn.

c) Of course there are alternative generators for the subgroups. For example $\langle 2 \rangle = \langle 10 \rangle$ and $\langle 4 \rangle = \langle 8 \rangle$.

d) Asking, if $\langle 8 \rangle \subseteq \langle 10 \rangle$ leads to $\gcd(12,10) \mid 8$ which is true.