Cosets in groups

Throughout this handout, $(G, \cdot)$ is a group and H is a subgroup of G.

Definition. *For a fixed element $a \in G$, the set $aH := \{ah : h \in H\}$ is called the left coset of H determined by a. Similarly, the set $Ha := \{ha : h \in H\}$ is called the right coset of H determined by a. When we simply talk about "cosets" here, we will always mean left cosets.*

Theorem. *The family $\{aH : a \in G\}$ of all (left-)cosets is a partition of the set G, that is, any two cosets are either disjoint or identical, and $\bigcup_{a\in G} aH = G$.*
A similar statement holds for right cosets.

Let us define a relation $\sim$ on G as: $a \sim b$ whenever $a^{-1}b \in H$. Then $\sim$ is an equivalence relation, and $a \sim b$ iff $a^{-1}b \in H$ iff $(\exists h \in H) b = ah$ iff $b \in aH$.

Proving that $\sim$ is an equvalence relation:
Firstly, $\sim$ is clearly reflexive, since for any $a \in G$, $a^{-1}a = e \in H$. For proving the symmetry of $\sim$, let $a, b \in G$, and assume $a \sim b$. Since H is closed under taking inverse, and $a^{-1}b \in H$, we also have $(a^{-1}b)^{-1} = b^{-1}a \in H$, which proves $b \sim a$. It remains to prove the transitivity of $\sim$. Let $a, b, c \in G$ and assume $a \sim b$ and $b \sim c$. Since $a^{-1}b \in H$ and $b^{-1}c \in H$, and H is closed under multiplication, so $a^{-1}c = (a^{-1}b)(b^{-1}c) \in H$ as required. Thus, $\sim$ is indeed an equivalence relation.

Theorem (Lagrange). *Assume H is finite. Then for any $a \in G$, $|aH| = |H|$. Hence, if G is also finite, then the order of H divides the order of G; the number $[G : H] := |G|/|H|$ is called the* **index** *of H in G, it is the number of different cosets of H.*

Proof. The claim easily follows from the previous theorem and the fact (proved earlier and nicknamed the Sudoku property) that the map $f_a : G \to G : x \mapsto ax$ is a bijection, and hence $f_a : H \to aH : x \mapsto ax$ is one-to-one and also onto (since aH is the range of f_a restricted to the subset H).

Theorem (Product Rule). *Let H be a subgroup of G, K be a subgroup of H, and assume that both indexes $[G : H]$ and $[H : K]$ are finite. Then so is $[G : K]$ and $[G : K] = [G : H][H : K]$.*

Indeed, if $\{a_1, \dots, a_m\}$ are representatives of the cosets of H in G, and $\{b_1, \dots, b_n\}$ are representatives of the cosets of K in H, then $\{a_ib_j : 1 \le i \le m,\ 1 \le j \le n\}$ are easily seen to be representatives of the cosets of K in G.

Remark. While the relation $\sim$ is symmetric, the definition of $\sim$ is intrinsically "left-handed"; a right-handed definition ($a \sim b$ iff $ab^{-1} \in H$) would give a different equivalence relation. The reason is that, in general, the right coset Ha can be different from the left coset aH. As an example, consider S_3 and the subgroup $H = \{123, 213\}$. For $a = 231$, we have $Ha = \{231, 321\}$ while $aH = \{231, 132\}$. However, it is easy to see that for a subgroup of index 2, left and right cosets are the same (a coset must be either H itself or $G \setminus H$). Subgroups for which left- and right-cosets are the same play a critical role in group theory; they are called normal subgroups. Of course, in an Abelian group all subgroups are normal.