Definition. Two elements a and b of G are said to be *conjugate in* G if there is some $g \in G$ such that $b = gag^{-1}$ (i.e., if and only if they are in the same orbit of G acting on itself by conjugation). The orbits of G acting on itself by conjugation are called the *conjugacy classes of* G.

Examples

(1) If G is an abelian group then the action of G on itself by conjugation is the trivial action: $g \cdot a = a$, for all $g, a \in G$, and for each $a \in G$ the conjugacy class of a is $\{a\}$.

(2) If $|G| > 1$ then, unlike the action by left multiplication, G does *not* act transitively on itself by conjugation because $\{1\}$ is always a conjugacy class (i.e., an orbit for this action). More generally, the one element subset $\{a\}$ is a conjugacy class if and only if $gag^{-1} = a$ for all $g \in G$ if and only if a is in the center of G.

(3) In S_3 one can compute directly that the conjugacy classes are $\{1\}$, $\{(1\ 2), (1\ 3), (2\ 3)\}$ and $\{(1\ 2\ 3), (1\ 3\ 2)\}$. We shall shortly develop techniques for computing conjugacy classes more easily, particularly in symmetric groups.

As in the case of a group acting on itself by left multiplication, the action by conjugation can be generalized. If S is any subset of G, define

$$gSg^{-1} = \{gsg^{-1} \mid s \in S\}.$$

A group G acts on the set $\mathcal{P}(G)$ of all subsets of itself by defining $g \cdot S = gSg^{-1}$ for any $g \in G$ and $S \in \mathcal{P}(G)$. As above, this defines a group action of G on $\mathcal{P}(G)$. Note that if S is the one element set $\{s\}$ then $g \cdot S$ is the one element set $\{gsg^{-1}\}$ and so this action of G on all subsets of G may be considered as an extension of the action of G on itself by conjugation.

Definition. Two subsets S and T of G are said to be *conjugate in* G if there is some $g \in G$ such that $T = gSg^{-1}$ (i.e., if and only if they are in the same orbit of G acting on its subsets by conjugation).

We now apply Proposition 2 to the action of G by conjugation. Proposition 2 proves that if S is a subset of G, then the number of conjugates of S equals the index $|G : G_S|$ of the stabilizer G_S of S. For action by conjugation

$$G_S = \{g \in G \mid gSg^{-1} = S\} = N_G(S)$$

is the normalizer of S in G. We summarize this as

Proposition 6. The number of conjugates of a subset S in a group G is the index of the normalizer of S, $|G : N_G(S)|$. In particular, the number of conjugates of an element s of G is the index of the centralizer of s, $|G : C_G(s)|$.

Proof: The second assertion of the proposition follows from the observation that $N_G(\{s\}) = C_G(s)$.

The action of G on itself by conjugation partitions G into the conjugacy classes of G, whose orders can be computed by Proposition 6. Since the sum of the orders of these conjugacy classes is the order of G, we obtain the following important relation among these orders.

Theorem 7. *(The Class Equation)* Let G be a finite group and let $g_1, g_2, ..., g_r$ be representatives of the distinct conjugacy classes of G not contained in the center $Z(G)$ of G. Then

$$|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|.$$

Proof: As noted in Example 2 above the element $\{x\}$ is a conjugacy class of size 1 if and only if $x \in Z(G)$, since then $gxg^{-1} = x$ for all $g \in G$. Let $Z(G) = \{1, z_2, ..., z_m\}$, let $\mathcal{K}_1, \mathcal{K}_2, \dots, \mathcal{K}_r$ be the conjugacy classes of G not contained in the center, and let g_i be a representative of $\mathcal{K}_i$ for each i. Then the full set of conjugacy classes of G is given by

$$\{1\},\ \{z_2\},\ \dots,\ \{z_m\},\ \mathcal{K}_1,\ \mathcal{K}_2,\ \dots,\ \mathcal{K}_r.$$

Since these partition G we have

$$\begin{aligned} |G| &= \sum_{i=1}^{m} 1 + \sum_{i=1}^{r} |\mathcal{K}_i| \\ &= |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|, \end{aligned}$$

where $|\mathcal{K}_i|$ is given by Proposition 6. This proves the class equation.

Note in particular that all the summands on the right hand side of the class equation are divisors of the group order since they are indices of subgroups of G. This restricts their possible values (cf. Exercise 6, for example).

Examples

(1) The class equation gives no information in an abelian group since conjugation is the trivial action and all conjugacy classes have size 1.

(2) In any group G we have $\langle g \rangle \le C_G(g)$; this observation helps to minimize computations of conjugacy classes. For example, in the quaternion group Q_8 we see that $\langle i \rangle \le C_{Q_8}(i) \le Q_8$. Since $i \notin Z(Q_8)$ and $|Q_8 : \langle i \rangle| = 2$, we must have $C_{Q_8}(i) = \langle i \rangle$. Thus i has precisely 2 conjugates in Q_8, namely i and $-i = kik^{-1}$. The other conjugacy classes in Q_8 are determined similarly and are

$$\{1\},\quad \{-1\},\quad \{\pm i\},\quad \{\pm j\},\quad \{\pm k\}.$$

The first two classes form $Z(Q_8)$ and the class equation for this group is

$$|Q_8| = 2 + 2 + 2 + 2.$$

(3) In D_8 we may also use the fact that the three subgroups of index 2 are abelian to quickly see that if $x \notin Z(D_8)$, then $|C_{D_8}(x)| = 4$. The conjugacy classes of D_8 are

$$\{1\},\quad \{r^2\},\quad \{r, r^3\},\quad \{s, sr^2\},\quad \{sr, sr^3\}.$$

The first two classes form $Z(D_8)$ and the class equation for this group is

$$|D_8| = 2 + 2 + 2 + 2.$$

Before discussing more examples of conjugacy we give two important consequences of the class equation. The first application of the class equation is to show that groups of prime power order have nontrivial centers, which is the starting point for the study of groups of prime power order (to which we return in Chapter 6).

Theorem 8. If p is a prime and P is a group of prime power order p^α for some $\alpha \geq 1$, then P has a nontrivial center: $Z(P) \neq 1$.

Proof: By the class equation

$$|P| = |Z(P)| + \sum_{i=1}^{r} |P : C_P(g_i)|$$

where $g_1, \dots, g_r$ are representatives of the distinct non-central conjugacy classes. By definition, $C_P(g_i) \neq P$ for $i = 1, 2, \dots, r$ so p divides $|P : C_P(g_i)|$. Since p also divides $|P|$ it follows that p divides $|Z(P)|$, hence the center must be nontrivial.

Corollary 9. If $|P| = p^2$ for some prime p, then P is abelian. More precisely, P is isomorphic to either Z_{p^2} or $Z_p \times Z_p$.

Proof: Since $Z(P) \neq 1$ by the theorem, it follows that $P/Z(P)$ is cyclic. By Exercise 36, Section 3.1, P is abelian. If P has an element of order p^2, then P is cyclic. Assume therefore that every nonidentity element of P has order p. Let x be any nonidentity element of P and let $y \in P - \langle x \rangle$. Since $|\langle x, y \rangle| > |\langle x \rangle| = p$, we must have that $P = \langle x, y \rangle$. Both x and y have order p so $\langle x \rangle \times \langle y \rangle = Z_p \times Z_p$. It now follows directly that the map $(x^a, y^b) \mapsto x^a y^b$ is an isomorphism from $\langle x \rangle \times \langle y \rangle$ onto P. This completes the proof.

Conjugacy in S_n

We next consider conjugation in symmetric groups. Readers familiar with linear algebra will recognize that in the matrix group $GL_n(F)$, conjugation is the same as "change of basis": $A \mapsto PAP^{-1}$. The situation in S_n is analogous:

Proposition 10. Let σ, τ be elements of the symmetric group S_n and suppose σ has cycle decomposition

$$(a_1\, a_2\, \dots\, a_{k_1})\; (b_1\, b_2\, \dots\, b_{k_2}) \dots .$$

Then $\tau\sigma\tau^{-1}$ has cycle decomposition

$$(\,\tau(a_1)\;\tau(a_2)\;\dots\;\tau(a_{k_1})\,)\;(\,\tau(b_1)\;\tau(b_2)\;\dots\;\tau(b_{k_2})\,)\dots,$$

that is, $\tau\sigma\tau^{-1}$ is obtained from σ by replacing each entry i in the cycle decomposition for σ by the entry $\tau(i)$.

Proof: Observe that if $\sigma(i) = j$, then

$$\tau\sigma\tau^{-1}(\tau(i)) = \tau(j).$$

Thus, if the ordered pair i, j appears in the cycle decomposition of σ, then the ordered pair $\tau(i), \tau(j)$ appears in the cycle decomposition of $\tau\sigma\tau^{-1}$. This completes the proof.

Example

Let $\sigma = (1\,2)(3\,4\,5)(6\,7\,8\,9)$ and let $\tau = (1\,3\,5\,7)(2\,4\,6\,8)$. Then

$$\tau\sigma\tau^{-1} = (3\,4)(5\,6\,7)(8\,1\,2\,9).$$

Definition.

(1) If $\sigma \in S_n$ is the product of disjoint cycles of lengths $n_1, n_2, \dots, n_r$ with $n_1 \leq n_2 \leq \cdots \leq n_r$ (including its 1-cycles) then the integers $n_1, n_2, \dots, n_r$ are called the *cycle type* of σ.

(2) If $n \in \mathbb{Z}^+$, a *partition* of n is any nondecreasing sequence of positive integers whose sum is n.

Note that by the results of the preceding section the cycle type of a permutation is unique. For example, the cycle type of an m-cycle in S_n is $1, 1, \dots, 1, m$, where the m is preceded by $n - m$ ones.

Proposition 11. Two elements of S_n are conjugate in S_n if and only if they have the same cycle type. The number of conjugacy classes of S_n equals the number of partitions of n.

Proof: By Proposition 10, conjugate permutations have the same cycle type. Conversely, suppose the permutations σ_1 and σ_2 have the same cycle type. Order the cycles in nondecreasing length, including 1-cycles (if several cycles of σ_1 and σ_2 have the same length then there are several ways of doing this). Ignoring parentheses, each cycle decomposition is a list in which all the integers from 1 to n appear exactly once. Define τ to be the function which maps the i^{th} integer in the list for σ_1 to the i^{th} integer in the list for σ_2. Thus τ is a permutation and since the parentheses which delineate the cycle decompositions appear at the same positions in each list, Proposition 10 ensures that $\tau\sigma_1\tau^{-1} = \sigma_2$, so that σ_1 and σ_2 are conjugate.

Since there is a bijection between the conjugacy classes of S_n and the permissible cycle types and each cycle type for a permutation in S_n is a partition of n, the second assertion of the proposition follows, completing the proof.

Examples

(1) Let $\sigma_1 = (1)(3\ 5)(8\ 9)(2\ 4\ 7\ 6)$ and let $\sigma_2 = (3)(4\ 7)(8\ 1)(5\ 2\ 6\ 9)$. Then define τ by $\tau(1) = 3$, $\tau(3) = 4$, $\tau(5) = 7$, $\tau(8) = 8$, etc. Then

$$\tau = (1\ 3\ 4\ 2\ 5\ 7\ 6\ 9)(8)$$

and $\tau\sigma_1\tau^{-1} = \sigma_2$.

(2) If in the previous example we had reordered σ_2 as $\sigma_2 = (3)(8\ 1)(4\ 7)(5\ 2\ 6\ 9)$ by interchanging the two cycles of length 2, then the corresponding τ described above is defined by $\tau(1) = 3$, $\tau(3) = 8$, $\tau(5) = 1$, $\tau(8) = 4$, etc., which gives the permutation

$$\tau = (1\ 3\ 8\ 4\ 2\ 5)(6\ 9\ 7)$$

again with $\tau\sigma_1\tau^{-1} = \sigma_2$, which shows that there are many elements conjugating σ_1 into σ_2.