Def: Let $H$ be a subgroup of a group $G$. Then the number (or cardinality) of left cosets of $H$ in $G$ is called the index of $H$ in $G$, and denoted $(G:H)$.

Examples:

$3\mathbb{Z} < \mathbb{Z}$ \hspace{1em} $(\mathbb{Z}:3\mathbb{Z}) = 3$ \hspace{1em} $|H| = |3\mathbb{Z}| = \infty$

$\mathbb{Q}^* < \mathbb{R}^*$ \hspace{1em} $(\mathbb{R}^*:\mathbb{Q}^*) = \infty$ \hspace{1em} Countable \hspace{1em} $|\mathbb{Q}^*| = 2$

$\mathbb{Z} < \mathbb{R}$ \hspace{1em} $(\mathbb{R}:\mathbb{Z}) = \infty$ \hspace{1em} Uncountable \hspace{1em} $|\mathbb{Z}| = \infty$

If $G$ is finite, then $(G:H) = \frac{|G|}{|H|}$.

(from the proof of Lagrange).

Also $|G| = (G:e)$. So $(G:H) = \frac{(G:e)}{(H:e)}$ (if $G$ is finite).

Thm: Let $K \leq H \leq G$. If $(G:H)$ and $(H:K)$ are both finite, then so is $(G:K)$, and $(G:K) = (G:H)(H:K)$.

Also: if $a \in G$ and $b \in H$ then

$$(ab)H = a(bH)$$

($H$ is normal)

$$(ab)h = ah$$

$ax : x \in bH$$

same $\rightarrow \{(ab)h : h \in H\}$

Idea of proof:

Proof: Following Eq. 38, suppose $(G:H)<\infty$ and $(H:K)<\infty$.

Let $\{a_iH : i = 1,\ldots, r\}$ be the distinct left cosets of $H$ in $G$, and let $\{b_jK : j = 1,\ldots, s\}$ be the distinct left cosets of $K$ in $H$.

We want to show: $\{(a_ib_j)K : i = 1,\ldots, r, j = 1,\ldots, s\}$ are the distinct left cosets of $K$ in $G$.

(1) Clearly all of them are left cosets of $K$ in $G$. 


(2) They're distinct. Suppose \((a_i, b_j)K = (a_\ell b_m)K\)\\\\\(a_i, b_j \in (a_\ell b_m)K\) (because\\\\\(K \subseteq H\))\\\\\(\therefore a_i, b_j = (a_\ell b_m)h_j \) for some \(h_j \in H\)\\\\\(\therefore a_i = a_\ell b_m b_j^{-1}, \) so \(a_i \in a_\ell H, \quad i = \ell, \ldots, \ell\)\\\\\(\therefore H = a_\ell H, \quad i = \ell, \ldots, \ell\)\\\\Now we have \((a_i, b_j)K = (a_\ell b_m)K, \) so \(a_i, b_j \in (a_\ell b_m)K,\) so \(a_i b_j = a_\ell b_m k\) for some \(k \in K.\)\\\\\(\therefore b_j \in b_m K, \) so \(b_j k = b_m k.\) \(j = \ell, \ldots, \ell\)

(3). They give all of the cosets. Let \(g \in G.\) Then \(g \in a_i H,\) for some \(i.\) Write \(g = a_i h,\) for some \(h \in H.\) Then \(k \in K,\) for \(h \in K,\) so \(h = b_j k,\) for some \(k \in K.\)\\\\\(\therefore g = a_i b_j k, \) so \(g \in (a_i, b_j)K.\)\\\\So \(\{(a_i, b_j)K : i = \ell, \ldots, \ell; j = \ell, \ldots, \ell\}\) are the distinct cosets of \(K\) in \(G;\)\\\\\(\therefore (G : K) = \prod (G : H) (H : K).\) \\

It's also true if \((G : K)\) is finite, then so are \((G : H)\) and \((H : K)\) b/c \(\{\text{cosets of } K \text{ in } G\} \rightarrow \{\text{cosets of } H \text{ in } G\}\) is onto and \(\{\text{cosets of } K \text{ in } H\} \rightarrow \{\text{cosets of } C \text{ in } G\}\) is one-to-one.

**On your homework:** \((G : H)\) is also the number (or cardinality) of right cosets of \(H\) in \(G.\)

One last fact (about Lagrange's theorem). Let \(G\) be a finite group and let \(n = |G|\). Then \(a^n = e \iff a \in G.\)

**Proof:** \(l \mid \text{divides } n,\) and \(a^l = e,\) so \(a^n = (a^l)^{n/l} = e^{n/l} = e\) (because \(\text{gcd}(n, l) = 1\)).
Products of groups:

Groups we have so far: cyclic, symmetric, dihedral.

\[ \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^* \]

(under addition) (under multiplication)

Recall that, if \( S_1, \ldots, S_n \) are sets, then their product

\[ S_1 \times \cdots \times S_n = \prod_{i=1}^{n} S_i \]

is the set

\[ \{(s_1, \ldots, s_n) : s_i \in S_i \forall i\} \]

ordered \( n \)-tuples.

Example: \( \mathbb{R}^n = \mathbb{R} \times \cdots \times \mathbb{R} \) (\( n \) times).

**Def.** Let \( G_1, \ldots, G_n \) be groups. Then their product

\[ G_1 \times \cdots \times G_n = \prod_{i=1}^{n} G_i \]

is the set \( \prod_{i=1}^{n} G_i \), with

operation defined componentwise:

\[ (g_1, \ldots, g_n) \times (h_1, \ldots, h_n) = (g_1h_1, \ldots, g_nh_n) \in \prod_{i=1}^{n} G_i \]

It is associative because the operation on each \( G_i \) is associating.

It has identity element \((e, e, \ldots, e)\).

It has an inverse operation \((g_1, \ldots, g_n)^{-1} = (g_1^{-1}, \ldots, g_n^{-1})\).

If all of the \( G_i \) are abelian, then so is \( \prod_{i=1}^{n} G_i \), and we may refer to the product as the direct sum of the \( G_i \):

\[ G_1 \oplus G_2 \oplus \cdots \oplus G_n = \bigoplus_{i=1}^{n} G_i \]

**Caution:** For infinite products of groups (defined similarly), the direct sum is a proper subgroup of the product.

So they're different for infinite products/direct sums.

**Examples:** (i) \( \mathbb{R}^2 = \mathbb{R} \times \mathbb{R} \) (or \( \mathbb{R} \oplus \mathbb{R} \)), adding componentwise (as in the vector space).
(2) \[ \mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1)\} \]

identity \[ \text{order } 2; \text{ e.g. } 2(0,1) = (2 \cdot 0, 2 \cdot 1) = (0,2) \]

This is a group of order 4 and is not cyclic.

\[ \mathbb{Z}_2 \times \mathbb{Z}_2 \cong V, \text{ (Klein } V\text{-group).} \]

\[ (0,0) \mapsto e \]

\[ (0,1) \mapsto a \]

\[ (1,0) \mapsto b \]

\[ (1,1) \mapsto c \]

\[ \text{Isomorphism} \]

(3) \[ \mathbb{Z}_2 \times \mathbb{Z}_3 = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\} \]

identity \[ \text{what is the order?} \]

The order of \((1,1)\) divides 6, and +,

\[ + 2 \quad 2(1,1) = (2 \cdot 1, 2 \cdot 1) = (0,2) \quad \neq (0,0) \]

\[ + 3 \quad 3(1,1) = (3 \cdot 1, 3 \cdot 1) = (1,0) \quad \neq (0,0) \]

\[ \therefore \quad |(1,1)| = 6, \quad \text{so } \mathbb{Z}_2 \times \mathbb{Z}_3 \text{ is cyclic, and isomorphic to } \mathbb{Z}_6. \]

This is an example of:

**Thm:** Let \( m, n \in \mathbb{Z}^+ \). The largest order of an element of \( \mathbb{Z}_m \times \mathbb{Z}_n \) is \([m,n] = \text{lcm}(m,n)\) (this is the smallest \( r > 0 \) such that \( m \mid r \) and \( n \mid r \); the least common multiple of \( m \) and \( n \)).

**Proof:** Let \( 1 \in \mathbb{Z}_m \) have order \( m \), so \( r \cdot 1 = 0 \) in \( \mathbb{Z}_m \iff m \mid r \) (by what we showed earlier). Similarly, let \( 1 \in \mathbb{Z}_n \) have order \( n \), so \( r \cdot 1 = 0 \) in \( \mathbb{Z}_n \iff n \mid r \).

\[ \therefore \quad r \cdot (1,1) = (r \cdot 1, r \cdot 1) \text{ is equal to } (0,0) \iff m \mid r \text{ and } n \mid r. \]

So, the order of \((1,1)\) is the smallest \( r \in \mathbb{Z}^+ \) such that \( r \cdot (1,1) = (0,0) = \text{smallest } r \geq 0 \text{ such that } m \mid r \text{ and } n \mid r \)

\[ = \lfloor m/n \rfloor \]
Also, \( \forall (a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n, \ m \cdot a = 0 \) in \( \mathbb{Z}_m \)
(by what we showed earlier today), so (since \( n \mid (r - a) \)) \( r - a = 0 \) in \( \mathbb{Z}_m \)
\( (r = \text{lcm}(m,n)) \). Similarly \( n \cdot b = 0 \) in \( \mathbb{Z}_n \) because \( n \mid m \) and
\( n \cdot b = 0 \) in \( \mathbb{Z}_n \). \( \cdot n(a,b) = (r-a, n \cdot b) = (0,0) \), so
the order of \( (a,b) \) divides \( r \). In particular, the order \( \leq n \).

In the proof, we also notice that the largest order occurs
with the element \( (1,1) \).