DEF Let A and B be any two groups (not necessarily subgroups of some group G), and let $A\times B$ be the cartesian product of the two sets A and B, i.e. $A\times B$ is the set of all pairs (a,b) with $a\in A$ and $b\in B$. We define "component-wise" multiplication on $A\times B$ by

$$(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2),$$

using the multiplications in the two groups A and B.

THM A If A and B are any two groups, the cartesian product $A\times B$, with component-wise multiplication, is a group, also denoted by $A\times B$ called the (external) direct product of A and B. In $A\times B$ the identity element is $(1,1)$ and the inverse of (a,b) is (a^{-1}, b^{-1}).

EXERCISE 1 Prove Theorem A.

THM B. Let H and K be subgroups of a group G. Assume

(1) both H and K are normal subgroups

(2) $H\cap K = 1$

(3) $HK = G$

$$\begin{tikzcd}[column sep=small] & G \arrow[dl, dash] \arrow[dr, dash] & \\ H \arrow[dr, dash] & & K \arrow[dl, dash] \\ & 1 & \end{tikzcd}$$

Then the map $\varphi : H\times K \to G$ defined by $\varphi((h,k)) = hk$ is an isomorphism, so

$$\boxed{G \cong H\times K}$$

If H and K satisfy (1), (2), (3) we say G is the (internal) direct product of H & K.

Proof. Using (1) and (2) we show first that H and K commute elementwise, i.e.

$$* \quad hk = kh \quad \forall h\in H, k\in K.$$

In fact, for $h\in H$ and $k\in K$,

$$hkh^{-1}k^{-1} = \underbrace{h.kh^{-1}k^{-1}}_{\in H} = \underbrace{hkh^{-1}.k^{-1}}_{\in K} \in H\cap K = 1;$$

the two ⓖ since $H \lhd G$ and $K \lhd G$. From $hkh^{-1}k^{-1}=1$ we get $*$.

We show next that φ is injective. In fact, if $\varphi((h_1,k_1))=\varphi((h_2,k_2))$, i.e.

$$h_1k_1 = h_2k_2$$

then

$$h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K = 1,$$

so $h_1=h_2$ and $k_1=k_2$, so $(h_1,k_1)=(h_2,k_2)$.

It follows from (3) that φ is surjective.

Thus $\varphi: H\times K \to G$ is bijective.

Finally, we show that φ is a homomorphism: For (h_1,k_1) & $(h_2,k_2) \in H\times K$,

$$\begin{aligned}\varphi((h_1,k_1)(h_2,k_2)) &= \varphi((h_1h_2, k_1k_2))\\ &= h_1h_2k_1k_2\\ &= h_1k_1 \cdot h_2k_2 \quad (\text{by } *)\\ &= \varphi((h_1,k_1))\varphi((h_2,k_2)).\end{aligned}$$

Thus φ is a bijective homomorphism, i.e. an isomorphism.

THM.C Let A and B be cyclic groups of orders m and n, and assume $(m,n)=1$. Then the external direct product of A and B is also cyclic, of order mn.

Proof. Since $|A|=m$ and $|B|=n$, we have $|A\times B|=mn$.

Let a and b be generators of A and B, i.e. let $A=\langle a\rangle$ and $B=\langle b\rangle$.

Then a & b have orders m and n. Let l be the order of (a,b). It suffices to show:

$$* \quad l = mn$$

Since the (cyclic) subgroup $\langle(a,b)\rangle$ then has order $mn = |A\times B|$, so $A\times B=\langle(a,b)\rangle$.

The order of (a,b) is the least positive integer l so that $(a,b)^l=(1,1)$, i.e. the least positive integer l so that both $a^l=1$ and $b^l=1$. Since a and b

have orders m and n, we have $m \mid l$ and $n \mid l$. Therefore $[m, n] \mid l$.
Since $(m, n) = 1$, we have $[m, n] = mn$. Therefore

$$\checkmark \qquad mn \mid l.$$

But $|\langle(a, b)\rangle| = l$ and $|A \times B| = mn$, so Lagrange's Theorem gives

$$\checkmark\!\!\checkmark \qquad l \mid mn.$$

Combining $\checkmark$ and $\checkmark\!\!\checkmark$ gives $*$.

EXERCISE 2. Prove that each group of prime order is cyclic.

EXAMPLES. Let A and B be groups of order 2 and 3 (both cyclic, by Exercise 2. Then $A \times B$ is cyclic of order 6 by THM C.

However if A and B each have order 2, then $A \times B$ is not cyclic:
Let $A = \langle a \rangle$ and $B = \langle b \rangle$, so $A = \{1, a\}$ and $B = \{1, b\}$.
Then $A \times B = \{(1,1), (a,1), (1,b), (a,b)\}$ and each element of $A \times B$ except for the identity element, has order 2. For example, $(a,b)^2 = (a^2, b^2) = (1,1) = 1$ so (a,b) has order $\mid 2$, but $(a,b) \neq (1,1)$, so (a,b) has order 2.
In particular, $A \times B$, which has order 4, has no element of order 4, so is not cyclic.

THM D. Let G_1 and G_2 be cyclic groups. If $|G_1| = |G_2|$, then $G_1 \cong G_2$, i.e.

"Cyclic groups of equal order are isomorphic."

EXERCISE 3. Prove Theorem D.

REMARK The simpler statement "Groups of equal order are isomorphic" is false.
For example, $C_2 \times C_2$ is not isomorphic to C_4, nor is S_3 isomorphic to C_6.

DEF An <u>automorphism</u> of a group G is an isomorphism $\alpha: G \to G$.

EXERCISE 4 Prove that the set $\mathrm{Aut}(G)$ of all automorphisms of G is a subgroup of S_G.

Semidirect products generalize direct products. We start this time with

DEF If a group G has subgroups H and K so that

(1) K (but not necessarily H) is normal

(2) $H \cap K = 1$

(3) $HK = G$,

then we say that G is the internal semidirect product of H and K, and write $G = H \ltimes K$

THM E. If $G = H \ltimes K$, then each element of G is of the form hk for exactly one pair of elements h, k with $h \in H$, $k \in K$. Also

$$(*) \qquad h_1 k_1 \cdot h_2 k_2 = h_1 h_2 \cdot k_1^{h_2^{-1}} k_2 \quad \text{with} \quad k^h = hkh^{-1}$$

showing how the multiplication in G is determined by

(a) the multiplication in H

(b) the multiplication in K

(c) the map from $K \times H$ to H given by $k, h \mapsto h^k$.

EXERCISE 5 Prove the first statement of the Theorem, using (2) and (3). Then prove equation $(*)$.

EXAMPLE $S_3 = \langle t_1 \rangle \ltimes \langle r \rangle$. In fact, with $t_1 = (23)$ and $r = (123)$,

(1) $\langle r \rangle \triangleleft S_3$, by a previous Exercise, and $\langle t_1 \rangle$ is a subgroup of S_3

(2) $\langle t_1 \rangle \cap \langle r \rangle = 1$

(3) $\langle t_1 \rangle \langle r \rangle = S_3$, e.g. since $|\langle t_1 \rangle \langle r \rangle| = \dfrac{|\langle t_1 \rangle||\langle r \rangle|}{|\langle t_1 \rangle \cap \langle r \rangle|} = \dfrac{2.3}{1} = 6$.

We will come to external semidirect products later.

EXERCISE 6. Let G be a group and let K be a normal subgroup. For $k \in K$ and $g \in G$ put $\alpha_g(k) = k^g$. Prove that, for each $g \in G$, $\alpha_g \in \operatorname{Aut} K$, and that the map $g \mapsto \alpha_g$ is a homomorphism from G to $\operatorname{Aut} K$.