DEF For each group G and each $g \in G$, we put $g^0 = 1$ and for $n \in \mathbb{N}$ define

$$g^n = \underbrace{g \cdots g}_{n \text{ factors}} \quad \& \quad g^{-n} = \underbrace{g^{-1} \cdots g^{-1}}_{n \text{ factors}}, \text{ i.e. } g^{-n} = (g^{-1})^n.$$

THM A (Rules for Powers) For each group G, each $g \in G$, and all $m \& n \in \mathbb{Z}$,

(1) $g^{m+n} = g^m g^n$

(2) $g^{-n} = (g^{-1})^n = (g^n)^{-1}$

(3) $(g^m)^n = g^{mn}$.

Proof. There are many cases: e.g. $m>0, n>0$; $m>0, n<0$; $m<0, n<0$, ..., and some of the arguments are tedious, and will be omitted.

(1)$_{++}$ For $m \& n \in \mathbb{N}$,

$$g^{m+n} = \underbrace{g \cdots g}_{m+n \text{ factors}} = \underbrace{g \cdots g}_{m} \cdot \underbrace{g \cdots g}_{n} = g^m g^n.$$

(3)$_{++}$ For $m \& n \in \mathbb{N}$,

$$(g^m)^n = \underbrace{(g \cdots g)}_{m} \cdots \underbrace{(g \cdots g)}_{m} = \underbrace{g \cdots g}_{mn} = g^{mn}$$

(2)$_{+}$ For $n \in \mathbb{N}$,

$$g^n (g^{-1})^n = \underbrace{g \cdots g}_{n} \cdot \underbrace{g^{-1} \cdots g^{-1}}_{n} = \underbrace{g \cdots g}_{n-1} \cdot \underbrace{g^{-1} \cdots g^{-1}}_{n-1} = \cdots = g \cdot g^{-1} = 1,$$

so by EXERCISE 5 on 8.4, $(g^{-1})^n = (g^n)^{-1}$.

EXERCISE 1. Prove (2) for $n=0$, and (1)&(3) if either $m>0 \& n=0$ or $m=0 \& n>0$

EXERCISE 2. Prove (1) for the case $m<0$ & $n<0$.

Proof of (1_{+-}). Suppose $m\in\mathbb{N}$ and n is a negative integer, i.e. $n=-l$ with $l\in\mathbb{N}$. Then if $m\geq l$, we have $m+n=m-l\geq 0$, so

$$g^{m+n}g^{l}=g^{m-l}g^{l}\overset{(=)}{=}g^{(m-l)+l}=g^{m}.$$

Multiplying on the right by $(g^{l})^{-1}$ gives

$$g^{m+n}=(g^{m+n}g^{l})(g^{l})^{-1}=g^{m}(g^{l})^{-1}\overset{(=)}{=}g^{m}g^{-l}=g^{m}g^{n},$$

Here we have used (1_{++}) or (1_{0+}) at $(=)$ and (2_{+}) at $(=)$. This verifies 1_{+-} in the case $m\geq l$.

EXERCISE 3. Finish the proof of (1_{+-}) by dealing with the case $0<m<l$.

EXERCISE 4. Prove (1) in the case $m<0$, $n<0$.

Proof of (3_{+-}). For $m\in\mathbb{N}$ and n a negative integer, i.e. $n=-l$ with $l\in\mathbb{N}$,

$$(g^{m})^{n}=(g^{m})^{-l}\overset{(=)}{=}((g^{m})^{-1})^{l}\overset{(=)}{=}((g^{-1})^{m})^{l}\overset{(=)}{=}(g^{-1})^{ml}\overset{(=)}{=}g^{-ml}=g^{mn},$$

the three $(=)$ by (2_{+}) and the $(=)$ by (3_{++}).

EXERCISE 5. Prove (3) for the remaining cases $m<0$ & $n>0$ and $m<0$ & $n<0$.

COR. Let g be an element of a group G. Then for all $m,n\in\mathbb{Z}$, g^{m} commutes with g^{n}, i.e. $g^{m}g^{n}=g^{n}g^{m}$.

Proof. $g^{m}g^{n}=g^{m+n}=g^{n+m}=g^{n}g^{m}$.

DEF For each group G and element $g\in G$, the order of g is the least positive integer d for which $g^{d}=1$, if there are such positive integers. If not, g has order ∞.

EXAMPLE. In $\mathbb{Q}^*$ (the multiplicative group of nonzero rational numbers), -1 has order 2 and 2 has order ∞. In $\mathbb{C}^\times$, i has order 4, since the first few positive powers of i are $i^1=i$, $i^2=-1$, $i^3=-i$, $i^4=1$. In S_3, the three-cycle $r=(123)$ has order 3, since

$$r^2 = rr = (123)(123) = (132) = (123)^{-1},$$

so the first few positive powers of r are $r^1=(123)$, $r^2=(132)$, $r^3=1$.

THM B For each group G and each element $g \in G$, the set $\{g^n : n \in \mathbb{Z}\}$, denoted $\langle g \rangle$, is a subgroup of G. If g has infinite order, then the g^n for $n \in \mathbb{Z}$ are all different, so $\langle g \rangle$ is an infinite group. If g has finite order d, then $\langle g \rangle = \{1, g, \cdots, g^{d-1}\}$ and $\langle g \rangle$ has order d. Subgroups of the form $\langle g \rangle$ are called <u>cyclic</u>.

EXAMPLE. In S_3, the subgroups $\{1\}$, $\{1, t\}$ for $t=1,2,3$ and $\{1, r, r^{-1}\}$ are cyclic. However S_3 itself is not cyclic, since by the COR cyclic subgroups are abelian, while S_3 is not abelian (eg. since $(12)(23)=(123)$ while $(23)(12)=(132)$.)

Proof. To show that $\langle g \rangle$ is a subgroup of G, let's use EXERCISE 4 on 8.2: First, $\langle g \rangle \neq \emptyset$ since $g = g^1 \in \langle g \rangle$. Second, for every pair of elements of $\langle g \rangle$, i.e. for g^m & g^n (where $m, n \in \mathbb{Z}$) we have $g^m (g^n)^{-1} = g^m g^{-n} = g^{m-n} \in \langle g \rangle$.

If $g^m = g^n$ for some $m, n \in \mathbb{Z}$ with $m \neq n$, we have

$$g^{m-n} = g^m g^{-n} = g^m (g^n)^{-1} = g^n (g^n)^{-1} = 1$$

Thus some positive power of g is 1 (g^{m-n} if $m > n$ & g^{n-m} if $n < m$). It follows that if g has order ∞, then the g^n for $n \in \mathbb{Z}$ are all different.

Finally, if g has finite order d, then for each $n \in \mathbb{Z}$ we can write $n = dq + r$ with $q \in \mathbb{Z}$, $r \in \mathbb{Z}$ and $0 \le r < d$, so $g^n = g^{dq+r} = g^{dq} g^r = (g^d)^q g^r = g^r$, since $g^d = 1$. Thus $\langle g \rangle = \{1, g, \cdots, g^{d-1}\}$. The elements g^r with $0 \le r < d$ are all different, giving $|\langle g \rangle| = d$, since $g^r = g^s$ with $0 \le r, s < d$ and $r \neq s$ would imply $g^{r-s} = 1$, contradicting the fact that d is the smallest positive integer with $g^d = 1$.

THM C. (Subgroups of Cyclic Groups). Let G be a cyclic group, ie $G = \langle g \rangle$ for some g.
(1) If G is infinite, then each subgroup $\neq 1$ of G has the form $H = \langle g^n \rangle$ for some $n \in \mathbb{N}$, and this H is the only subgroup of index n in G.
(2) If G is finite, ie $G = \langle g \rangle$ with g of order n, then for each divisor d of n, G has exactly one subgroup H of order d; and $H = \langle g^e \rangle$ where $n = de$.

EXERCISE 6 How many different subgroups does a cyclic group of order 6 have?

Proof. (1) Let $H \neq 1$ be a subgroup of an infinite cyclic group $G = \langle g \rangle$. Let n be the least positive integer with $g^n \in H$. Then $(g^n)^k \in H$ for all $k \in \mathbb{Z}$, so $\langle g^n \rangle \subset H$. Conversely, if $g^m \in H$, let $m = kn + r$ with $0 \le r < n$. Then $g^r = g^{m-kn} = g^m (g^n)^{-k} \in H$ (since g^m & $g^n \in H$), so $r = 0$ by the minimality of n. Thus $m = kn$, so $g^m = (g^n)^k \in \langle g^n \rangle$, showing $H \subset \langle g^n \rangle$. Thus we have shown $H = \langle g^n \rangle$.

EXERCISE 7 Prove that the different cosets of $\langle g^n \rangle$ in $\langle g \rangle$ (an infinite cyclic group) are $g^r \langle g^n \rangle$ with $r = 0, 1, \cdots, n-1$.

(2) Let G be finite cyclic of order n, with $G = \langle g \rangle$. It is easy to check that for $n = de$, $\langle g^e \rangle$ is a subgroup of order d in G. Now let H be any subgroup of G, and let e be the least positive integer with $g^e \in H$ (e exists since $g^n = 1 \in H$). Then $\langle g^e \rangle \subset H$ (since $(g^e)^k \in H$ for all $k \in \mathbb{Z}$). Conversely if $g^m \in H$, $m = ke + r$ with $0 \le r < e$ implies $r = 0$, so $g^m \in \langle g^e \rangle$ giving $H = \langle g^e \rangle$. Since $g^n = 1 \in H$ we get $e \mid n$ so $n = de$.