1. If H is a subgroup of G, the *index* $[G{:}H]$ is the number of distinct right cosets gH, where $g \in G$. Note that this is also the number of left cosets Hg, since the bijection $G \xrightarrow{\sim} G$, $g \mapsto g^{-1}$ takes each right coset gH to a left coset Hg^{-1}.

2. *Proposition:* If $[G{:}H] = 2$, then H is a normal subgroup of G.

PROOF: If $[G{:}H] = 2$, then G partitions into right and left cosets as $G = H \cup gH = H \cup Hg$, where g is any element not in H. Thus:

$$gH = G \setminus H = Hg\,,$$

or equivalently $gHg^{-1} = H$, which is the definition of a normal subgroup. (Here $G \setminus H$ means G with the elements of H removed.)

3. *Proposition:* If $n, m > 0$ with $\gcd(n, m) = 1$, then the product of the cyclic groups C_n and C_m is isomorphic to the cyclic group C_{nm} :

$$C_n \times C_m \cong C_{nm}\,.$$

PROOF: Let $C_n = \langle x \rangle$ and $C_m = \langle y \rangle$, so that $C_n \times C_m = \{(x^i, y^j) \mid i, j \in \mathbb{Z}\}$. Of course, these are not all distinct elements, since $x^k = 1$ whenever $n|k$, and $y^k = 1$ whenever $m|k$. Now, let $z := (x, y)$.

I claim z has order nm. Clearly $z^{nm} = (x^{nm}, y^{nm}) = (1, 1) = 1$, so $\mathrm{ord}(z) \le nm$. Now, since $\gcd(n, m) = 1$, we can write $an + bm = 1$ for integers a, b. Thus $z^k = 1$ means $(x^k, y^k) = (1, 1)$, i.e., $n|k$ and $m|k$, so that:

$$nm \,|\, (ank + bmk) = k\,.$$

That is, $z^k = 1 \Longrightarrow nm|k$, and $\mathrm{ord}(z) = nm$.

Therefore $C_n \times C_m = \{z, z^2, \ldots, z^{nm} = 1\}$, which is clearly a cyclic group C_{nm}.

NOTE: Let us rewrite this as: $C_n \times C_m \cong \mathbb{Z}_n^+ \times \mathbb{Z}_m^+$, so that $z \leftrightarrow (1 \bmod n, 1 \bmod m)$ and $z^k \leftrightarrow k(1, 1) = (k \bmod n, k \bmod m)$. Thus, we have the isomorphism:

$$\begin{array}{rcl} \mathbb{Z}_{nm}^+ & \to & \mathbb{Z}_n^+ \times \mathbb{Z}_m^+ \\ k \bmod nm & \mapsto & (k \bmod n\,,\, k \bmod m)\,. \end{array}$$

Since this is an bijection, we get the remarkable fact:

Chinese Remainder Theorem: Suppose n, m are relatively prime. Then for any $i \bmod n$ and $j \bmod m$, there is a unique $k \bmod nm$ such that $k \equiv i \bmod n$ and $k \equiv j \bmod m$.

4. *Proposition:* If G is a group with 6 elements, then G is isomorphic to the cyclic group C_6 or the dihedral group D_3.

Proof: CASE (1) Suppose G has an element x of order 6. Then the cyclic subgroup $\langle x\rangle = \{1, x, x^2, \ldots, x^5\}$ has 6 elements and is all of G, so that G is cyclic.

CASE (2) Suppose G has an element x of order 3, but none of order 6. Taking some element $y \notin \langle x\rangle = \{1, x, x^2\}$, we have:

$$G = \langle x\rangle \cup y\langle x\rangle = \left\{ \begin{array}{ccc} 1, & x, & x^2 \\ y, & yx, & yx^2 \end{array} \right\} .$$

QUESTION: Which of these 6 elements is y^2 ?

- Since the index $[G{:}\langle x\rangle] = 2$, the subgroup $\langle x\rangle$ is normal by Quiz Question 2. Thus we have a quotient group $G/\langle x\rangle = \{\overline{1}, \overline{y}\}$, and clearly $\overline{y}^2 = \overline{1}$, i.e., $y^2 \in \langle x\rangle$.

- If $y^2 = x$, what is the order of y ? We have $y^6 = x^3 = 1$, so $\operatorname{ord}(y)$ divides 6, and $\operatorname{ord}(y) \neq 1, 2$. If $\operatorname{ord}(y) = 3$, then $1 = y^3 = xy$ and $y = x^{-1} = x^2$, which is false. Thus $\operatorname{ord}(y) = 6$, contrary to our assumption. Hence $y^2 = x$ is impossible.

- We can show $y^2 = x^2$ is impossible by an exactly similar argument. For example, if $\operatorname{ord}(y) = 3$, then $1 = y^3 = x^2 y$, so that $y = x^{-2} = x$, which is false.

- The only remaining possiblility is $y^2 = 1$.

QUESTION: What is yxy^{-1} ?

- Since as noted $\langle x\rangle$ is normal, we have $y\langle x\rangle y^{-1} = \langle x\rangle$ and $yxy^{-1} \in \langle x\rangle$.

- Since conjugating does not change the order of an element, we have $\operatorname{ord}(yxy^{-1}) = \operatorname{ord}(x) = 3$. Thus $yxy^{-1} = x$ or x^2.

- If $yxy^{-1} = x$, then $yx = xy$ and:
$$\langle xy\rangle = \{1, xy, x^2y^2, x^3y^3, x^4y^4, x^5y^5\} = \{1, xy, x^2, y, x, x^2y\} ,$$
so that $\operatorname{ord}(xy) = 6$, contrary to assumption. (In other words: $C_2 \times C_3 \cong C_6$.)

- The only remaining possibility is: $yxy^{-1} = x^2$.

SUMMARY: G is generated by elements x, y with $x^3 = y^2 = 1$ and $yx = x^2 y$. But we know that this defines the multiplication table of D_3 , and we have $G \cong D_3$.

CASE (3) Suppose G has only elements of order 1 and 2. Then for any $x \in G$, we have $x^{-1} = x$. For any $x, y \in G$, we have $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$, so G is abelian.

Now consider two distinct elements $x, y \neq 1$, which clearly generate the subgroup:

$$H := \langle x, y\rangle = \{1, x, y, xy\} \cong C_2 \times C_2 .$$

But then G, with 6 elements, could not possibly be partitioned into disjoint cosets of H, each with 4 elements. (Indeed, for any subgroup $H \subset G$, we have $\#H \mid \#G$ for this same reason.) Thus this case is impossible.