CHAPTER VI

GROUP-THEORETIC PROBLEMS

One of the major motivating factors in the investigation of graph isomorphism is the hope that a successful determination of its complexity status will provide new insights into P vs. NP problem. In the preceding chapters, we have developed a number of results which (partially) settle the complexity of testing isomorphism in certain subclasses of graphs. We have concentrated on the group-theoretic approach because it adds a wealth of algebraic properties which may be exploited when determining the automorphism group of a graph. In this development, group-theoretic problems have assumed an auxiliary, although crucial role, and have served to reveal algebraic properties of the problem which were exploited in the design of the algorithms. In this chapter, we reverse this situation and discuss the complexity of group-theoretic problems in the abstract. Although we take graph isomorphism and other combinatorial problems as point of departure, these group-theoretic problems are of interest in their own right, not only as mathematically interesting questions, but also as algorithmic problems with considerable significance for Computer Science. In particular, there is a rich set of such problems which appear to be natural candidates for problems in NP that are neither in P nor are NP-complete.

1. Some Combinatorial Problems as Group-Theoretic Problems

In this section, we translate a number of combinatorial problems, graph isomorphism for one, into purely group-theoretic questions. The purpose of this translation is to expose a (sometimes hidden) algebraic nature of such problems, and to establish a continuity of the present subject with the preceding ones.

In Chapter II, we interpreted the set of isomorphisms between two graphs as a coset of the automorphism group. Our first task is to translate the problem of graph isomorphism into a membership question in double cosets of certain permutation groups, thereby entirely voiding the problem of its topological and combinatorial aspects.
**Definition 1**

Let $A, B < S_n$ be permutation groups of degree $n$. The *double coset* of $A$ and $B$ containing an element $\pi$ of $S_n$ is the set

$$A\pi B = \{ \alpha \pi \beta \mid \alpha \in A, \beta \in B \}$$

of permutations in $S_n$.

In particular, the set $AB = \{ \alpha \beta \mid \alpha \in A, \beta \in B \}$ is the double coset of $A$ and $B$ containing the identity permutation. Since right cosets of $A$ are either disjoint or equal, the double coset $A\pi B$ is the union of some right cosets of $A$. Similarly, it is the union of certain left cosets of $B$. Therefore, both the order of $A$ and the order of $B$ divide the cardinality of $A\pi B$. Specifically, one knows

**Lemma 1**

The cardinality of the double coset $A\pi B$ is $|A\pi B| = \frac{|A| \cdot |B|}{|A\pi \cap B|}$.

The lemma follows from Lemma 20 of Chapter III by putting the element $\alpha \pi \beta$ in $A\pi B$ into 1-1 correspondence with the element $\pi^{-1} \alpha \pi \beta$ of $A\pi B$.

Double cosets are either disjoint or equal. However, the double coset $A\pi B$ need not be of cardinality equal to the cardinality of the double coset $A\psi B$. Thus, double cosets partition the elements of $S_n$ into classes of nonuniform size. We first show that the membership problem for certain double cosets is just graph isomorphism.

Let $X = (V, E)$ be a graph with $n$ vertices, $V = \{1, ..., n\}$. We consider $X$ obtained by superimposing two structures, $L_X$ and $C_X$. Specifically, the structure $C_X$ is the complete graph $K_n = \{(1,...,n), \{(i,j) \mid 1 \leq i < j \leq n\}\}$, and the structure $L_X$ is the pair $(E, \overline{E})$, where $\overline{E}$ is the complement of $E$, i.e., $\overline{E} = \{(i,j) \mid 1 \leq i < j \leq n, (i,j) \notin E\}$. Now superimposing $L_X$ and $C_X$ may be thought of as labelling the edges of $K_n$ with labels of two kinds, "edge" and "not an edge". More abstractly, we consider superimposing $L_X$ onto $C_X$ as a permutation in $\text{Sym}(E \cup \overline{E})$, i.e., a 1-1 map from the set of all unordered pairs $(i,j)$ in $E \cup \overline{E}$ onto all unordered pairs $(i,j)$ in the edge set of $K_n$.

We first investigate when two permutations $\pi$ and $\psi$ in $\text{Sym}(E \cup \overline{E})$ specify the graph $X$ identically. Since we consider the labels in the sets $E$ and $\overline{E}$ indistinguishable, it is clear that exactly the permutations in the right coset $\text{Sym}(E) \times \text{Sym}(\overline{E}) \pi$ specify identical graphs. We set $A = \text{Sym}(E) \times \text{Sym}(\overline{E})$ and note that $A$ is the automorphism group of the *labelling* structure $L_X$. 

Next, we ask when two permutations \( \pi, \psi \in \text{Sym}(E \cup \overline{E}) \) specify isomorphic graphs. Let \( X_\pi \) be the graph specified by \( \pi \), \( X_\psi \) the graph specified by \( \psi \). Then \( X_\psi \) must be obtainable from \( X_\pi \) by a permutation in \( S_n \). So, let \( B \) be the permutation group induced by \( S_n \) on the set of all edges of \( K_n \). Then \( X_\pi \) and \( X_\psi \) are isomorphic iff the permutation \( \psi \) may be obtained as the product \( \alpha \pi \beta \), where \( \alpha \in A \) and \( \beta \in B \), i.e., iff \( \psi \in A \pi B \). Note that \( B \) is the symmetry group of the labelled structure \( C_X \). We therefore obtain

**Proposition 1 (Hoffmann)**

Let \( X = (V, E) \) and \( X' = (V, E') \) be two graphs with \( n \) vertices. Let \( \overline{E} \) and \( \overline{E}' \) be the complement edge sets of \( X \) and \( X' \), respectively. Then \( X \) and \( X' \) are isomorphic iff each permutation \( \psi \in \text{Sym}(E \cup \overline{E}) \) which maps \( E \) onto \( E' \) and \( \overline{E} \) onto \( \overline{E}' \) is in the double coset \( AB \), where \( A = \text{Sym}(E) \times \text{Sym}(\overline{E}) \) and \( B \) is the group of actions of \( \text{Sym}(V) \) on the set \( E \cup \overline{E} \).

The proof is straightforward. Note that if one such permutation \( \psi \) is in \( AB \), then the set of all such permutations is precisely one of the right cosets of \( A \) contained in \( AB \).

**Example 1**

Consider the graph \( X \) of Figure 1 below. Its edge set \( E \) is \( \{a = (1,2), b = (2,3), c = (3,4), d = (4,5), e = (1,5)\} \). The complement set is \( \overline{E} = \{f = (1,3), g = (2,4), h = (3,5), i = (1,4), k = (2,5)\} \). \( X \) is specified by every permutation in \( A = \text{Sym}\{(a,b,c,d,e)\} \times \text{Sym}\{(f,g,h,i,k)\} \). The graph \( X' \) of Figure 2 below
has the edge set $E' = \{a,c,h,i,k\}$ with the complement set $\overline{E}' = \{b,d,e,f,g\}$. This graph may be specified by $\psi = (b,c,h,e,k,g,d,i,f)$, which is a permutation mapping $E$ onto $E'$ and $\overline{E}$ onto $\overline{E}'$. One verifies that $\psi = \alpha \beta$, where $\alpha = (a,e)(b,c)(h,k,i)$ is in $A$ and $\beta = (a,k,e)(b,h,f)(d,i,g)$. Let $B$ be the permutation group induced by $S_6$ on the set $E \cup \overline{E}$. Then $\beta \in B$ since it is induced by the permutation $\varphi = (1,2,5)$, thus $\varphi \in AB$, i.e., the two graphs are isomorphic. Note that the factorization of $\psi$ is not unique. A different factorization is, for example, $\alpha' \beta'$, where $\alpha' = (b,d,e)(f,g,h)$ and $\beta' = (b,k,g)(c,h,d)(e,i,f)$.

More generally, let $L_X$ be a combinatorial structure with the automorphism group $A$, $C_X$ a combinatorial structure with the automorphism group $B$, where $A$ and $B$ are permutation groups with the same permutation domain $V$. Let $\pi \in \text{Sym}(V)$ be a permutation specifying how to superimpose $L_X$ onto $C_X$, thereby obtaining the "labelled" structure $X_\pi$. Then a permutation $\psi \in \text{Sym}(V)$ specifies a structure isomorphic to $X_\pi$ iff $\psi \in A \cap B$.

Next, the automorphism group of the structure specified by $\pi$ is clearly $A^\pi \cap B$: Let $\psi \in \text{Sym}(V)$ be an automorphism of $X_\pi$. Then $\psi$ must also be an automorphism of $C_X$, hence is in $B$. Furthermore, since the structure $L_X$ has been mapped into $(L_X)^\pi$, $\psi$ must be in $A^\pi$. Conversely, it is clear that any permutation in $A^\pi \cap B$ is an automorphism of $X_\pi$. Theorem 7 of Chapter II is a special case of this observation.

Having interpreted double cosets as isomorphism classes, we may consider the number of double cosets into which $\text{Sym}(V)$ is partitioned by the groups $A$ and $B$ as the number of nonisomorphic ways in which the structures $L_X$ and $C_X$ may be superimposed (see also Section 6 below). We therefore know

**Corollary 1**

The number of nonisomorphic graphs with $n$ vertices and $p$ edges is equal to the number of double cosets into which $S_{p+q}$ is partitioned by the subgroups $A$ and $B$, where $A = S_p \times S_q$, $q = \binom{n}{2} - p$, and $B$ is the group induced by $S_n$ on the set of all unordered pairs $(i,j)$, $1 \leq i,j \leq n$, assuming these pairs have been enumerated in some order.

Other combinatorial applications include the number of nonisomorphic graph vertex labellings, e.g., the number of distinct necklaces with $n$ beads and a prescribed number of beads of equal colors, and edge labellings of graphs other than the complete graph $K_n$. 
We determine the number of nonisomorphic graphs with 4 vertices and 3 edges. Assuming a lexicographic enumeration of the unordered pairs \((i,j), 1 \leq i < j \leq 4\), the group \(B\) is generated by the two permutations \((2,4)(3,5)\) and \((1,4,6,3)(2,5)\). We have \(p = 3\) and \(q = 3\), so that \(A = S_3 \times S_3\). By exhaustive enumeration one can prove that \(\{(\), (3,4), (3,5,4)\} is a complete set of representatives for double cosets of \(A\) and \(B\), thus there are exactly 3 nonisomorphic graphs with 3 edges and 4 vertices. The double coset of \(A\) and \(B\) containing \((\)\) consists of 4 right cosets of \(A\), and so does the double coset of \(A\) and \(B\) containing (3,4), but the double coset containing (3,5,4) consists of 12 right cosets of \(A\).

We have translated graph isomorphism into a membership problem of certain double cosets, and graph automorphism into an intersection problem of certain permutation groups. We therefore call the problem of testing membership in a double coset generalized isomorphism, and the problem of determining generators of the intersection of two permutation groups generalized automorphism. We should inquire whether admitting arbitrary permutation groups in this reformulation alters the difficulty of these problems, and we explore this question next.

2. Group-Theoretic Problems of Intermediate Difficulty

We examine some group-theoretic problems which are at least as hard as graph isomorphism, i.e., graph isomorphism can be polynomial time reduced to every one of them. All problems discussed in this section are clearly in \(NP\). Furthermore, the existence problems are polynomial time equivalent to the associated counting problems. For \(NP\)-complete existence problems, the associated counting problems are believed to be more difficult. Therefore, we do not believe that these problems are \(NP\)-complete.

We group the problems loosely by their apparent relatedness. All problems are shown to be polynomially transformable into each other and are therefore of equal difficulty. Furthermore, there are easy reductions establishing that these problems are at least as hard as graph isomorphism.

Throughout this section, we assume that all groups are specified by generating sets of size polynomial in their degree.
2.1. Double Coset Problems

Recall that double cosets may be understood as the equivalence classes of an equivalence relation induced on $S_n$ by the subgroups $A$ and $B$ of $S_n$. That is, $\pi, \psi \in S_n$ are equivalent iff there exists $\alpha \in A$ and $\beta \in B$ such that $\psi = \alpha \pi \beta$. We investigate first the complexity of testing this equivalence given generating sets for $A$ and for $B$. We call this test the **Double Coset Membership Problem**. As pointed out before, the problem is a generalized isomorphism question. Note that Double Coset Membership is clearly a problem in **NP**.

As a subproblem, we consider testing whether $\pi$ is equivalent to the identity permutation $(\cdot)$, i.e., whether $\pi = \alpha \beta$ for some $\alpha \in A$, $\beta \in B$. This **Group Factorization Problem** is of difficulty equal to Double Coset Membership for reasons hinted at in the remark following Lemma 1 above.

The counting problem associated with Group Factorization is determining the number of distinct factorizations $\alpha \beta_1$ of $\pi$ over $A$ and $B$. We show that this problem is no harder than Group Factorization. There are no known **NP-complete** existence problems whose associated counting problems are known to be in **NP**. We therefore view the polynomial time equivalence of Group Factorization and its associated counting problem as evidence against the possibility that the Double Coset Membership Problem is **NP-complete**.

**PROBLEM 1** (Double Coset Membership)

Given the groups $A, B \leq S_n$ by generating sets and the permutations $\pi, \psi \in S_n$, test whether $\psi \in AnB$.

**PROBLEM 2** (Group Factorization)

Given the groups $A, B \leq S_n$ by generating sets and the permutation $\pi \in S_n$, test whether there are $\alpha \in A$, $\beta \in B$, such that $\pi = \alpha \beta$. Equivalently, test whether $\pi \in AB$.

**PROBLEM 3** (Number of Factorizations)

Given the groups $A, B \leq S_n$ by generating sets and the permutation $\pi \in S_n$, determine the number $k \geq 0$ of distinct factorizations $\pi = \alpha \beta$ of $\pi$, where $\alpha \in A$, $\beta \in B$.

Clearly Problem 1 is in **NP**. We show that Problems 1 through 3 are of equal difficulty, i.e. polynomial time equivalent.
**Theorem 1** (Hoffmann)

Problems 1 and 2 are polynomial time equivalent.

**Proof** Since Problem 2 is a special case of Problem 1, we only need to reduce Problem 1 to Problem 2. For this reduction, we recall that the elements $\alpha\pi\beta$ of $A\pi B$ may be put into 1-1 correspondence with the elements $\pi^{-1}\alpha\pi\beta$ of $A^nB$. Thus, $\psi \in A\pi B$ iff $\pi^{-1}\psi \in A^nB$. Since $<K>^n = <K^n>$, this establishes a polynomial time reduction by the results of Chapter II.

In order to show the polynomial time equivalence of Problems 2 and 3, we need the following

**Lemma 2**

If $\pi = \alpha_1\beta_1 = \alpha_2\beta_2 = \cdots = \alpha_k\beta_k$, $\alpha_i \in A$, $\beta_i \in B$, are the distinct factorizations of $\pi$ over $A$ and $B$, then $k = |A \cap B|$.

**Proof** Let $C = A \cap B$. Since $\alpha_i\beta_i = \alpha_i\beta_i$, we have $\alpha_i^{-1}\alpha_i = \beta_i\beta_i^{-1}$, and so $\beta_i$ and $\beta_j$ are in the same right coset of $C$. Furthermore, if $\pi = \alpha\beta$ and $\gamma \in C$, then also $\pi = (\alpha\gamma^{-1})(\gamma\beta) = \alpha'\beta'$, thus the $\beta_i$ form a right coset of $C$. Finally, observe that $\alpha_i$ is uniquely determined by $\pi$ and $\beta_i$, thus $k = |C|$.

**Theorem 2** (Hoffmann)

Problems 2 and 3 are polynomial time equivalent.

**Proof** It is clear that we can reduce Problem 2 to Problem 3 in polynomial time. We establish the converse reduction as follows: First, test whether $\pi \in AB$ using the algorithm for Problem 2. This determines whether to output zero or a positive number. Second, if $\pi \in AB$, then determine $|C|$ with the algorithm below which makes repeated calls on the algorithm for Problem 2.

Let $C = A \cap B$, and let $A^{(0)}$, $B^{(0)}$, and $C^{(0)}$ be the pointwise stabilizers of $\{1, \ldots, i-1\}$ in $A$, $B$, and $C$, respectively. Here $A^{(1)} = A$, $B^{(1)} = B$, $C^{(1)} = C$, and $A^{(n+1)} = B^{(n+1)} = C^{(n+1)} = 1$. By Chapter II, we may assume that we have constructed complete right transversals $U_i$ and $V_i$ for $A^{(i+1)}$ in $A^{(i)}$ and for $B^{(i+1)}$ in $B^{(i)}$, respectively, in polynomial time. We will determine the orbit $\Delta_i$ of $i$ in $C^{(i)}$. Having done so, we can determine $|C|$ from the formula $|C| = \prod_{i=1}^{n} |\Delta_i|$, in polynomial time. Note that $|\Delta_i| \leq n-i+1$.

Let $\pi_i \in U_i$ be a right coset representative for $A^{(i+1)}$ in $A^{(i)}$ mapping $i$ into $j$, i.e., with $i\pi_i = j$. We do the following:
(a) Find \( \psi_i \in V_i \) such that \( i^{(i)} = j \). If there is no such \( \psi_i \), then \( j \) cannot be in \( \Delta_i \).

(b) Let \( \chi = \pi_i \psi_i^{-1} \), where \( \psi_i \) was found in Step (a). Then \( j \in \Delta_i \) iff \( \chi \in A^{(i+1)}B^{(i+1)} \).

The correctness of Step (a) follows trivially from \( C^{(i)} = A^{(i)} \cap B^{(i)} \) and Theorem 3 of Chapter II. For Step (b), observe that \( j \in \Delta_i \) iff there are representatives \( \pi_k \in U_k \) and \( \psi_k \in V_k \), \( i \leq k \leq n \), such that

\[
\varphi = \pi_n \pi_{n-1} \cdots \pi_1 = \psi_n \psi_{n-1} \cdots \psi_i \in C^{(i)}
\]

Thus, \( j \in \Delta_i \) iff

\[
\chi = \pi_i \psi_i^{-1} = \pi^{-1}_{i+1} \cdots \pi^{-1}_n \psi_n \psi_{n-1} \cdots \psi_{i+1} = \pi \psi' \in A^{(i+1)}B^{(i+1)}
\]

Observe that we test at most \( n-i+1 \) products \( \pi_i \psi_i^{-1} \) for membership in \( A^{(i+1)}B^{(i+1)} \). Therefore, the reduction is polynomial time. \( \square \)

2.2. Intersection Problems

Recall Lemma 20 of Chapter III: There is a 1-1 correspondence between the right cosets of \( A \) contained in the double coset \( AB \) and the right cosets of \( A \cap B \) in \( B \). This relationship is also reflected in the interpretation of double cosets and of group intersection as general isomorphism and general automorphism, respectively.

We have exploited the relationship between \( AB \) and \( A \cap B \) in the reduction of Theorem 2 when determining \( |A \cap B| \). We now show that Double Coset Membership is polynomial time equivalent to Group Intersection. Thus the interpretation of the two problems as generalized isomorphism and automorphism, respectively, is accurate in the sense that Theorem 6 of Chapter II remains valid in this generalization.

**Problem 4 (Coset Intersection Emptiness)**

Given the groups \( A, B \in S_n \) by generating sets and given a permutation \( \pi \in S_n \), test whether \( A \pi \cap B \) is empty.

**Problem 5 (Group Intersection)**

Given the groups \( A, B \in S_n \) by generating sets, determine a generating set for \( C = A \cap B \).
**Problem 6 (Setwise Stabilizer)**

Given the group $A < S_n$ by a generating set, and given a subset $X$ of $\{1, \ldots, n\}$, determine a generating set for the setwise stabilizer $A_X$ of $X$ in $A$.

**Lemma 3**

Problems 4 and 2 are polynomial time equivalent.

**Proof** A simple calculation shows that $\pi \in AB$ iff $A\pi \cap B \neq \phi$. 

We will show that Problems 4 through 6 are polynomial time equivalent with Problem 2.

**Theorem 3 (Hoffmann)**

Problem 5 can be reduced to Problem 2 in polynomial time.

**Proof** Recall the proof of Theorem 2. We will extend the algorithm given there and determine generators for $C = A \cap B$. As before, let $A^{(i)}$, $B^{(i)}$, and $C^{(i)}$ denote the pointwise stabilizers of $\{1, \ldots, i-1\}$ in $A$, $B$, and $C$, respectively, and recall that $A^{(1)} = A$, $B^{(1)} = B$, $C^{(1)} = C$, and $A^{(n+1)} = B^{(n+1)} = C^{(n+1)} = I$. Let $U_i$ and $V_i$ be complete right transversals for $A^{(i+1)}$ in $A^{(i)}$ and for $B^{(i+1)}$ in $B^{(i)}$. We will determine complete right transversals $W_i$ for $C^{(i+1)}$ in $C^{(i)}$, $1 \leq i \leq n$.

For each $\pi_1 \in U_i$, we first determine whether $j = \pi_1 i$ is a point in $\Delta_i$, the orbit of $i$ in $C^{(i)}$. Next, we outline how to find a coset representative $\psi_1 \in W_i$ mapping $i$ into $j$, provided Step (b) of the procedure in the proof of Theorem 2 determines that $j$ is in $\Delta_i$. Let $\pi_1$ and $\psi_1$ be the representatives found in Step (b), and recall that

$$
\chi = \pi_1 \psi_1^{-1} \in A^{(i+1)}B^{(i+1)}
$$

iff

$$
\pi_1 \psi_1^{-1} = \pi_{i+1}^{-1} \pi_{i+2}^{-1} \cdots \pi_n^{-1} \psi_n \cdots \psi_{i+2} \psi_{i+1}
$$

where $\pi_{i+k} \in U_{i+k}$ and $\psi_{i+k} \in V_{i+k}$. Therefore,

$$
\chi_i = \pi_i \psi_i^{-1} \in A^{(i+1)}B^{(i+1)}
$$

iff

$$
\chi_{i+k} = \pi_{i+k} \pi_{i+k-1}^{-1} \cdots \pi_i \psi_i^{-1} \cdots \psi_{i+k-1} \psi_{i+k}^{-1} \in A^{(i+k+1)}B^{(i+k+1)}
$$

We proceed as follows: Let $\chi_i = \pi_i \psi_i^{-1} \in A^{(i+1)}B^{(i+1)}$ be the pair of coset representatives
determined by Step (b), and set k to i.

(c) Find a pair $\pi_{k+1} \in U_{k+1}$, $\psi_{k+1} \in V_{k+1}$, such that $\pi_{k+1}X_k\psi_{k+1}^{-1} \in A^{(k+2)}B^{(k+2)}$.

Note that such a pair must always exist.

Repeat Step (c) letting $X_{k+1} = \pi_{k+1}X_k\psi_{k+1}^{-1}$ for the found pair, and increment k until we have determined $X_n = ()$. The desired coset representative is now $\pi_n\pi_{n-1} \cdots \pi_1$, where the $\pi_k$ have been found in Step (c) above.

This procedure makes at most $O(n^3)$ calls on the algorithm for Problem 2. Therefore, we can determine the sets $W_i$ forming a generating set for $C$ by a polynomial time reduction to Problem 2 and therefore, by Lemma 3 above, to Problem 4.

**Theorem 4 (Luks)**

Problems 5 and 6 are polynomial time equivalent.

**Proof** Let $A < S_n$ and $X$ a subset of $\{1, ..., n\}$. Let $\overline{X}$ be the complement of $X$, i.e. $\overline{X} = \{1, ..., n\} - X$. Since $A_X = A \cap \text{Sym}(X) \times \text{Sym}(\overline{X})$, it is clear that Problem 6 can be reduced to Problem 5, in polynomial time.

Conversely, let $A, B < S_n$ be the groups we wish to intersect. We construct the group $D$ isomorphic to $A \times B$ acting on a set of size $n^2$ consisting of all pairs $(i,j)$, $1 \leq i \leq n$. The elements of $D$ are the pairs $(\alpha, \beta)$, where $\alpha \in A$, $\beta \in B$. The action of $(\alpha, \beta)$ is defined by

$$(i,j)(\alpha, \beta) = (i^\alpha, j^\beta).$$

If $A$ and $B$ are generated by the sets $K_A$ and $K_B$ of cardinality $m_1$ and $m_2$, respectively, then we may construct a generating set for $D$ of size $m_1 + m_2$ in polynomial time.

Let $Z = \{(i,i) \mid 1 \leq i \leq n\}$. Then it is clear that the setwise stabilizer $D_Z$ of $Z$ in $D$ is isomorphic to the intersection of $A$ and $B$. Furthermore, using projection, it is easy to construct generators for $A \cap B$ from generators for $D_Z$.

**Theorem 5 (Lipton, Kannan)**

Problem 4 can be reduced to Problem 6 in polynomial time.

**Proof** We wish to test whether $A \pi \cap B$ is empty given an algorithm for Problem 6. We assume that $A, B < \text{Sym}(X)$, and consider the group $D = \{(\alpha, \beta) \mid \alpha \in A, \beta \in B\}$ acting on $X \times X$ by the rule $(x,y)(\alpha, \beta) = (x^\alpha, y^\beta)$. Consider the sets $Z = \{(x,x) \mid x \in X\}$ and $Z' = \{(x^{n-1}, x) \mid x \in X\}$. We test in the manner described below whether $D$ contains an element $\delta$ such that $Z_\delta = Z'$ using an algorithm for Problem 6. Clearly this is the case iff $A \pi \cap B$ is not empty.
So, consider the problem of finding an element $\delta$ in the group $D < \text{Sym}(Y)$ which maps the subset $Z$ of $Y$ onto the subset $Z'$ of $Y$. Here we construct the group $G = D \cap C_2$ acting on the disjoint union $Y_1 \cup Y_2$ of two copies of the set $Y$. Using an algorithm for Problem 6, we determine a generating set for the subgroup $G'$ of $G$ which stabilizes setwise $Z_1 \cup Z_2$, where $Z_1$ is the subset $Z$ in the copy $Y_1$, $Z_2$ the subset $Z'$ in the copy $Y_2$ of $Y$. Let $H = G' \cap D \times D$ be the setwise stabilizer of $Y_1$ in $G'$. Since $(G:D \times D) = 2$, the index of $H$ in $G'$ is at most 2. Therefore, using the techniques of Chapter II, we can determine $H$ from a generating set for $G'$. We conclude the proof of the theorem by showing that $(G':H) = 2$ iff $D$ contains an element $\delta$ which maps $Z$ onto $Z'$.

Assume there exists an element $\delta \in D$ such that $Z^\delta = Z'$. Then $\psi = (\delta, \delta^{-1}; (1,2))$ must exchange $Z_1$ with $Z_2'$, hence $\psi \in G'$. Since $\psi$ does not stabilize $Y_1$, the index of $H$ in $G'$ must be 2. Conversely, let $(G':H) = 2$ and consider an element $\psi \in G'$ which is not in $H$. Then $\psi$ must be of the form $(\delta, \gamma; (1,2))$. Since $Z_1 \subset Y_1$ and $Z_2 \subset Y_2$, $Z_1^\delta$ must be $Z_1'$, i.e., $\delta$ is the desired element of $D$. 

We have now established the polynomial time equivalence of Problems 1 through 6.

2.3. Miscellaneous Problems

We now consider the following two problems which are polynomial time equivalent to Double Coset Membership:

**Problem 7 (Centralizer in Another Group)**

Given the groups $A, B < S_n$ by generating sets, determine a generating set for the centralizer $C_A(B)$ of $B$ in $A$.

**Problem 8 (Restricted Graph Automorphism)**

Given a graph $X = (V,E)$ and a permutation group $A < \text{Sym}(V)$, determine generators for all automorphisms of $X$ which are also in $A$, i.e., find generators for $A \cap \text{Aut}(X)$.

First, we establish the polynomial time equivalence of Problem 7 with Problems 4 through 6. We begin with a polynomial time reduction of Problem 7 to Problem 5, Group Intersection. For this, we need some elementary results about the structure of the centralizer (in $S_n$) of a cyclic group $Z$ generated by a permutation $\pi \in S_n$. 


Let \( \pi, \psi \in S_n \) be permutations, where \( \pi \), in cycle notation, is 
\[ \pi = (i_1, ..., i_p)(i_{p+1}, ..., i_q) \cdot \cdot \cdot (i_r, ..., i_t). \]
Then the conjugate of \( \pi \) under \( \psi \) is the permutation 
\[ \pi^\psi = (i_1^\psi, ..., i_p^\psi)(i_{p+1}^\psi, ..., i_q^\psi) \cdot \cdot \cdot (i_r^\psi, ..., i_t^\psi). \]
We illustrate this elementary observation in the following

**Example 3**

Let \( \pi = (1,2)(3,4)(6,7,9) \) and \( \psi = (1,2,3,4)(5,6) \) be permutations in \( S_9 \). Then 
\[ \pi^\psi = (1^\psi,2^\psi)(3^\psi,4^\psi)(6^\psi,7^\psi,9^\psi) = (2,3)(4,1)(5,7,9), \]
which is readily verified. \( \Box \)

**Lemma 4**

Let \( A < S_n \) be generated by \( \{ \alpha_1, \alpha_2, ..., \alpha_p \} \), and let \( C_i \) be the set of all permutations in 
\( S_n \) which commute with \( \alpha_i \), i.e., 
\[ C_i = \{ \pi \in S_n \mid \pi^{-1}\alpha_i\pi = \alpha_i \}. \]
Then \( C_{S_a}(A) = \bigcap_{i=1}^{p} C_i. \)

**Proof**

It is easy to see that the sets \( C_i \) are groups. Therefore, \( D = \bigcap_{i=1}^{p} C_i \) is also a 
group. Let \( \gamma \in D, \alpha \in A. \) Since \( \alpha \) is a finite product of the \( \alpha_i \), clearly \( \gamma^{-1}\alpha\gamma = \alpha \), thus 
\( \gamma \in C_{S_a}(A). \) Conversely, let \( \gamma \in C_{S_a}(A). \) Since \( \alpha_i \in A, \gamma^{-1}\alpha_i\gamma = \alpha_i, 1 \leq i \leq p, \) thus \( \gamma \in D. \)
Therefore, \( C_{S_a}(A) = D. \) \( \Box \)

As a consequence of the lemma, \( C_i = C_{S_a}(\alpha_i) = C_{S_a}(Z_i) \), where \( Z_i \) is the cyclic group 
generated by \( \alpha_i. \)

**Lemma 5**

Let \( \pi \in S_n \) be a permutation, \( Z = \langle \pi \rangle \) the cyclic group generated by \( \pi \). Then genera-
tors for the centralizer \( C_{S_a}(Z) \) can be determined in polynomial time.

**Proof**

Let \( \pi \) be written in cycle notation with the distinct cycle lengths 
\( l_1, l_2, ..., l_r \), and with \( m_i \) cycles of length \( l_i \). Here we also consider cycles of length 1. 
\( \psi \in S_n \) commutes with \( \pi \) iff \( \pi^\psi = \pi \). By Lemma 4, we therefore look for all those per-
mutations \( \psi \) such that conjugation under \( \psi \) "rotates" the cycles of \( \pi \) and/or 
exchanges cycles of equal length. Since the cycle notation is unique up to these two 
rewriting rules, \( C_{S_a}(Z) \) must consist precisely of those permutations.

For each \( i \leq r \), we examine the cycles of length \( l_i \). By inspection, we will produce 
a set \( K_i \) of permutations generating all those permutations \( \psi \) which commute with \( \pi \) 
and are such that all points which lie in cycles of \( \pi \) of length other than \( l_i \) are fixed by 
\( \psi. \)

Let \( J_{1,}, ..., J_{m_i} \) be all the cycles in \( \pi \) of length \( l_i \). The set \( K_i \) will consist of permuta-
tions \( \xi_{1,1}, ..., \xi_{1,m_i} \) and two permutations \( \alpha_i \) and \( \beta_i \). \( K_i \) contains no other permutation.
We let \( \xi_{1,s} = J_s, \quad 1 \leq s \leq m_i. \) Furthermore, if \( J_s = (j_{s,1}, j_{s,2}, \ldots, j_{s,l_i}) \), then 
\[
\alpha_i = (j_{1,1}, j_{2,1}) \cdot \cdots \cdot (j_{l_i,1}, j_{l_i,2}), \quad \text{and} \quad \beta_i = (j_{1,1}, j_{2,1}) \cdot \cdots \cdot (j_{l_i,1}, j_{l_i,2}).
\]

Recall that \( S_n \) is generated by \( \alpha = (1,2) \) and \( \beta = (1,2,\ldots,n) \). Thus, it is clear that \( \alpha_i \) and \( \beta_i \) generate permutations \( \psi \) which conjugate \( \pi \) by permuting the order of the cycles of length \( 1 \) in all possible ways. Since the \( \xi_{i,k} \) generate all rotations of these cycles, \( K_i \) generates all permutations \( \psi \in S_n \) such that conjugation under \( \psi \) fixes all cycles in \( \pi \) of length other than \( l_i \) and rearranges and/or rotates the cycles of length \( l_i \) in all possible ways. By Lemma 4, therefore, \( \langle \bigcup_{i=1}^{r} K_i \rangle = C_{S_n}(Z) \).

Observe that \( \sum_{i=1}^{r} m_i l_i = n \), thus \( |K| \) is \( O(n) \), and so \( K \) can be constructed in polynomial time. •

In Section 4 we will show that \( C_{S_n}(Z) \) arises as the automorphism group of a very simple graph which can be constructed from \( \pi \) in \( O(n) \) steps.

**Example 4**

Let \( \pi = (1,2)(3,5,6)(4,7)(8,12)(9,11,13)(10)(14) \) be a permutation in \( S_{14} \) generating the group \( Z \). \( \pi \) has two cycles of length 1, three cycles of length 2, and two cycles of length 3.

We consider first the cycles of length 3, which are \( (3,5,6) \) and \( (9,11,13) \). We obtain 
\[
\xi_{1,1} = (3,5,6), \quad \xi_{1,2} = (9,11,13), \quad \alpha_1 = (3,9)(5,11)(6,13), \quad \text{and} \quad \beta_1 = \alpha_1. \]
Thus, \( K_1 = \{ \xi_{1,1}, \xi_{1,2}, \alpha_1 \} \). Next, we consider the three cycles of length 2, which are \( (1,2), (4,7), \) and \( (8,12) \). Here we obtain the set \( K_2 \) consisting of \( \xi_{2,1} = (1,2), \xi_{2,2} = (4,7), \xi_{2,3} = (8,12), \alpha_2 = (1,4)(2,7), \) and \( \beta_2 = (1,4,8)(2,7,12) \). Finally, for the cycles of length 1, the permutations \( \xi \) are each the identity permutation, and \( \alpha_3 = \beta_3 = (10,14) \). Together, these permutations generate \( C_{S_n}(Z) \). □

**Theorem 6**

Problem 7 can be polynomial time reduced to Problem 5.

**Proof** Let \( A, B \subset S_n \), with known generating sets. We can find generators for \( C_{A}(B) \) in two steps:

(a) Determine generators for \( C_{S_n}(B) \).

(b) Intersect \( C_{S_n}(B) \) with \( A \).

In Section 3, we will show how to do Step (a) in polynomial time. For the present, we do Step (a) by constructing \( C_{S_n}(<\beta>) \) for each of the generators \( \beta \) of \( B \) using Lemma 5,
and then intersect these groups, thereby obtaining $C_{\mathcal{A}}(B)$ by Lemma 4. 

**Theorem 7 (Luks)**

Problem 6 can be reduced to Problem 7 in polynomial time.

**Proof** Let $A < S_n, X$ a subset of $\{1, ..., n\}$. We will determine generators for $A_X$, the setwise stabilizer of $X$ in $A$, using an algorithm for Problem 7.

Let $A'$ be the group isomorphic to $A$ acting on 

$$Y = \{ (i, j) \mid 1 \leq i \leq n, j = 1, 2 \}$$

constructed by associating with $a \in A$ the permutation $a'$ of $Y$ where $(i,j)^{a'} = (i^a, j)$.

Let $\pi$ be the permutation of $Y$ where, for $i \in X$, $(i,j)^{\pi} = (i,j)$, and, for $i \notin X$, $(i,1)^{\pi} = (i,2)$ and $(i,2)^{\pi} = (i,1)$. Let $Z$ be the group generated by $\pi$. Then it is easy to see that $C_{A'}(Z)$, the centralizer in $A'$ of $Z$, is isomorphic to $A_X$. Generators for $A_X$ are easily obtained from generators for $C_{A'}(Z)$.

Note that the proof of Theorem 7 shows that Problem 7 remains hard even when restricting the group $B$ to a cyclic group. Finally, we establish the equivalence of Problem 8 with the Problems 1-7.

**Theorem 8 (Luks)**

Problem 8 is polynomial time equivalent with Problems 5 and 6.

**Proof** Let $A < S_n$ be a group in which we wish to stabilize the subset $Y$ of $\{1, ..., n\}$. Without loss of generality we may assume that $|Y| > 1$. Now $A_Y = A \cap \text{Sym}(Y) \times \text{Sym}(\overline{Y})$. We observe that $\text{Sym}(Y) \times \text{Sym}(\overline{Y})$ is the automorphism group of the graph 

$$X = \{(1, ..., n), \{(i,j) \mid i, j \in Y\}\},$$

hence finding generators for $A_Y$ is an instance of Problem 8. Conversely, by Theorem 7 of Chapter II, given a graph $X$, $A \cap \text{Aut}(X)$ is the intersection of three permutation groups with known generators.

We have now established the polynomial time equivalence of Problems 1 through 8. A number of special cases of these problems are in $P$, and we discuss them in Section 4. In Section 3 we discuss a special case of Group Intersection that is in $\text{NP} \cap \text{coNP}$.
2.4. Isomorphism Complete Problems

Recall that problems which are polynomial time equivalent to graph isomorphism have been called isomorphism complete. There are many known isomorphism complete problems. Because of Section 1, we use the following two problems as representatives:

**Problem 9 (Existence of Graph Isomorphism)**

Given nonnegative numbers \( p, q, \) and \( n \), such that \( p + q = \binom{n}{2} \) and a permutation \( \pi \in S_{p+q} \). Determine whether \( \pi \in AB \), where \( A \) is isomorphic to \( S_p \times S_q \) and \( B \) is the permutation group induced by \( S_n \) on the set of all unordered pairs \((i,j), 1 \leq i < j \leq n\).

**Problem 10 (Graph Automorphism)**

Given nonnegative numbers \( p, q, \) and \( n \), such that \( p + q = \binom{n}{2} \), determine a generating set for \( A \cap B \), where \( A \) is isomorphic to \( S_p \times S_q \) and \( B \) is the permutation group induced by \( S_n \) on the set of all unordered pairs \((i,j)\).

The interpretation of these problems as graph isomorphism and graph automorphism, respectively, follows from Proposition 1 and the subsequent discussion. So, the polynomial time equivalence of Problems 9 and 10 follows from the results of Section 2 of Chapter II. It is clear from the problem formulation that Problem 9 can be reduced in polynomial time to Problem 1. We have not found a reduction in the converse direction, and we conjecture that none exists.

2.5. Remarks

We have given a collection of group-theoretic problems which are at least as hard as graph isomorphism. The problems are naturally related to graph isomorphism. For one, graph isomorphism can be reduced to each of these problems in polynomial time by easy and straightforward reductions. These are the first examples of such reductions among natural problems in \( \text{NP} \) of unknown complexity status. Furthermore, as pointed out already, Double Coset Membership is itself an abstract isomorphism question involving structures which are apparently more general than graphs.
Of course, our conjecture that these problems lie properly between P and NP-complete is more speculative than the implied conjecture that $P \neq NP$.

It is not out of question that these problems ultimately belong to P. However, the length of time that graph isomorphism, the problem on the lowest level of difficulty, has resisted a polynomial time solution does not suggest that this possibility is very likely. It is also possible that the problems are polynomial time equivalent with graph isomorphism. If they are not, then it must be that permutation groups of degree n are intrinsically more complicated objects than the automorphism groups of graphs of size polynomial in n. In particular, an open question closely related to this is the following:

**Problem 11**

Given a permutation group G of degree n, is there a graph X with m vertices such that G is isomorphic to Aut(X), the automorphism group of X, and m is polynomial in n?

It is known that every permutation group G is isomorphic to the automorphism group of some graph X. However, the size of the graph X is polynomial in the order of G, not the degree of G. Should the above question have an affirmative answer, then it is not difficult to show that Problems 1 through 8 are isomorphism complete.

3. **A Problem with a Short Verifiable Solution**

In this section, we show that Problem 5, Group Intersection, has a special case which is in $NP \cap \text{coNP}$. That is, for certain permutation groups we may guess a generating set for their intersection and can then verify with certainty in polynomial time that we have guessed correctly. Specifically, we consider

**Problem 12 (Intersection of Commuting Groups)**

Given generating sets for the commuting permutation groups A and B, find a generating set for $A \cap B$.

Recall that two subgroups of $S_n$ commute iff $AB = BA$. Note that the commutativity of groups does not necessarily imply that the two groups commute element by
element, or that one is a subgroup of the normalizer of the other (cf. Chapter V, Definition 7). For example, one verifies easily that with $A = \langle (1,2), (1,3)(2,4) \rangle$ and $B = \langle (1,2,3) \rangle$ we have $AB = BA = S_4$. Yet neither $B$ normalizes $A$ nor $A$ normalizes $B$.

The key property of commuting groups to be exploited is stated in the following lemma which is easy to prove.

**Lemma 6**

Let $A$ and $B$ be subgroups of a finite group $G$. Then the complex $AB$ is a group iff $AB = BA$.

We exploit this lemma by observing that since the complex $AB$ is the group $\langle A, B \rangle$ for commuting groups, we may determine the order of $AB$ using the techniques of Chapter II. For noncommuting groups there seems to be no easy way for determining the cardinality of the complex $AB$. Applying Lemma 20 of Chapter III, we then compute the order of the intersection $A \cap B$ from the orders of $A$, $B$, and $AB$.

Having determined the order of $A \cap B$ in polynomial time, we may now verify that a (guessed) set $K$ of permutations generates $A \cap B$: First, test for each $\pi \in K$ whether $\pi \in A \cap B$, i.e., whether $\pi \in A$ and $\pi \in B$. This establishes that $K$ generates a subgroup of $A \cap B$. Then, compute the order of the group generated by $K$. If it is equal to the order of $A \cap B$, then $\langle K \rangle = A \cap B$. Otherwise, $\langle K \rangle$ is a proper subgroup of the intersection. By the results of Chapter II, all steps require polynomial time only. In summary, we have just shown

**Theorem 9 (Hoffmann)**

Problem 12 is in $\text{NP} \cap \text{coNP}$.

We know of no polynomial time test of whether two permutation groups commute. In some cases, this may be verified using Lemma 7 below.

**Lemma 7**

If the indices $(\langle A, B \rangle : A)$ and $(\langle A, B \rangle : B)$ are coprime, then $AB = BA = \langle A, B \rangle$.

**Proof** Since $(AB : B) = (A : A \cap B)$ we have $(\langle A, B \rangle : A) \geq (A : A \cap B)$. So, $(\langle A, B \rangle : A \cap B) \leq (\langle A, B \rangle : A) - (\langle A, B \rangle : B)$. Since $(\langle A, B \rangle : A)$ and $(\langle A, B \rangle : B)$ both divide $(\langle A, B \rangle : A \cap B)$, by coprimality, $(\langle A, B \rangle : A) - (\langle A, B \rangle : B)$ must divide $(\langle A, B \rangle : A \cap B)$. Thus, $(\langle A, B \rangle : A \cap B) = (\langle A, B \rangle : A) - (\langle A, B \rangle : B)$, hence $\langle A, B \rangle = AB$. 

For example, for $A = \langle (1,2), (1,3)(2,4) \rangle$ and $B = \langle (1,2,3) \rangle$ we have $(\langle A, B \rangle : A) = 3$ and $(\langle A, B \rangle : B) = 8$, hence $A$ and $B$ commute.
4. Subproblems in P

We now discuss a number of special cases of the problems of Section 2 with known polynomial time solutions. We group these problems by the general problem of which they are special instances. Of particular prominence are intersection algorithms, since they form the basis of many of the algorithms in the preceding chapters.

4.1. Group Intersection Problems

We consider the following set of problems:

**Problem 13 (Intersection with a Normalizing Group)**
Given permutation groups \( A, B < S_n \) by generating sets, determine generators for \( A \cap B \), provided that \( B \) normalizes \( A \).

**Problem 14 (Intersection with a p-Group)**
Given permutation groups \( A, B < S_n \) by generating sets, determine generators for \( A \cap B \), provided that \( A \) is a p-group.

**Problem 15**
Given permutation groups \( A, B < S_n \) by generating sets, determine generators for \( A \cap B \), provided that \( A \) is in the class \( \Gamma_b \) and \( b \) is a fixed constant.

**Problem 16**
Given permutation groups \( A, B < S_n \) with a polynomial time membership test, determine generators for \( A \cap B \), provided that both \( A \) and \( B \) are \((k,c)\)-accessible from a group \( G < S_n \) with known generators.

**Problem 17**
Given permutation groups \( A, B < S_n \) with a polynomial time membership test, determine generators for \( A \cap B \), provided that \( A \) is \((k,c)\)-accessible from a group \( G < S_n \) with known generators, \( B \) is a subgroup of \( G \), and generators for \( B \) are known.

Except for Problem 13, we can obtain polynomial time algorithms from earlier algorithms after suitable modifications. We begin with Problem 13.

The first crucial observation to be made is that \( AB = BA \) provided that one of the groups is a subgroup of the normalizer of the other. For if \( B \) normalizes \( A \), say, then
\[ A\pi = \pi A \text{ for all elements } \pi \in B. \text{ So, we have } AB = \langle A,B \rangle \text{ and can therefore test membership in } AB. \]

The second crucial observation is that the normalizing property is "inherited" by the pointwise stabilizers:

**Lemma 8**

Let \( B \) normalize \( A \), where \( A, B < S_n \). Then for any point \( i \in \{1,\ldots,n\}, B_i \) normalizes \( A_i \).

**Proof** Let \( \psi \in A_i, \pi \in B_i \). Since \( B \) normalizes \( A \), we have \( \pi^{-1}\psi\pi \in A \). But \( \pi^{-1}\psi\pi = i \), hence \( \pi^{-1}\psi\pi \in A_i \). 

As a consequence of Lemma 8, we also have \( A^{(i)}B^{(i)} = \langle A^{(i)},B^{(i)} \rangle \), where \( A^{(i)} \) and \( B^{(i)} \) are the pointwise stabilizers of \( \{1,\ldots,i-1\} \) in \( A \) and \( B \), respectively. Thus, we have a polynomial time membership test in these double cosets as well. That is, we may convert the proof of Theorem 3 into a deterministic polynomial time algorithm.

Before giving the algorithm, we make two observations which increase the efficiency of the method.

First, consider the trial and error membership tests of Step (c) in the proof of Theorem 3: The purpose of these tests is to factor a permutation \( \pi \in AB \) as \( \pi = \alpha\beta \), where \( \alpha \in A, \beta \in B \). We observe that this factorization can be achieved directly, provided every entry \( \varphi \) in the representation matrix for \( AB \) is already factored in this way. For, let \( \pi = \varphi_n \cdots \varphi_1 \), where \( \varphi_k = \alpha_k\beta_k \). Then, since \( B \) normalizes \( A \), we have \( \pi = (\alpha'_n \cdots \alpha'_1)(\beta_n \cdots \beta_1) = \alpha'\beta' \). Here we know \( \pi \) and \( \beta' \), hence we can also compute \( \alpha' \).

To see how the entries of a representation matrix can be obtained in the suitable form, consider the matrix construction by the techniques of Chapter II: We sift the generators for both \( A \) and \( B \) followed by sifting pair products, thus, in principle, we know each entry as a word of permutations in \( A \) and \( B \). These words are now brought into the required form \( \alpha\beta \) using the above considerations. It is necessary to do this for each new coset representative when entering it, for otherwise the new words might grow to exponential length (cf. the discussion at the end of Subsection 3.1 of Chapter II).

Now observe that for \( A, B < S_n \) the group \( \langle A_1,B_1 \rangle \) is a subgroup of \( \langle A,B \rangle \). Therefore, if \( \alpha \) is a coset representative for \( (A^{(i)}B^{(i)})_m \) in \( A^{(i)}B^{(i)} \), then it must also be a coset representative for \( (A^{(j)}B^{(j)})_m \) in \( A^{(j)}B^{(j)} \), where \( j < i \). So, the representation matrices for \( A^{(i)}B^{(i)}, 1 \leq i \leq n+1 \), may be combined into a single \( n \) by \( n \) matrix with nonempty entries of the form \( (\alpha, \beta, k) \), where \( \alpha\beta \) is a nonempty entry in the representation.
matrices for $A^{(k)}B^{(k)}, A^{(k-1)}B^{(k-1)}, \ldots, A^{(1)}B^{(1)}$.

An implementation of these ideas is quite straightforward, but it requires computing the matrix for $A^{(0)}B^{(0)}$ completely before computing the matrix $A^{(i-1)}B^{(i-1)}$. It is not hard to see that the computation requires at most $O(n^8)$ steps assuming we have already computed representation matrices for $A$ and $B$ from which to obtain generating sets for the groups $A^{(i)}$ and $B^{(i)}$ of size $O(n^2)$ at most.

Given below is the algorithm for intersecting normalizing groups based on these ideas.

**Algorithm 1 (Intersection with a Normalizing Group)**

**Input**
Generating sets $K_A$ and $K_B$ for the permutation groups $A, B < S_n$, where $B$ normalizes $A$.

**Output**
A representation matrix for $C = A \cap B$.

**Comment**
See Proposition 3 below for a method of testing whether $B$ normalizes $A$. Note that Step 3 below computes representation matrices for the groups $A^{(i)}B^{(i)}$ in accordance with the ideas outlined above.

**Method**
1. begin
2. Compute representation matrices for $A$ and $B$ using Algorithms 2 and 3 of Chapter II;
   
   **comment** Let $A^{(i)}, B^{(i)},$ and $C^{(i)}$ be as in the proof of Theorem 3;
3. Compute representation matrices for the groups $A^{(i)}B^{(i)}, n > i > 1$;
4. Initialize a representation matrix for $C = A \cap B$ to represent the trivial group $I$;
5. for $i := n$ downto 1 do
6.     for each pair $\pi, \psi$ of entries in row $i$ of the representation matrices of $A$ and $B$, respectively, such that $i^\pi = i^\psi = j$ do
7.         if $\pi\psi^{-1} \in A^{(i+1)}B^{(i+1)}$ then begin
8.             let $\pi\psi^{-1} = \varphi_n \cdots \varphi_{i+1}$, where $\varphi_k = \alpha_k\beta_k, \alpha_k \in A^{(i+1)}, \beta_k \in B^{(i+1)}$, $n \geq k \geq i+1$;
9.             enter $\beta_n\beta_{n-1} \cdots \beta_{i+1}\psi$ as coset representative into row $i$, column $j$ of the representation matrix for $C$;
10.        end;
11. output the representation matrix for $C$;
12. end.
The correctness of the algorithm is obvious from Theorem 3 and above discussion. Furthermore, an elementary analysis shows

**Proposition 2 (Hoffmann)**

Problem 13 may be solved in \(O((|K_A| + |K_B|) \cdot n^2 + n^6)\) steps, where \(K_A\) and \(K_B\) are generating sets for the two groups.

Given generating sets for both groups, it is easy to test whether a group \(B\) normalizes a group \(A\):

**Proposition 3 (Hoffmann)**

Given generating sets \(K_A\) and \(K_B\) for the groups \(A, B < S_n\), one can test whether \(B\) normalizes \(A\) in \(O(|K_A| \cdot n^2 + n^6)\) steps.

**Proof** In \(O(|K_A| \cdot n^2 + n^6)\) steps we can construct a representation matrix for \(A\) from \(K_A\). Having done so, we then have an \(O(n^2)\) membership test in \(A\). Clearly \(B\) normalizes \(A\) iff, for every pair of generators \(\pi \in K_A\) and \(\psi \in K_B\), the conjugate \(\psi^{-1} \pi \psi\) is in \(A\).

We next discuss Problem 14. Recall Section 4 of Chapter IV. Based on Lemmata 8 and 9 of that chapter we may design a recursive procedure for intersecting the \(p\)-group \(G\) with any other group \(H\). The computation of this recursive procedure can be reorganized, just as in the case of intersecting two \(p\)-groups, resulting in reduced overhead. In this manner, we obtain an intersection algorithm much like Algorithm 3 of Chapter IV. Essentially, the new algorithm differs only in how to determine point stabilizers when computing the coset \(J(A, Programming\), where \(\text{proj}_1(A)\) fixes \(x\) (Line 31 of the algorithm). Since \(\text{proj}_2(A)\) is not a \(p\)-group, Algorithms 2 and 3 of Chapter II must be used. Consequently, the algorithm has to spend \(O(n^6)\) steps when processing this base case of the recursion. It is not difficult to develop the details, and we can prove in summary

**Proposition 4 (Hoffmann)**

Let \(A, B < S_n\), where \(A\) is a \(p\)-group, and assume given generating sets \(K_A\) and \(K_B\) for \(A\) and \(B\), respectively. Then a generating set for \(A \cap B\) can be determined in \(O((|K_A| + |K_B|) \cdot n^2 + n^7)\) steps. Moreover, if \(B\) is also a \(p\)-group and if composition sequences and complete imprimitivity structures for both \(A\) and \(B\) are given, then a composition series for \(A \cap B\) may be determined in \(O(n^3)\) steps.

The second part of the proposition restates Theorem 5 of Chapter IV. The term \((|K_A| + |K_B|) \cdot n^2\) in the general bound originates from deriving strong generating sets
for A and B from the given sets $K_A$ and $K_B$.

Now consider Problem 15. Regarding the relationship of Lemmata 8 and 9 of Chapter IV with the rules for computing the set function $S_Y(G,\pi,\Sigma)$ of Subsection 3.1 of the same chapter, it is clear that we can modify Algorithm 3 of Chapter V so that it computes the intersection of a permutation group in $\Gamma_b$ with an arbitrary permutation group. The details are straightforward and it is clear that the resulting algorithm requires time polynomial in the degree of the groups, provided $b$ is a constant.

Finally, we observe that Problems 16 and 17 are in $P$ by Theorems 13 and 14 of Chapter II.

4.2. Centralizer and Center

We now show that Problem 7, Centralizer in Another Group, has two special cases which are in $P$. That is, we give a polynomial time algorithm for finding the centralizer (in $S_n$) of the permutation group $G < S_n$ with a given generating set $K$. Furthermore, observing that the centralizer of $G$ normalizes $G$, we apply Algorithm 1 and obtain a polynomial time algorithm for finding the center of $G$. In particular, we consider

**Problem 18 (Centralizer)**

Given a generating set $K$ for the group $G < S_n$, find a generating set for the centralizer $C_{S_n}(G)$ of $G$.

**Problem 19 (Center)**

Given a generating set $K$ for the group $G < S_n$, find a generating set for the center $C_G(G)$ of $G$.

We consider Problem 18 first, and begin by reexamining the centralizer $C_{S_n}(Z)$ of the cyclic group $Z$ generated by a permutation $\pi$. Recall the proof of Lemma 5. We argued that $\psi$ is in $C_{S_n}(<\pi>)$ iff conjugation under $\psi$ rearranges the ordering of cycles of equal length in $\pi$ and/or rotates the individual cycles. We now show that there is a directed graph $X_\pi$ whose automorphism group is precisely $C_{S_n}(<\pi>) = C_{S_n}(\pi)$. 
A cycle graph is a directed graph $X = (V,E)$ such that, for every $v \in V$, the indegree and the outdegree of $v$ are either both 0 or 1. Intuitively, a cycle graph consists of disjoint directed cycles and/or isolated points.

**Definition 2**
Let $\pi \in S_n$ be a permutation. The cycle graph $X_\pi$ of $\pi$ is the cycle graph $(V,E_\pi)$ where $V = \{1, \ldots, n\}$, and there is an edge from $i$ to $j$ in $E_\pi$ if $i^\pi = j$.

**Example 5**
For the permutation $\pi = (1,2)(3,5,6)(4,7)(8,12)(9,11,13)(10)(14)$ in $S_{14}$ we obtain the cycle graph $X_\pi$ of Figure 3 below.

![Figure 3](image)

Note that $X_\pi$ is unique, and that it can be constructed from $\pi$ in $O(n)$ steps. From the proof of Lemma 5, the following is now obvious:

**Lemma 9**
If $\pi \in S_n$ is a permutation, $X_\pi$ the cycle graph of $\pi$, then $\text{Aut}(X_\pi) = C_{S_n}(\pi)$.

In Section 2, we constructed $C_{S_n}(<K>)$ by first constructing $C_{S_n}(\pi)$ for all $\pi \in K$, and then intersecting these groups using Lemma 4. We observe now that instead of intersecting the groups $C_{S_n}(\pi)$, $\pi \in K$, we can superimpose the graphs $X_\pi$ resulting in a new graph $X_K$ whose automorphism group will be $C_{S_n}(<K>)$. Here we need to label the edges of each graph $X_\pi$ uniformly to prevent an automorphism of $X_K$ from mapping an edge belonging to $X_\pi$ to an edge belonging to $X_\psi$, where $\pi \neq \psi$.

A labelled cycle graph $X$ of degree $k$ is a directed multigraph $(V,E)$ and a mapping from $E$ into the set $\{1, \ldots, k\}$ such that the subgraph obtained by deleting all edges in $E$ which are not mapped to $i$ is a cycle graph $(1 \leq i \leq k)$. Intuitively, a labelled cycle graph is obtained by superimposing $k$ cycle graphs, where each edge of the $i^{\text{th}}$ cycle graph is labelled $i$. The resulting graph is a multigraph, since there may be more than one edge from a vertex $v$ to a vertex $w$. Note, however, that two different edges from $v$ to $w$ must be labelled differently. The subgraphs consisting of all the vertices and those edges which have the same label are called the constituents of $X$. 
**DEFINITION 3**

Let \( K \) be a set of permutations in \( S_n \). The **labelled cycle graph** \( X_K \) of \( K \) is the labelled cycle graph whose \(|K|\) constituents are the cycle graphs \( X_\pi, \pi \in K \).

Thus, \( X_K \) is of degree \(|K|\). Observe that we can construct \( X_K \) from \( K \) in \( O(n \cdot |K|) \) steps.

**EXAMPLE 6**

Let \( G = \langle K \rangle \), where \( K = \{(1,2,3,4), (2,4)\} \). Here \( G = D_4 \), the dihedral group of degree 4.

The labelled cycle graph \( X_K \) of \( K \) is shown in Figure 4 below.

![Figure 4](image)

Because of the labelling of \( X_K \) and by Lemma 4, the following is obvious.

**LEMMA 10**

Let \( G = \langle K \rangle \), \( K \) a subset of \( S_n \). Then \( C_{S_n}(G) = \text{Aut}(X_K) \), where \( X_K \) is the labelled cycle graph of \( K \).

We will show how to test isomorphism and determine the automorphism group of labelled cycle graphs.

**DEFINITION 4**

Let \( X \) be a connected labelled cycle graph, \( x \) and \( y \) distinct vertices of \( X \). The **cycle distance** \( d(x,y) \) of \( x \) and \( y \) is defined by

1. \( d(x,y) = 0 \) iff \( x \) and \( y \) lie on a common cycle in \( X \) whose edges are uniformly labelled.
2. \( d(x,y) = k \) iff \( z_1, \ldots, z_k \) is the smallest number of vertices in \( X \) such that \( d(x,z_1) = 0, d(z_k,y) = 0, \) and \( d(z_i,z_{i+1}) = 0, 1 \leq i < k \).

**EXAMPLE 7**

Let \( X \) be the connected labelled cycle graph shown in Figure 5 below.

![Figure 5](image)
Then \( d(1,2) = 0, d(1,3) = 1, d(1,4) = 2. \) \( \square \)

The isomorphism test of labelled cycle graphs to be described next rests on the following key observation.

**Theorem 10**

Let \( X = (V_X, E_X) \) and \( Y = (V_Y, E_Y) \) be isomorphic connected labelled cycle graphs. Then every isomorphism \( \iota \) from \( X \) to \( Y \) is fully determined by the image \( x^\iota \) of an arbitrary vertex \( x \in V_X \).

**Proof** Without loss of generality we assume that both \( X \) and \( Y \) have more than one vertex. So, let \( \iota \) be an isomorphism from \( X \) to \( Y \), \( x \) any vertex in \( X \), and \( x^\iota \) the image of \( x \) under \( \iota \) in \( Y \). Since cycles of uniformly labelled edges are mapped again into such cycles whose edges have the same label in \( Y \), and since cycles in every constituent are disjoint, it follows that the image of every vertex \( u \) in \( X \) of cycle distance 0 from \( x \) is determined by \( x^\iota \). Since vertices \( z \) in \( X \) of cycle distance 1 from \( x \) have a cycle distance 0 from some other vertex \( u \) in \( X \) with \( d(x,u) = 0 \), the same argument shows that the image of every such \( z \) is fully determined by \( u^\iota \) and therefore by \( x^\iota \). Proceeding by induction on the cycle distance from \( x \), since both \( X \) and \( Y \) are connected, it follows that the image of every vertex of \( X \) under \( \iota \) is fully determined by \( x^\iota \).

\[ \text{From Theorem 10, we obtain the following corollaries:} \]

**Corollary 2 (Fontet, Hoffmann)**

If \( X \) and \( Y \) are connected labelled cycle graphs of degree \( k \) with \( n \) vertices each, then isomorphism of \( X \) and \( Y \) can be tested in \( O(n^2\cdot k) \) steps.

**Proof** Let \( x \) be a fixed arbitrary vertex of \( X \). In \( O(n\cdot k) \) steps we can test, for each vertex \( y \) in \( Y \), whether mapping \( x \) into \( y \) determines an isomorphism. \( \square \)

Note \( X_K \) is a connected multigraph iff the group \( <K> \) is transitive. Consequently, Theorem 10 is a restatement of Theorem 5 of Chapter V. It is a stronger form of the theorem, since the fact that \( \text{Aut}(X) \) is semiregular for some graph \( X \) does not necessarily imply that there is a simple procedure for deciding whether mapping a vertex \( x \) to a vertex \( y \) may be extended to an automorphism of \( X \).

**Corollary 3**

If \( X \) is a connected labelled cycle graph of degree \( k \) with \( n \) vertices, then generators for \( \text{Aut}(X) \) can be determined in \( O(n^2\cdot k) \) steps.

**Proof** Immediate from Corollary 2 and the observation that \( |\text{Aut}(X)| \leq n. \) \( \square \)
We now consider how to test isomorphism of labelled cycle graphs which are not necessarily connected. Intuitively, we will split the graphs \( X \) and \( Y \) into components, and test isomorphism of each component. Having classified the components into isomorphism classes, it is clear that \( X \) and \( Y \) are isomorphic iff exactly half the components in each isomorphism class belong to \( X \).

**Theorem 11 (Fontet, Hoffmann)**

Let \( X \) and \( Y \) be labelled cycle graphs of degree \( k \) with \( n \) vertices each. Then we can test isomorphism of \( X \) and \( Y \) in \( O(n^2 \cdot k) \) steps.

**Proof** In \( O(n \cdot k) \) steps we can find the components of \( X \) and \( Y \). If \( X \) and \( Y \) do not have an equal number of components of equal size, then they cannot be isomorphic. So, let \( X \) and \( Y \) have \( p_i \) components of size \( m_i \), \( 1 \leq i \leq r \). We test at most \( p_i^2 \) components of size \( m_i \) for isomorphism. By Corollary 2, this requires a total of \( O(p_i^2 \cdot m_i^2 \cdot k) \) steps. Since \( \sum_{i=1}^{r} p_i \cdot m_i = n \), isomorphism of \( X \) and \( Y \) can be tested in \( O(n^2 \cdot k) \) steps. It is clear that we can construct an isomorphism in the same time bound.

We therefore obtain the following

**Corollary 4**

If \( X \) is a labelled cycle graph of degree \( k \) with \( n \) vertices, then generators for \( \text{Aut}(X) \) can be found in \( O(n^2 \cdot k) \) steps.

**Proof** \( \text{Aut}(X) \) is generated by a set \( K_1 \cup K_2 \), where \( K_1 \) generates all automorphisms which fix setwise the vertices of each component of \( X \), and \( K_2 \) generates all possible permutations of isomorphic components of \( X \).

Let \( X \) have \( p_i \) components of size \( m_i \), \( 1 \leq i \leq r \). We can find these components in \( O(n \cdot k) \) steps. By Corollary 3, we find the set \( K_1 \) in \( O((\sum_{i=1}^{r} p_i \cdot m_i^2) \cdot k) \) steps, which is dominated by \( O(n^2 \cdot k) \).

By Theorem 11, in \( O(n^2 \cdot k) \) steps, we can classify the components of \( X \) into isomorphism classes and can find, in every isomorphism class, an isomorphism from an arbitrary representative component to each component in the class. It is trivial to produce the set \( K_2 \) from these maps. Note that both \( |K_1| \) and \( |K_2| \) are \( O(n) \).

**Example 6**

Let \( K = \{(1,2,3,4)(5,6,7,8), (2,4)(5,7)\} \). The labelled cycle graph \( X_K \) is of degree 2 and is shown in Figure 6 below. \( X_K \) has two isomorphic components with \( \iota = (1,6)(2,7)(3,8)(4,5) \) establishing the isomorphism.
Note that $\iota$ is completely determined by, for instance, $(1,6)$. Furthermore, the automorphisms setwise stabilizing the component vertices are generated by $\alpha = (1,3)(2,4)$ and $\beta = (6,8)(5,7)$. Thus, $\text{Aut}(X_K) = \langle \iota, \alpha, \beta \rangle$.

Corollary 4 has established that Problem 18 is in $P$ and so we could design a centralizer algorithm based on the proof of the corollary. However, we can do better and will show how to construct a representation matrix for the centralizer in the same time bound. Here it will be useful to rewrite the centralizer as direct product of wreath products of semiregular groups.

Let $X_K$ be the cycle graph of the generating set $K$ of the group $G < S_n$. We split $X_K$ into its connected components, which we then classify into the isomorphism classes $J_1, \ldots, J_s$. Since components in distinct classes are not isomorphic, it follows that $\text{Aut}(X_K)$ and therefore $C_{S_n}(<K>)$ is the (external) direct product

$$W_1 \times W_2 \times \cdots \times W_s$$

of certain groups $W_i$ which act, respectively, on the vertices of the components in the class $J_i$.

Next, let $J_i$ consist of $m_i$ components. Since these components are isomorphic graphs, they can be permuted in all $m_i!$ ways. Furthermore, since the automorphism groups of isomorphic graphs are isomorphic, it follows that the group $W_i$ is isomorphic to the wreath product of a group $C_i$ by the symmetric group $S_{m_i}$. Here the group $G_i$ is the automorphism group of a representative component in the class $J_i$.

The groups $G_i$, in turn, are semiregular (Theorem 5 of Chapter V, or Theorem 10 above). Therefore, a representation matrix for $G_i$ must contain only one row of nonempty entries off the diagonal, i.e., it is simply a listing of its elements.

With these structural properties of $C_{S_n}(G)$ in mind, we now discuss how to construct a representation matrix $M_W$ for a direct factor $W$ of $C_{S_n}(G)$ from the cycle graph $X_K$ of $G = <K>$. Let $J = \{Z_1, \ldots, Z_m\}$ be a class of isomorphic connected components of
$x_K$, where $Z_i = (V_i, E_i)$ is a connected component with $t$ vertices and $G$ is the (semiregular) automorphism group of $Z_i$. We assume given a representation matrix $M_i$ for $G$ and $m$ isomorphisms $\pi_i$ from $Z_1$ to $Z_i$. Here we set $\pi_1 = (\cdot)$.

We describe how to construct a representation matrix $M_W$ for $W = G \setminus S_m$. For this construction (but not for its timing) the semiregularity of $G$ is immaterial. $M_W$ is first subdivided into the $t \times t$ submatrices $M_{i,j}$, $1 \leq i, j \leq m$. Clearly, all entries of $M_{i,j}$ should be empty whenever $i > j$. The diagonal submatrices $M_{i,i}$ should be representation matrices for the automorphism groups of the components $Z_i$. Let $v_1, ..., v_t$ be the enumeration of the rows and columns of $M_i$. We enumerate the rows and columns of $M_W$ in the sequence

$$v_1, ..., v_t, v_1^{\pi_2}, ..., v_t^{\pi_2}, ..., v_1^{\pi_m}, ..., v_t^{\pi_m}$$

and let $M_{i,i}$ $(1 \leq i \leq m)$ be the matrix obtained from $M_i$ by replacing the nonempty entry $\varphi$ with $\varphi^{\pi_i}$. By Corollary 2 of Chapter II, $M_{i,i}$ is a representation matrix for $\text{Aut}(Z_i)$.

Observe that $\pi_i^{-1}\pi_j$ defines an isomorphism which maps the component $Z_i$ to $Z_j$. This isomorphism is easily altered to an isomorphism $\psi_{i,j}$ which is a permutation exchanging $Z_i$ with $Z_j$ and fixing the remaining components pointwise. Now the matrix $M_{i,j}$, $j > i$, is obtained from the matrix $M_{i,i}$ by replacing the nonempty entry $\varphi$ in $M_{i,i}$ with $\varphi^{\psi_{i,j}}$. The correctness of this step follows from Theorem 4 of Chapter II. We observe that the construction of $M_W$ given $M_i$ and the maps $\pi_i$ requires $O(t^3m^2)$ steps. However, if $G$ is semiregular, then $M_i$ contains at most $O(t)$ nonempty entries. In this case, the time required to construct $M_W$ reduces to $O(t^2m^2)$ steps.

Finally, consider constructing a representation matrix for $G = W_1 \times \cdots \times W_r$ given representation matrices $M_i$ for the groups $W_i$, where the $W_i$ are groups with disjoint permutation domains. Here it is obvious that with the proper enumeration of the points in the permutation domain of $G$, the matrix $M_W$ is in block diagonal form, where the blocks are just the matrices $M_i$. The resulting algorithm is given below.
**Algorithm 2 (Centralizer)**

**Input** A generating set $K$ of the permutation group $G \leq S_n$.

**Output** A representation matrix $M$ for the centralizer $C_{S_n}(G)$ of $G$.

**Method**

1. begin
2. Construct the labelled cycle graph $X_K$ from the generating set $K$;
3. Partition $X_K$ into its connected components;
4. Classify the connected components into the isomorphism classes $J_1, \ldots, J_s$ using Theorem 10;
   
   **comment** Step 4 chooses in each isomorphism class an arbitrary component $Z_1$ as class representative and constructs an isomorphism $\pi_i$ from $Z_1$ to each of the remaining components $Z_i$ in the class;
5. for each isomorphism class $J = \{Z_1, \ldots, Z_m\}$ do begin
6. find all automorphisms of $Z_1$ using Corollary 4 and construct from these a representation matrix $M_1$ for the group $\text{Aut}(Z_1)$;
7. from $M_1$ and the isomorphisms $\pi_i$, construct a representation matrix $M_J$ for the group $W$ of all automorphisms of the subgraph of $X_K$ consisting of the components in $J$;
8. end;
9. combine the representation matrices $M_J$ into a representation matrix $M$ of $C_{S_n}(G)$;
10. output($M$);
11. end.

The correctness of the algorithm is clear from Corollary 4 and the discussion above. Also from the preceding discussion follows

**Proposition 5 (Hoffmann)**

Algorithm 2 requires at most $O(n^2 |K|)$ steps, where $n$ is the degree of $G = \langle K \rangle$.

Proposition 5 should be compared with Proposition 2 of Chapter II: Due to the structural properties of the centralizer, it is often computationally easier to determine the centralizer of a group $G$ from its generating set $K$ than, for example, the order of $G$. 
We now turn to Problem 19 and give an efficient algorithm for determining the center of a permutation group. It is clear that $C_{S_n}(G)$ normalizes $G$, i.e., for all $\pi \in C_{S_n}(G)$, $\pi G = G \pi$. We may therefore use Algorithm 1 to intersect $C_{S_n}(G)$ with $G$ from which we obtain the center of $G$. By Propositions 2 and 5 we obtain immediately

**Proposition 6 (Hoffmann)**

Let $G < S_n$ be a permutation group of degree $n$ generated by a set $K$ of permutations. Then we can determine a generating set for $C_G(G)$, the center of $G$, in $O(n^2 \cdot |K| + n^6)$ steps.

### 4.3. An Automorphism Restriction Problem

We finally consider the following special case of Problem 8, Restricted Graph Automorphism:

**Problem 20**

Given a graph $X = (V,E)$ and a generating set for a Sylow $p$-subgroup $G$ of $\text{Sym}(V)$, where $p$ is a fixed prime, determine the group $H$ of all automorphisms of $X$ which are also in $G$.

A polynomial time solution for this problem becomes evident once we recall that $G$ may be represented as the automorphism group of a regular (directed) cone graph $X_G$ of degree $p$ (cf. Chapter III, Subsection 3.2). We propose to superimpose $X$ and $X_G$ obtaining a new graph $Y$. The pointwise stabilizer in $\text{Aut}(Y)$ of the roots of $X_G$ will be the group $H$ which now can be determined using the techniques of Chapter V. The fact that $X_G$ is, in general, a directed cone graph presents no problems and is handled by routine modifications of the algorithms.

As illustration of the approach, consider the following

**Example 9**

We are given the Sylow 2-subgroup $G = \langle(1,3), (5,6), (1,2)(3,4)\rangle$ of $S_8$ and the graph $X_{3,3} = X = \{(1, \ldots, 8), \{(1,4), (1,5), (1,6), (2,4), (2,5), (2,6), (3,4), (3,5), (3,6)\}\}$, and wish to find $H = \text{Aut}(X) \cap G$.

The graph $X_G$ is shown in Figure 7 below. We superimpose $X$ and $X_G$ in the natural way, and obtain the graph $Y$ of Figure 8. Note that the stabilizer of $a$ and $b$ in $\text{Aut}(Y)$ is now $\text{Aut}(X) \cap G$. □
Therefore, we obtain

**PROPOSITION 7 (Hoffmann)**

For a fixed prime number Problem 20 is in P.

A considerably harder problem would be finding a Sylow p-subgroup of the automorphism group of the graph X. While it is true that every Sylow p-subgroup of Aut(X) is the intersection of Aut(X) with some Sylow p-subgroup of Sym(V), it is not clear how to even recognize that a given Sylow p-subgroup of Sym(V) is suited for this purpose.

5. Normal Closure, Commutator Subgroups, Solvability, and Nilpotence

There is a large variety of group-theoretic problems which arise as mathematically interesting questions and have no direct relationship with graph isomorphism. In this section, we sample a few of these problems. We have selected problems which are in P and whose solutions, furthermore, involve easy variants of the methods of Chapter II.
5.1. Normal Closure

**Definition 5**

Let $H$ be a subgroup of $G$. The *normal closure* of $H$ in $G$ is the smallest normal subgroup $N$ of $G$ which contains $H$.

Since the normal closure is the intersection of all normal subgroups of $G$ which contain $H$, it is clear that $H$ has a unique normal closure in $G$.

**Example 10**

Consider $G = S_4 = \langle (1,2), (1,2,3,4) \rangle$ and the subgroup $H = C_3 = \langle (1,2,3) \rangle$. Since $(1,2,3)(1,2,3,4) = (2,3,4) \not\in H$, $H$ is not its own normal closure and must contain the subgroup $A_4 = \langle (1,2,3), (2,3,4) \rangle$. Since $A_4$ is normal in $S_4$, it is the normal closure of $H$ in $G$. □

We will develop an algorithm for finding the normal closure of a subgroup with known generating set. The algorithm will be applied later to construct commutator groups and to test solvability and nilpotence of permutation groups. Specifically, we consider

**Problem 21 (Normal Closure)**

Given a generating set $K_G$ for the permutation group $G < S_n$ and a generating set $K_H$ for a subgroup $H$ of $G$, determine generators for the normal closure of $H$ in $G$.

The algorithm to be given for Problem 21 will be an extension of Algorithm 3 of Chapter II. Conceptually, we begin with the construction of a representation matrix $M_0$ for $H$. We then construct a set $K_1$ consisting of the entries in $M_0$ conjugated under every generator in $K_G$ and construct from $M_0$ and $K_1$ a representation matrix $M_1$ for the group $H_1 = \langle H \cup K_1 \rangle$. We repeat this process for $H_1$ provided $H$ is a proper subgroup of $H_1$. Continuing in this fashion, the ascending chain of subgroups

$$H < H_1 < H_2 < \cdots < H_r = H_{r+1}$$

of $G$ eventually becomes stationary with a group $H_r$ which is the normal closure of $H$ in $G$. The following theorem states this approach precisely:

**Theorem 12**

Let $H = \langle K_H \rangle$ be a subgroup of $G = \langle K_G \rangle$, a permutation group of degree $n$, and let $K_0$ be the set of nonempty entries in a representation matrix $M_0$ of $H_0 = H$. For $i \geq 1$,
define recursively

\[ K_i = \{ \varphi^n \mid \varphi \in K_{i-1}, \pi \in K_G \}, \]

\[ H_i = \langle K_{i-1} \cup K_i \rangle, \]

\( K_i \) is the set of all nonempty entries in \( M_i \), a representation matrix for \( H_i \).

Then there exists an integer \( 0 \leq r \leq \log_2(|G|) \) such that \( N = H_r = H_{r+1} \) is the normal closure of \( H \) in \( G \).

**Proof** Clearly \( H_i \) is a subgroup of \( H_{i+1} \) and of \( G \) for all \( i \geq 0 \). If \( H_i \) is a proper subgroup of \( H_{i+1} \), then the order of \( H_{i+1} \) is at least twice the order of \( H_i \). On the other hand, if \( H_i \) is equal to \( H_{i+1} \), then also \( H_i = H_{i+j}, j > 0 \), and the subgroup chain is stationary past \( i \). Since \( H_i < G \), the chain must become stationary past \( r = \log_2(|G|) \).

Now let \( N \) be the normal closure of \( H \) in \( G \). Clearly \( H_i < N \) for all \( i \geq 0 \). Furthermore, if \( H_r = H_{r+1} \), then \( H_r \) is normal in \( G \). Hence \( H_r = N \).

A good implementation of the normal closure algorithm should not imitate Theorem 12 by constructing the groups \( H_i \) in succession, since this leads to sifting many redundant permutations. Rather, as each new entry into the representation matrix is made, we add to the queue of permutations to be sifted subsequently not only pair products but also all conjugates of the new entry under each generator of \( G \).

The resulting algorithm is now as follows:
**Algorithm 3 (Normal Closure)**

**Input** Generating sets $K_H$ and $K_G$ of the permutation groups $H$ and $G$, respectively, where $H < G < S_n$.

**Output** Representation matrix $M$ of the normal closure $N$ of $H$ in $G$.

**Method**
1. **begin**
2. initialize a representation matrix $M$ to represent the trivial group $I$;
3. $Queue := K_H$;
4. while $Queue$ is not empty do begin
5. remove $\varphi$ from $Queue$;
6. if sifting $\varphi$ causes the new entry $\psi$ in $M$ then begin
7. add to $Queue$ all pair products formed with $\psi$ and with nonempty entries in $M$;
8. add to $Queue$ $\{\psi^n \mid \pi \in K_H\}$;
9. end;
10. end;
11. output($M$);
12. end.

Let $M$ be the final matrix output by Algorithm 3. Since $M$ is closed under pair product sifting, it is the representation matrix of a group $N$. Clearly, $H < N < G$. The group $N$ is normal in $G$ because the conjugation of each entry of $M$ under every generator of $G$ is again in $N$. Moreover, each entry in $M$ arises as a product of generators of $H$, generators of $H$ conjugated under generators of $G$, and inverses of such permutations. Therefore $N$ is the normal closure of $H$ in $G$, i.e., Algorithm 3 is correct. The time required by the algorithm is analyzed in the following

**Proposition 8 (Furst, Hopcroft, Luks, Sims)**
Algorithm 3 requires at most $O(|K_H| \cdot n^2 + |K_G| \cdot n^4 + n^6)$ steps.

**Proof** Queue contains initially $|K_H|$ permutations. For each of the up to $O(n^3)$ entries made in $M$, we add up to $O(n^2)$ pair products and $|K_G|$ conjugates. Hence a total of at most $O(|K_H| + n^4 + |K_G| \cdot n^3)$ permutations are sifted, from which the stated bound follows. $\blacksquare$
5.2. Commutators and Commutator Groups

A number of important group properties can be formulated in terms of commutators and commutator derived subgroup towers. We now develop the necessary concepts to express solvability and nilpotence of groups in this framework.

**Definition 6**
For the elements \( \pi \) and \( \psi \) of a group \( G \), we call \( [\pi, \psi] = \pi^{-1} \psi^{-1} \pi \psi \) the commutator of \( \pi \) by \( \psi \).

The term commutator derives from the identity \( \pi \psi = \psi [\pi, \psi] \). The following lemma states this and other elementary identities for commutators and is easy to prove.

**Lemma 11**
(a) \( \pi \psi = \psi [\pi, \psi] \).
(b) \( [\pi, \psi] = [\psi, \pi]^{-1} \).
(c) \( [\pi, \psi \varphi] = [\pi, \varphi] [\pi, \psi] \varphi \).
(d) \( [\pi \varphi, \psi] = [\pi, \psi] \varphi [\varphi, \psi] \).

Extending Definition 6 for the complexes \( A, B \subset G \), we set
\[
[A, B] = \langle [\alpha, \beta] \mid \alpha \in A, \beta \in B \rangle
\]
Note that \( \langle [\alpha], [\beta] \rangle = \langle [\alpha, \beta] \rangle \) is not equal to \( [\alpha, \beta] \). Furthermore, the group \( [A, B] \) contains in general elements which are not commutators of elements in \( A \) by elements in \( B \). This remains true even when \( A \) and \( B \) are groups.

**Lemma 12**
For the subgroups \( A \) and \( B \) of \( G \) the following is true:
(a) \( [A, B] = [B, A] \).
(b) \( [A, B] \triangleleft [A, B] \).
(c) \( [A, B] \triangleleft A \) iff \( B \) normalizes \( A \).

**Proof** Part (a) follows from Lemma 11b. For Part (b), let \( \pi, \varphi \in A, \psi, \chi \in B \). By Lemma 11c, \( [\pi, \psi] \chi = [\pi, \chi]^{-1} [\pi, \psi \chi] \in [A, B] \), and by Lemma 11d, \( [\pi, \psi] \varphi = [\pi \varphi, \psi] [\varphi, \psi]^{-1} \in [A, B] \). Thus \( [A, B] \) is normal in \( [A, B] \). Part (c) is trivial.

**Definition 7**
The subgroup \( G' = \langle [\pi, \psi] \mid \pi, \psi \in G \rangle = [G, G] \) of \( G \) is called the commutator group or the derived group of \( G \).
We define higher commutator groups recursively by

(1) \( G^{(0)} = G \).

(2) \( G^{(i+1)} = (G^{(i)})' = [G^{(i)}, G^{(i)}], 0 \leq i \),

and prove a result about the subgroup tower

\[ G > G' > G^{(2)} > G^{(3)} > \ldots > G^{(r)} = G^{(r+1)} \]

which clearly consists of characteristic subgroups of \( G \). This subgroup tower is also called the derived series of \( G \).

**Theorem 13**

Let \( N \) be a subgroup of \( G \). Then \( N \) is normal in \( G \) with the abelian factor group \( G/N \) iff \( G' \subset N \).

**Proof** If \( N \) is normal in \( G \) and \( G/N \) is abelian, then, for \( n, \varphi \in G \),

\[ \pi \varphi N = (\pi N)(\varphi N) = (\varphi N)(\pi N) = \varphi \pi N, \]

hence \( [\pi, \varphi] \subset N \) by Lemma 11a. By the definition of \( G' \), therefore, \( G' \subset N \).

Now assume that \( G' \subset N \). For \( \pi \in N, \varphi \in G \) we have

\[ \pi^\varphi = \pi[\pi, \varphi] \subset NG' = N, \]

hence \( N \) is normal in \( G \). Now for \( \pi, \varphi \in G \) we have

\[ \pi \varphi N = \varphi \pi[\pi, \varphi] N = \varphi \pi N, \]

so \( G/N \) is abelian. ∗

By Theorem 13, we may interpret \( G' \) as the minimal normal subgroup of \( G \) such that \( G/G' \) is abelian. From the uniqueness of \( G' \) follows that \( G' \) is characteristic in \( G \).

If \( G \) is characteristically simple, therefore, either \( G' = G \), and then \( G \) is nonabelian, or \( G' = I \), and then \( G \) is abelian. Note that \( G' = I \) iff \( G \) is abelian.

**Definition 8**

The finite group \( G \) is solvable if \( G \) has a composition series in which every composition factor is abelian.

We can characterize solvability using commutator groups. The following result follows readily from Theorems 13 above and from Theorems 2 and 3 of Chapter V:

**Proposition 9**

The finite group \( G \) is solvable iff \( G^{(r)} = I \) for all \( r \geq \log_2(\mid G \mid) \).
Next, we discuss nilpotence of groups. Recall the definition of a central series for the group $G$ (Chapter III, Definition 10).

**Definition 9**

A group $G$ is **nilpotent** if $G$ has a central series.

From Chapter III we know that every (finite) $p$-group is nilpotent. However, the class of nilpotent groups is larger than the class of $p$-groups. It includes, for example, the abelian groups. We define recursively the following subgroups of the finite group $G$:

- $K_1(G) = G$, and
- $K_{i+1}(G) = [K_i(G), G]$.

We will express nilpotence in terms of the subgroup tower

$$G = K_1(G) > K_2(G) > \cdots > K_s(G) = K_{s+1}(G)$$

which clearly consists of characteristic subgroups of $G$.

**Lemma 13**

The subgroup tower

$$G = N^{(1)} > N^{(2)} > \cdots > N^{(t)} = 1$$

is a central series for $G$ iff $[N^{(i)}, G] < N^{(i+1)}$.

**Proof** Let $[N^{(i)}, G] < N^{(i+1)} < N^{(i)}$. By Lemma 12c, $N^{(i)}$ is normal in $G$. Furthermore, for $\pi \in N^{(i)}$ and $\psi \in G$, we have $\pi \psi N^{(i+1)} = \psi \pi N^{(i+1)} = \psi N^{(i+1)}$, hence $\pi N^{(i+1)}$ commutes with $\psi N^{(i+1)}$, i.e., $N^{(i)}/N^{(i+1)}$ is a subgroup of the center of $G/N^{(i+1)}$.

Conversely, assume that the groups $N^{(i)}$ form a central series. Then, for $\pi \in N^{(i)}$ and $\psi \in G$ we have $\pi \psi N^{(i+1)} = \psi N^{(i+1)}$, thus $[\pi, \psi] \in N^{(i+1)}$, i.e., $[N^{(i)}, G] < N^{(i+1)}$.

Since $K_{i+1}(G) = [K_i(G), G]$ and by Lemma 13 above, the subgroup tower

$$G = K_1(G) > K_2(G) > \cdots > K_s(G) = K_{s+1}(G)$$

is a central series for $G$ provided that $K_s(G) = 1$. In this case we call the tower the descending central series of $G$.

**Theorem 14**

$G$ is nilpotent iff $K_s(G) = 1$ for all $s \geq \log_2(|G|)$.

**Proof** By Lemma 13, $G$ has a central series if $K_s(G) = 1$, and so $G$ is nilpotent. Conversely, assume that $G$ has the central series
We will show that $K_1(G) < N^{(i)}$. Clearly $K_1(G) = G = N^{(1)}$. Assume inductively that $K_i(G) < N^{(i)}$. Then, by Lemma 13, $K_{i+1}(G) = [K_i(G), G] < [N^{(i)}, G] < N^{(i+1)}$.

The bound for $s$ follows from the fact that the $K_i(G)$ tower becomes stationary after the smallest value of $i$ such that $K_i(G) = K_{i+1}(G)$.

It is clear that nilpotence implies solvability. For if $G$ has the central series

$$G = N^{(1)} > N^{(2)} > \cdots > N^{(r)} = 1,$$

then the factor groups $N^{(i)/N^{(i+1)}}$ are certainly abelian, hence $G$ is solvable. However, nilpotence is the stronger property:

**Example 11**

Consider $G = S_4 = \langle (1,2), (1,2,3,4) \rangle$. Then $G^{(1)} = A_4 = \langle (1,2,3), (2,3,4) \rangle$, $G^{(2)} = V_4 = \langle (1,2)(3,4), (1,3)(2,4) \rangle$, and $G^{(3)} = 1$. Consequently, $S_4$ is solvable. However, $K_2(G) = K_3(G) = A_4$, and therefore $S_4$ is not nilpotent.

5.3. Testing Solvability and Nilpotence

By the results of the preceding section, testing solvability and nilpotence of permutation groups may be based on an efficient algorithm for constructing the commutator group $[A, B]$ of the groups $A$ and $B$ in $S_n$. We therefore consider the following three problems:

**Problem 22 (Commutator Group)**

Given generating sets $K_A$ and $K_B$ for the groups $A$ and $B$, respectively, where $A, B < S_n$, find a generating set for the commutator group $[A, B]$.

**Problem 23 (Solvability)**

Given a generating set $K$ for $G < S_n$, test whether $G$ is solvable.

**Problem 24 (Nilpotence)**

Given a generating set $K$ for $G < S_n$, test whether $G$ is nilpotent.

A seeming difficulty in designing an efficient algorithm for Problem 22 is finding a suitable generating set for $[A, B]$ given generating sets for $A$ and for $B$. Since the groups $A$ and $B$ may be large, we should not attempt to construct the set
K = \{ [\alpha, \beta] \mid \alpha \in A, \beta \in B \} which is clearly a generating set for [A,B]. The following theorem resolves this difficulty by reducing Problem 22 to Problem 21, finding the normal closure:

**Theorem 15**

Let \( A = <K_A> \) and \( B = <K_B> \) be two permutation groups of degree \( n \). Then \([A,B]\) is the normal closure in \(<A,B>\) of the group generated by the set \( K_1 = \{ [\alpha, \beta] \mid \alpha \in K_A, \beta \in K_B \} \).

**Proof** By Lemma 12b, \([A,B]\) is normal in \(<A,B>\). Hence it suffices to show that every commutator \([\alpha, \beta]\), \( \alpha \in A, \beta \in B \), is in the normal closure \( N \) of \( H = <K_1> \). Since \( K_A \) generates \( A \) and \( K_B \) generates \( B \),

\[
[a, b] = [a_1 a_2 \cdots a_r b_1 b_2 \cdots b_s],
\]

where \( a_i \) or \( a_i^{-1} \) is in \( K_A \) and \( b_j \) or \( b_j^{-1} \) is in \( K_B \), \( 1 \leq i \leq r, 1 \leq j \leq s \). By repeated application of Lemma 11, therefore, \([\alpha, \beta]\) can be expressed as finite product of elements of the form \([b_j, a_i]_\gamma \) or \([a_i, b_j]_\gamma \), where \( a_i \in K_A, \beta_j \in K_B, \) and \( \gamma \in <A,B> \). Therefore, \([\alpha, \beta] \in N\), and so \([A,B] = N\). ~

From Theorem 15 we immediately obtain polynomial time algorithms for Problems 22 through 24:

**Corollary 5 (Furst, Hopcroft, Luks, Sims)**

Given generating sets \( K_A \) and \( K_B \) for the groups \( A \) and \( B \), respectively, where \( A, B < S_n \), a representation matrix for \([A,B]\) can be determined in \( O((|K_A| + |K_B|)n^2 + n^6) \) steps.

**Proof** In \( O((|K_A| + |K_B|)n^2 + n^6) \) steps we compute representation matrices for \( A, B, \) and \(<A,B>\), from which we obtain generating sets for each group of size \( O(n^2) \). From these, we can compute an \( O(n^4) \) set \( K_1 \) of Theorem 15. The corollary now follows from Theorem 15 and Proposition 8. ~

**Corollary 6 (Furst, Hopcroft, Luks, Sims)**

Given a generating set \( K \) for the group \( G < S_n \), we can test in \( O(|K|n^2 + n^6 \log_2(|G|)) \) steps whether \( G \) is nilpotent or solvable.

**Proof** Immediate from Proposition 9, Theorem 14, and Corollary 5. ~
6. Open Problems

Despite much research, an accurate complexity classification of Problems 1 through 10 remains open. In Section 2 of this chapter, we have given technical evidence suggesting that none of these problems is NP-complete. However, we conjecture that at least Problems 1 through 8 do not belong to P.

We now discuss additional open problems. Problem 25 below is a question related to Problem 1, Double Coset Membership. Problem 26 generalizes the difficulty encountered in Chapter III in the design of a subexponential algorithm for (regular) cone graphs. It also generalizes the Labelled Graph Automorphism Problem (Problem 1 of Chapter III) in the group-theoretic sense.

**Problem 25 (Double Coset Partition)**
Given generating sets for the permutation groups A, B < Sₙ, determine r, the number of distinct double cosets of A and B in Sₙ.

**Problem 26 (Intransitive Subgroup Problem)**
Given generators for the group G = G₁ × G₂ × ⋯ × Gₘ < Sₙ, where |Gᵢ| ≤ k for some constant k, and given a polynomial time membership test for a subgroup H of G as well as for the subgroups Hᵢ = H ∩ Gᵢ, determine generators for H.

Problem 25 has the following special case: If the groups A and B are restricted to the groups occurring in Problems 9 and 10, then Problem 25 asks for the number of nonisomorphic graphs with n vertices and a prescribed number of edges. It is not evident that even the restricted version of Problem 25 is in NP. There is, however, a subexponential (in n) algorithm for this restricted version.

We pointed out earlier that an efficient algorithm for Problem 26 entails a subexponential algorithm for (regular) cone graphs along the ideas of Section 2 of Chapter III. Such an algorithm would also entail an efficient isomorphism test for graphs whose adjacency matrices have eigenvalues with multiplicities bounded by a fixed constant, but this class of graphs can be handled using a slightly different approach. A good starting point for Problem 26 might be the following restriction:
**Problem 27 (Subspace Problem)**

Given a polynomial time membership test for a linear subspace $S < \mathbb{Z}_2^m$ of the $m$-dimensional vector space over the integers modulo 2, and given the vectors $v_1, \ldots, v_k \in \mathbb{Z}_2^m$ such that $\dim(<S, v_1, \ldots, v_k>) = \dim(S) + k$, determine the dimensionality of $S$.

Typically, the subspace $S$ of Problem 27 (or the subgroup $H$ of Problem 26) is specified as the automorphism group of a combinatorial structure, e.g. a graph or a matrix. So far, every successful attack on such instances of Problem 27 has exploited special properties of the combinatorial object and therefore cannot be generalized.

Finally, we mention a class of open problems more directly related to graph isomorphism about which little seems to be known: Given a graph $X$ whose automorphism group is to be determined. Which additional *a priori* information about $\text{Aut}(X)$ simplifies this problem? For example, such additional information could be that $\text{Aut}(X)$ is elementary abelian, or that the stabilizer of a vertex $v$, $\text{Aut}_v(X)$, is a known permutation group $G$. The Labelled Graph Automorphism Problem is a solved instance of this question.

Related to the spirit of this problem area is the open problem of testing isomorphism of rigid graphs, i.e., of graphs that have only trivial automorphisms. It is known that this problem is equivalent to recognizing rigidity, but it is not known to be isomorphism complete. Moreover, an isomorphism between two rigid graphs is unique.

7. Notes and References

Brown, Hjelmeland, and Masinter [1974] consider double coset partitions of $S_n$ as nonisomorphic vertex labellings of graphs, and so interpreting double cosets as isomorphism classes is implicit in their work. Problem 25 is from that paper, and the authors give an exponential algorithm for it.

The group-theoretic generalization of graph isomorphism is from Hoffmann [1981a]. Problems 7 and 8 were proposed in private correspondence by Luks who also proved first the polynomial time equivalence of Problems 5 through 8. The relation-
ship between testing membership in double cosets and intersecting permutation groups is from Hoffmann [1980b]. The idea of the proofs of Theorems 2 and 3 goes back to an exponential algorithm for intersecting permutation groups of Sims [1971b]. Problem 4 was considered by Kannan and Lipton (unpublished) who proved the equivalence of Problems 4 and 5. The proof given here (Theorem 5) is due to Luks (private communication).

The structure of problems in NP which are neither complete nor in P has been studied by Ladner [1975]. Valiant [1979] discusses the complexity of enumeration problems. A brief survey of the material appears in Garey and Johnson [1979].

Problem 12 and Theorem 9 are from Hoffmann [1980b], as are Problem 13 and Algorithm 1. Proposition 4 is noted in Luks [1980].

Section 4.2 follows Hoffmann [1981]. According to C.C. Sims, the centralizer algorithm dates back to at least 1970. A published version can be found in Fontet [1977]. The center algorithm, in contrast, appears to be new.

The presentation of the group-theoretic material in Section 5 follows Huppert [1967]. Furst, Hopcroft and Luks [1980b] give a polynomial time algorithm for computing the normal closure. Their version is based on the proof of Theorem 12. Algorithm 3 is superior and was suggested by C.C. Sims. Furst, Hopcroft and Luks [1980b] apply the normal closure algorithm to test solvability, but do not mention the nilpotence test.