Group: A *group* is a set G with an associative operation with an identity e where every element has an inverse. If the operation is commutative, we say that G is commutative or *Abelian*. Examples:

• Any ring under its addition.

• The set R^* of the invertible elements (or units) in a ring R with identity, under multiplication. Important special cases: the non-zero elements of a field; the residues coprime to n in $\mathbf{Z}_n$, here $|\mathbf{Z}_n^*| = \varphi(n)$ where φ is Euler's function; the invertible $n \times n$ matrices over a field, i.e. the ones with non-zero determinants, this group is non-commutative.

• The congruences (or isometries) of the plane or space (i.e. the distance preserving geometric transformations such as reflections, rotations, translations, etc.) form a group under composition.

• Also, the congruences of the plane or space mapping a given figure onto itself form a group under composition. This is called the *symmetry group* (or group of symmetries) of the figure. The symmetry group of a rectangle is called the *Klein group* and is denoted by K. It consists of the identity and the three reflections over the center and the bisectors of the opposite sides. K cannot have more than these four elements since a congruence is completely determined by the images of the vertices, and if we look at the image of a given vertex, it determines the places of the other vertices, as well. Denoting the 3 reflections by a, b, and c, we get $K = \{e, a, b, c\}$ where $a^2 = b^2 = c^2 = e$, $ab = ba = c$, $bc = cb = a$, and $ca = ac = b$, so K is Abelian.

• The symmetry group of a regular n-gon ($n \geq 3$) is called the *dihedral group* of degree n and is denoted by D_n. D_n consists of n rotations around the center by degrees $2k\pi/n$, $0 \leq k \leq n-1$, and n reflections over the n axes of symmetry. D_n cannot have more than these $2n$ elements since a congruence is completely determined by the images of two adjacent vertices, and the first vertex can be mapped into any of the n vertices, and the second vertex must remain its neighbor. Let r denote the rotation by $2\pi/n$ and t be any reflection, then $D_n = \{t^j r^k \mid 0 \leq j \leq 1, 0 \leq k \leq n-1\}$ where $t^2 = r^n = e$ and $rt = tr^{-1}$. This shows that D_n is not commutative.

• In elementary combinatorics, permutations mean all possible orders $i_1, i_2, \ldots, i_n$ of the numbers $1, 2, \ldots, n$. But we can consider permutations also as bijections of the set $\{1, 2, \ldots, n\}$ onto itself. If π is such a bijection and $\pi(j) = i_j$, $j = 1, 2, \ldots, n$, then we write $\pi = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}$. Here $i_1, i_2, \ldots, i_n$ is the "old" permutation. In the new interpretation, we can define the composition of two permutations π and σ as $(\pi\sigma)(j) = \pi(\sigma(j))$, $j = 1, 2, \ldots, n$. These "new" permutations form a group under composition, called the *symmetric group* of degree n and denoted by S_n. Clearly, $|S_n| = n!$, and it is non-Abelian for $n \geq 3$ (as we shall see immediately).

It is more convenient to describe permutations using *cycles*. The cycle denoted by $(i_1, i_2, \ldots, i_k)$ is the permutation which maps i_1 to i_2, i_2 to i_3, etc., and finally i_k to i_1, whereas leaves all other numbers unchanged. Every permutation is the product of disjoint cycles: we pick any element as i_1, take its image as i_2, then i_3 is the image of i_2, etc., until i_1 occurs as an image, and then the cycle gets closed. We pick any element which did not occur sofar and repeat the same process, etc. We see that this representation is essentially unique: no other modifications can be done than to write a cycle of length k in k ways by starting with any of its elements; to change the order of the cycles in the product, as disjoint cycles commute; and to insert or omit the one-element cycles (i.e. the fixed points of the permutation). E.g. $(1,2)(1,3) = (1,3,2)$ and $(1,3)(1,2) = (1,2,3)$ proving that S_n is non-commutative for $n \geq 3$.

The cycles of length 2 are called *transpositions*. Every cycle, hence every permutation is the product of transpositions, e.g. $(1, 2, 3, \ldots, k) = (1, k)(1, k-1) \ldots (1, 3)(1, 2)$. This representation is not unique, since writing the cycle with another first element, we shall get different factors. Even the number of factors is not unique, e.g. we can extend any product by two copies $(ab)(ab)$ of any transposition. But the parity of the factors is unique (see the exercises). A permutation is *even* or *odd* if this number of factors is even or odd, resp. The even permutations form a group A_n called the *alternating group* of degree n. $|A_n| = n!/2$ (for $n \geq 2$) and is non-Abelian for $n \geq 4$.

- The *quaternion group* Q is a non-commutative group of 8 elements: $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ where $(\pm i)^2 = (\pm j)^2 = (\pm k)^2 = -1$ (as if i, j, k were complex units), and $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$ (as if i, j, k were the usual unit vectors in the three-dimensional coordinate system under the cross product).

- A *cyclic group* consists of the powers (with integer exponents) of a single element g called a generator. Notation: $\langle g \rangle$. It is easy to check that in an infinite cyclic group $g^r = g^s \iff r = s$, and in a cyclic group of n elements $g^r = g^s \iff r \equiv s \pmod{n}$. As $g^j g^k = g^{j+k}$, the group operation essentially means addition for the exponents, and so every infinite cyclic group is isomorphic to $\mathbf{Z}$ and every cyclic group of n elements is isomorphic to $\mathbf{Z}_n$. The generators of $\mathbf{Z}$ are 1 or -1, and $\mathbf{Z}_n = \langle t \rangle \iff \gcd(t, n) = 1$. Some other examples for cyclic groups are the even numbers under addition (generated by 2 or -2), the complex nth roots of unity under multiplication (the generators are the primitive nth roots of unity), the non-zero elements of a finite field under multiplication. Every cyclic group is commutative, but the converse is false, the smallest counterexample is K.

Order of an element $g \in G$: $o(g)$ is the smallest positive integer k satisfying $g^k = e$, and $o(g) = \infty$ if there is no such k. This means that in the finite case, the powers of g are periodic and $o(g)$ is the smallest period. This implies $g^r = e \iff o(g) \mid r$, moreover $g^r = g^s \iff r \equiv s \pmod{o(g)}$. We thus see that $o(g)$ is the number of distinct powers of g, i.e. $|\langle g \rangle| = o(g)$. Hence, a finite group G is cyclic iff $|G| = o(g)$ for some $g \in G$. Lagrange's theorem (see below) implies $o(g) \mid |G|$ for $|G| < \infty$. If $o(g) = \infty$, then $g^r = g^s \iff r = s$.

Subgroup: $H \subseteq G$ is a subgroup in the group G if it is a group under the operation of G. Notation: $H \leq G$. When determining whether $H \leq G$, we have to check first that the operation makes sense, i.e. the product of any two elements of H is in H, i.e. H is closed for the operation in G. The associative law holds automatically as $H \subseteq G$. It can be shown that only the identity of G can be the identity of H, and the same applies for the inverses. This implies that $H \leq G$ iff it contains the identity of G, and is closed for the operation in G and for taking inverses. Examples: The complex roots of unity form a subgroup in $\mathbf{C}^*$; the rotations form a subgroup in D_n; $A_n \leq S_n$. It can be shown that every subgroup of a cyclic group is cyclic.

Coset: If $H \leq G$ and $g \in G$, then $gH = \{gh \mid h \in H\}$ is a *left coset*, and $Hg = \{hg \mid h \in H\}$ is a *right coset*. We prove that two left cosets are either disjoint or equal: If $u \in fH \cap gH$, then $u = fh_1 = gh_2$ for some $h_i \in H$. Thus we can express f as $f = gh_2h_1^{-1}$. To show $fH \subseteq gH$, write fh_3 as $fh_3 = (gh_2h_1^{-1})h_3$. Since H is closed for multiplication and inverses, we have $fh = gh_4 \in gH$. The containment $gH \subseteq fH$ follows similarly or by symmetry. Thus the left cosets form a partition of G.

Every left coset is of the same size, as $\varphi : H \to gh$ is a bijection: injectivity follows from multiplying $gh_1 = gh_2$ by g^{-1} from the left to obtain $h_1 = h_2$. As G is the disjoint union of left cosets, each of size $|H|$, we obtain $|G| = |G| \cdot |G : H|$ where $|G : H|$ denotes the number of left cosets called the *index* of H (in G). This is *Lagrange's Theorem.* Thus $|H|$ divides $|G|$ for $|G| < \infty$. As a special case, we get $o(g) \mid |G|$ for finite groups since $|\langle g \rangle| = o(g)$. This yields that if $|G| = p$ where p is a prime, then G is isomorphic to $\mathbf{Z}_p$ since any non-identity element has order p, so G is cyclic generated by any of them.

We can repeat the previous argument also for the right cosets instead of the left ones. If G is finite, then Lagrange's Theorem implies that the number of right cosets is the same as the number of left cosets (namely $|G|/|H|$). This holds also for $|G| = \infty$ using the bijection $gH \mapsto Hg^{-1}$. Therefore the index always means the number (or cardinality) of the (right or left) cosets. Note that the left and right cosets are not necessarily the same.