Cosets as equivalence classes. Suppose G is a group with a subgroup H. We define a relation $\simeq$ on G as follows:

$$x \simeq y \text{ iff } x^{-1}y \in H.$$

This relation is an equivalence relation. To see this we need to see that it is reflexive, symmetric and transitive. Firstly it is reflexive as $x^{-1}x = 1 \in H$ implies that $x \simeq x$. To see that it is symmetric suppose $x \simeq y$. Then $x^{-1}y \in H$ and as H is a subgroup it follows that $y^{-1}x = (x^{-1}y)^{-1} \in H$ and thus $y \simeq x$. Finally to see that the relation is transitive notice that if $x \simeq y$ and $y \simeq z$ then $x^{-1}y, y^{-1}z \in H$. Being a subgroup, H is closed under the group multiplication and thus $x^{-1}z = (x^{-1}y)\cdot(y^{-1}z) \in H$. Thus $x \simeq z$.

Notice that $x \simeq y$ if and only if $x^{-1}y \in H$ if and only if $y \in xH$. Hence the equivalence class of x is $[x] = xH$, the left coset of H in G.

Theorem 1.1 *(Lagrange) Let G be a finite group with a subgroup H. Then $|H|$ divides $|G|$.*

Proof Using the equivalence relation above, G gets partitioned into pairwise disjoint equivalence classes, say

$$G = a_1H \cup a_2H \cup \cdots \cup a_rH$$

and adding up we get

$$|G| = |a_1H| + |a_2H| + \cdots + |a_rH| = r \cdot |H|.$$

Notice that the map from G to itself that takes g to a_ig is a bijection (the inverse is the map $g \mapsto a_i^{-1}g$) and thus $|a_iH| = |H|$. $\square$

Remark. If we had used instead the relation $x \simeq y$ iff $xy^{-1} \in H$, we would have had $[x] = Hx$. Hence G also partions into a pairwise disjoint union of right cosets. (Recall that in general the partions into right cosets and into left cosets are different).

Examples. (1) The subsets $\{1\}$ and G are always subgroups of G.

(2) The subset $C_n = \{a \in \mathbb{C} : a^n = 1\}$ is a subgroup of $(\mathbb{C}, \cdot)$. In fact $1^n = 1$ and if $a, b \in C_n$ then $(ab)^n = a^nb^n = 1$ and $(a^{-1})^n = (a^n)^{-1} = 1$. Thus both the subgroup criteria (a) and (b) hold.

(3) $H = \{\text{id}, (1, 2)\}$ is a subgroup of S_3. Clearly (a) holds as $\text{id} \in H$ and direct inspection shows that (b) holds as well.

Definition. Let G be a group and $a \in G$. The *cyclic subgroup* generated by a is $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$.

Remark. We have that $1 = a^0 \in \langle a \rangle$. We also have that $\langle a \rangle$ is closed under the group multiplication and taking inverses since $a^n \cdot a^m = a^{n+m}$ and $(a^n)^{-1} = a^{-n}$. Hence $\langle a \rangle$ is a subgroup of G. It is clearly the smallest subgroup of G that contains a.

Definition. We say that a group G is cyclic if there exists an element $a \in G$ where $G = \langle a \rangle$.

Definition. Let G be a group and $a \in G$. The order of a, denoted $o(a)$, is defined as follows. If there is a positive integer m such that $a^m = 1$ then $o(a)$ is the smallest such integer. If there is on the other hand no such positive integer we say that a is of infinite order and write $o(a) = \infty$.

Remarks.(1) If $o(a) = n < \infty$, then

$$\langle a \rangle = \{1 = a^0, a^1, \ldots, a^{n-1}\}$$

where the elments $1, a, a^2, \ldots, a^{n-1}$ are distinct. To see why the elements are different suppose for a contraction that $a^r = a^s$ for some $0 \leq r < s \leq n-1$. But then $a^{s-r} = 1$ where $0 < s - r \leq n - 1 < n$. This however contradicts the fact that $n = o(a)$ is the smallest positive integer where $a^n = 1$.

(2)Thus $o(a) = n = |\langle a \rangle|$. Note also that $a^m = 1$ iff $n|m$. It follows that $a^r = a^s$ if and only if $n|(r - s)$. (The structure of the group is just like that of $\mathbb{Z}_n$).

(3) Let G be a finite group and $a \in G$. As $o(a) = |\langle a \rangle|$ that divides $|G|$ by Lagrange, we have from Remark (2) that $a^{|G|} = 1$.

Let $G = \langle a \rangle$ be a finite cyclic group. By Lagrange any subgroup has a order d that is a divisor of n. For cyclic groups there is conversely exactly one subgroup of order d for each divisor d.

Proposition 1.2 *Let $G = \langle a \rangle$ be a finite cyclic group of order n and let d be a divisor of n. The subgroup $\langle a^{n/d} \rangle$ is the unique subgroup of order d.*

Proof. Let H be a subgroup of order d. As $\langle a^{n/d} \rangle$ has also d elements it suffices to show that $H \subseteq \langle a^{n/d} \rangle$. Let $a^m \in H$. By Remark (3) above we have $1 = a^{m|H|} = a^{md}$ and, by Remark (2), it follows that $n = o(a)$ divides md. Hence n/d divides m, say $m = r \cdot (n/d)$, and $a^m = (a^{n/d})^r \in \langle a^{n/d} \rangle$. $\square$

Proposition 1.3 *Let p be a prime number and G be a group such that $|G| = p$. The group G is cyclic.*

Proof As $p \geq 2$ there has to be some element $a \neq 1$ in G. Then $|\langle a \rangle| \geq 2$ and (by Lagrange's Theorem) $|\langle a \rangle|$ divides $|G| = p$. As p is a prime we must have $|\langle a \rangle| = p$ and thus $\langle a \rangle = G$. $\square$.

III. Congruences and quotient groups.

Definition. Let G be a group. A *congruence* on G is an equivalence relation $\simeq$ on G that satisfies:

$$a_1 \simeq a_2, b_1 \simeq b_2 \Rightarrow a_1 b_1 \simeq a_2 b_2.$$

Remark. This extra condition is needed to introduce a well defined multiplication on the equivalence classes $[a] \cdot [b] = [ab]$.

Lemma 1.4 *Let G be a group with congruence $\simeq$. Then $N = [1]$ is a subgroup of G that satisfies:*

$$g^{-1}Ng \subseteq N$$

for all $g \in G$. Furthermore $a \simeq b$ if and only if $a^{-1}b \in N$.

Proof. To see that N is a subgroup, we go through the subgroup criteria. As $\simeq$ is reflexive we have $1 \simeq 1$ and thus $1 \in N = [1]$. It remains to see that N is closed under group multiplication and taking inverses. For the first of these, notice that of $a, b \in N$ then $a, b \simeq 1$ and the congruence property gives us that $ab \simeq 1 \cdot 1 = 1$. Thus $ab \in N$. To see that N is closed under taking inverses, suppose that $a \in N$ then $a \simeq 1$ and the congruence property gives us that $1 = a^{-1}a \simeq a^{-1} \cdot 1 = a^{-1}$. This shows that $a^{-1} \in N$.

It remains to see that N has the requested extra property. So suppose $a \in N$. Then $a \simeq 1$ and the congruence property implies that $g^{-1}ag \simeq g^{-1} \cdot 1 \cdot g = 1$. Hence $g^{-1}ag \in N$. Finally we have $a \simeq b$ iff $1 = a^{-1}a \simeq a^{-1}b$ iff $a^{-1}b \in [1] = N$. $\square$

Definition. A subgroup H of G is said to be a normal subgroup if

$$g^{-1}Hg \subseteq H \quad \forall g \in G.$$

Notation. We write $H \trianglelefteq G$ or $G \trianglerighteq H$ for 'H is a normal subgroup of G'

Lemma 1.5 *Let G be a group with a normal subgroup N and define a relation $\simeq$ on G by $x \simeq y$ if and only if $x^{-1}y \in N$. Then $\simeq$ is a congruence on G and $[a] = aN$. In particular $[1] = N$.*

Proof We have seen in the proof of Lagrange's Theorem that $\simeq$ is an equivalence relation and that $[a] = aN$. It remains to see that the congruence property holds. So suppose that $a_1 \simeq a_2$ and $b_1 \simeq b_2$. This means that $a_1^{-1}a_2, b_1^{-1}b_2 \in N$. We want to show that $a_1b_1 \simeq a_2b_2$. But this follows from

$$(a_1b_1)^{-1}(a_2b_2) = b_1^{-1}(a_1^{-1}a_2)b_2 = (b_1^{-1}b_2) \cdot b_2^{-1}(a_1^{-1}a_2)b_2.$$

As N is normal we have that $b_2^{-1}(a_1^{-1}a_2)b_2 \in N$ and thus the equation above shows that $(a_1b_1)^{-1}a_2b_2$ is a product of two elements from N. As N is a subgroup of G, this product is in N. Hence $a_1b_1 \simeq a_2b_2$. $\square$

Remark. It follows from Lemmas 1.4 and 1.5 that there is a 1-1 correspondence between congruences on G and normal subgroups of G.

Remarks. (1) We write often more shortly H^a instead of $a^{-1}Ha$ and call it a *conjugate* of H by a. Similarly if $x \in G$ then $x^a = a^{-1}xa$ is a *conjugate* of x by a.

(2) Let $x, a, b \in G$ and 1 be the identity element in G. Then

$$x^{ab} = (ab)^{-1}xab = b^{-1}(a^{-1}xa)b = (x^a)^b$$
$$x^1 = 1^{-1} \cdot x \cdot 1 = x.$$

It follows then that if $H \leq G$ we also have $H^{ab} = (H^a)^b$ and $H^1 = H$.

(3) Notice that H^a is a subgroup of G: firstly $1 = a^{-1} \cdot 1 \cdot a = 1^a \in H^a$ and then $x^a y^a = a^{-1}xaa^{-1}ya = a^{-1}(xy)a = (xy)^a$ and $(x^a)^{-1} = (a^{-1}xa)^{-1} = a^{-1}x^{-1}a = (x^{-1})^a$. In fact the group H^a has the same structure as H. (The conjugation by a is a bit like a renaming or an ornament).

Lemma 1.6 *The following are equivalent:*

(a) $H \trianglelefteq G$,
(b) $H^a = H$ *for all* $a \in G$,
(c) $Ha = aH$ *for all* $a \in G$.

Proof (b)⇒(a) is obvious. To prove (a)⇒(b), notice that (a) implies in particular that for any $a \in G$ we have $H^{a^{-1}} \subseteq H$ and therefore

$$H = H^e = H^{a^{-1}a} = (H^{a^{-1}})^a \subseteq H^a.$$

This gives $H^a = H$. It now only remains to show that (b)⇔(c). But this is easy

$$a^{-1}Ha = H \ \Leftrightarrow a \cdot a^{-1}Ha = aH \ \Leftrightarrow Ha = aH.$$

This finishes the proof. □

Definition. Let G be a group with a subgroup H. The number of left cosets of H in G is called the *index* of H in G and is denoted $[G : H]$.

Remark. Suppose that G is finite. Recall from the proof of Lagrange's Theorem that we get a partition of G into a union of pairwise disjoint union of left cosets

$$G = a_1H \cup a_2H \cup \cdots \cup a_nH.$$

As each of the cosets have order $|H|$, it follows that $|G| = r \cdot |H|$. Hence $[G : H] = r = |G|/|H|$. (Likewise we have that G can be written as a pairwise disjoint union of right cosets and the same reasoning shows that their number is also $|G|/|H|$.

Examples. (1) Every subgroup N of an abelian group G is normal (since then obviously $aN = Na$ for all $a \in G$).

(2) The trivial subgroup $\{1\}$ and G itself are always normal subgroups of G.

(3) If H is a subgroup of G such that $[G : H] = 2$ then $H \trianglelefteq G$ (since the left cosets are $H, G \setminus H$ which are also the right cosets. Hence the right cosets are the same as the left cosets).

The quotient group G/N. Let G be a group with a congruence $\simeq$ and a corresponding normal subgroup N. Let

$$G/N = \{\, [a] = aN : \, a \in G\}$$

with a binary operation $[a] \cdot [b] = [ab]$ (that is $aN \cdot bN = abN$). Notice that this is well defined as $\simeq$ is a congruence. To see that G/N is a group with respect to this binary operation we check that the three group axioms hold.

Firstly there is an identity element, namely $[1] = N$ as $[1] \cdot [a] = [1 \cdot a] = [a]$ and

$[a] \cdot [1] = [a \cdot 1] = [a]$.

Secondly every element $[a] \in G/N$ has an inverse, namely $[a^{-1}]$ since $[a] \cdot [a^{-1}] = [a \cdot a^{-1}] = [1]$ and $[a^{-1}] \cdot [a] = [a^{-1} \cdot a] = [1]$.

Finally associativity in G/N follows from associativity in G:

$$[a] \cdot ([b] \cdot [c]) = [a] \cdot [bc] = [a(bc)] = [(ab)c] = [ab] \cdot [c] = ([a] \cdot [b]) \cdot [c].$$

Remark. That the binary operation on G/N is well defined followed from the fact that $\simeq$ is a congruence. There is another way of seeing this using the fact that N is normal in G. First we introduce set products in the natural way. So if $X, Y \subseteq G$ then we let $X \cdot Y = \{xy : x \in X, y \in Y\}$. Then, using this set product as the action on G/N, we get

$$[a] \cdot [b] = aN \cdot bN = abNN = abN = [ab].$$

Hence the binary operation (being the same as the set multiplication) is well defined. Notice that we used the fact that N is normal when applying $Nb = bN$. Also $N \cdot N \subseteq N$ as N is a subgroup and $N = N \cdot \{1\} \subset N \cdot N$ as $1 \in N$. Thus $N \cdot N = N$.

Remark. Notice that the size of the group G/N is $[G : N]$ and when G is finite this is the same as $|G|/|N|$.

Examples. (1) We always have $G \trianglelefteq G$. The congruence with respect to the normal subgroup G is $x \simeq y \Leftrightarrow x^{-1}y \in G$. As the latter holds for any $x, y \in G$ we are identifying all the elements. Hence

$$G/G = \{[1]\} = \{G\}$$

is the trivial group with only one element.

(2) The trivial subgroup $N = \{1\}$ is always normal in G. The congruence in this case is given by $x \simeq y \Leftrightarrow x^{-1}y \in N \Leftrightarrow x^{-1}y = 1 \Leftrightarrow y = x$. Thus

$$G/N = \{\{a\} : a \in G\}.$$

The structure is just like the structure of G: $\{a\} \cdot \{b\} = \{ab\}$. (The curly bracket is there just as a decoration).

(3) Let $G = S_3 = \{\mathrm{id}, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$ and $N = A_3 = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}$. Here $[G : N] = 2$ and thus G/N has two elements. Notice that these are

$$N = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\} = [\mathrm{id}] = [(1\ 2\ 3)] = [(1\ 3\ 2)]$$

and

$$(1\ 2)N = \{(1\ 2), (2\ 3), (1\ 4)\} = [(1\ 2)] = [(1\ 3)] = [(2\ 3)].$$

(So here we have identified all the even permutations and likewise all the odd permutations). $G/N = \{1 = [\mathrm{id}],\ a = [(1\ 2)]\}$. This is the unique group structure with 2 elements: $1 \cdot a = a \cdot 1 = a$, $1 \cdot 1 = 1$ and $a \cdot a = 1$.