Summary about Cyclic Groups

In the following, $(G, \cdot)$ always denotes a group with identity e.

Definition. *Given $a \in G$, the set $\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$ of all powers of a is clearly a subgroup of G, and is called the* **cyclic** *subgroup generated by a. If $\langle a \rangle = G$, we say that G is a cyclic group. Clearly, $\langle a \rangle$ is Abelian (since $a^i a^j = a^{i+j} = a^j a^i$). The size of $\langle a \rangle$ is called the* **order** *of a and is denoted by $o(a)$ ($|a|$ in some books).*

Theorem. *All subgroups of a cyclic group are cyclic. For a positive integer n, there is exactly one cyclic group of order n up to isomorphism, and there's only one infinite cyclic group up to isomorphism. More precisely, any infinite cyclic group is isomorphic to $(\mathbb{Z}, +)$, and any cyclic group of order n is isomorphic to $(\mathbb{Z}_n, +)$.*

Theorem. *The only subgroups of $(\mathbb{Z}, +)$ are $d\mathbb{Z} := \{dn : n \in \mathbb{Z})$, $d = 0, 1, 2, \ldots$*

[Hint for a proof: let $I \leq \mathbb{Z}$ and start with the smallest positive element of I (if any).]

Theorem. *Let $a \in G$. If a has infinite order, then the elements a^k, $k \in \mathbb{Z}$, are all distinct. That is, if there are distinct integers i and j such that $a^i = a^j$, then a has finite order.*

If a has finite order, then $o(a)$ is equal to the least positive integer r for which $a^r = e$ (and such integers do exist!); in many books this is the definition of order.

If a has finite order r, then $a^k = e$ if and only if $r|k$; and $a^i = a^j$ if and only if $i \equiv j \pmod{r}$. In other words, $\{k : a^k = e\} = r\mathbb{Z}$.

Theorem. *Let $a \in G$ have (finite) order r. If k and r are relatively prime, then $\langle a^k \rangle = \langle a \rangle$. In general, if $k \in \mathbb{Z}$ is arbitrary, then $\langle a^k \rangle = \langle a^{gcd(k,r)} \rangle$.*

Corollary. *Let $a \in G$ have (finite) order r.*

If $gcd(k, n) = 1$ then $o(a^k) = r$.

If k divides r, then the order of a^k is r/k.

For a general $k \in \mathbb{Z}$, the order of a^k is $r/gcd(k, r)$.

Example. The order of 1,2,3,4,5 in $(\mathbb{Z}_{10}, +)$ are 10,5,10,5,2.

Corollary. *If G is a cyclic group of order n, and $d \in \mathbb{N}$, then G has a subgroup of order d if and only if d divides n.*

Note that this is not true for arbitrary groups G: the group A_4 (which has order 12) has no subgroups of order 6. But the statement is true in arbitrary groups when d a prime-power (this is one of the Sylow theorems).