CHAPTER V

GRAPHS OF FIXED VALENCE AND CONE GRAPHS OF FIXED DEGREE

We will now develop a polynomial time isomorphism test for graphs of fixed valence. Having done so, we then discuss the wider applicability of these techniques. We already remarked that the method can be used for testing isomorphism of cone graphs of fixed degree. It is also true that it can be used for testing isomorphism of other graphs, and we discuss these generalizations at the end of the chapter.

The basic approach to testing isomorphism of graphs of fixed valence is as in Chapter IV: Let $X = (V,E)$ be a graph of valence $d$, $e$ an edge of $X$. Without loss of generality, we assume that $X$ is connected. As before, we consider the subgraphs $X_k$ of $X$, $0 \leq k \leq h+1$, induced by classifying the vertices of $X$ by their distance from the edge $e$, and we determine generators for the groups $\text{Aut}_e(X_k)$. Finding generators for $\text{Aut}_e(X_{k+1})$ from generators for $\text{Aut}_e(X_k)$ and the edge set $E_k$ (defined as in Chapter IV) again divides into

1. finding the subgroup $B$ of $A = \text{Aut}_e(X_k)$ consisting of all automorphisms in $A$ which can be extended to an automorphism in $\text{Aut}_e(X_{k+1})$, and
2. finding generators for $A^{[k]}(X_{k+1})$, the pointwise stabilizer in $\text{Aut}_e(X_{k+1})$ of all vertices at distance $k$ or less from $e$ in $X_{k+1}$.

We will see that Step (2) is as easy as in the case of trivalent graphs and that it can be done by inspection. Step (1) is accomplished by the same general ideas as in the trivalent case. That is, it involves classifying the edges in $E_k$ into types and families, studying the action of $A$ on the set $W$ consisting of all subsets (of small cardinality) of the set $V_k$, and computing the setwise stabilizer of the ancestries of equal type. The newly arising difficulty is that the groups in which the setwise stabilizer is to be determined are not necessarily $p$-groups. Because of this, we have to develop new group-theoretic machinery.

We present the algorithm as follows: First, we develop the basic algorithm for computing $\text{Aut}_e(X)$, where $X$ is a connected graph of valence $d$ and $d$ is a constant, and discuss this algorithm in every aspect except for the step computing setwise stabilizers. Having established the basic method, we then prove that the automorphism groups arising have a particular structure which we have to describe using additional
concepts from Group Theory. Finally, we show how to exploit this structure and design a polynomial time algorithm for computing setwise stabilizers in such groups. This new algorithm will be a generalization of Algorithm 2 of Chapter IV.

1. The Basic Algorithm

We will design an algorithm for the following

**Problem 1**

Let $X$ be a connected graph of valence $d$, where $d$ is a constant, and let $e$ be an edge of $X$. Determine a generating set for $\text{Aut}_e(X)$, the group of all automorphisms of $X$ (setwise) stabilizing the edge $e$.

Elementary arguments establish that a polynomial time algorithm for Problem 1 gives a polynomial time algorithm for testing isomorphism of (not necessarily connected) graphs of valence $d$.

1.1. Outline of the Method

We approach Problem 1 in the same way as Problem 1 of Chapter IV. Let $X = (V, E)$ be a connected graph of valence $d$, $e = (v_1, v_2)$ an edge of $X$. Assume we wish to determine $\text{Aut}_e(X)$. As before, let $V_k$ be the set of vertices of distance $k$ from $e$ and let $h$ be the height of $X$, i.e., let $V = V_0 \cup V_1 \cup \cdots \cup V_h$. The subsets $E_k$ of edges of $X$, $0 \leq k \leq h$, are defined by

$$E_k = \{ (u, w) \mid u \in V_k, w \in V_k \cup V_{k+1} \},$$

where $V_{h+1} = \emptyset$ by definition. We define the graphs $X_j$, $0 \leq j \leq h+1$, as in Chapter IV:

- $X_0 = (V_0, \emptyset)$
- $X_1 = (V_0 \cup V_1, E_0)$
- $X_2 = (V_0 \cup V_1 \cup V_2, E_0 \cup E_1)$
- $\vdots$
- $X_h = (V, E_0 \cup \cdots \cup E_{h-1})$
- $X_{h+1} = (V, E) = X$

We will determine generators for $\text{Aut}_e(X_{k+1})$ from generators for $\text{Aut}_e(X_k)$, $0 \leq k \leq h$. 
\[ \text{Aut}_e(X_0) \text{ is, of course, } \langle (v_1, v_2) \rangle. \]

Let \( A = \text{Aut}_e(X_k) \). Determining \( \text{Aut}_e(X_{k+1}) \) proceeds in two steps: First, determine the subgroup \( B \) of \( A \) consisting of all permutations in \( A \) which may be extended to an automorphism of \( \text{Aut}_e(X_{k+1}) \), and extend \( B \) to the larger permutation domain. Second, determine generators for the pointwise stabilizer of all vertices in \( V_0 \cup \cdots \cup V_k \) in the group \( \text{Aut}_e(X_{k+1}) \). The first step will be reduced to finding the setwise stabilizer in a homomorphic image of \( \text{Aut}_e(X_k) \). Due to the definition of the edge set \( E_{k+1} \), the second step can be accomplished by inspection.

Consider the group \( \tilde{A} \), the restriction of \( A = \text{Aut}_e(X_k) \) to the vertex set \( V_k \). We determine the subgroup \( \tilde{B} \) consisting of those permutations in \( \tilde{A} \) which may be extended to automorphisms of the graph \( (V_k \cup V_{k+1}, E_k) \). Since \( \tilde{B} \) is a subgroup of \( \tilde{A} \), every element of \( \tilde{B} \) may be extended to an automorphism in \( \text{Aut}_e(X_{k+1}) \). Clearly \( \tilde{B} \) is the restriction of the group \( \text{Aut}_e(X_{k+1}) \) to \( V_k \).

Our first task will be to review how to determine \( \tilde{B} \) from a setwise stabilizer in a homomorphic image of the group \( \tilde{A} \).

Let \( u \in V_{k+1} \) and recall that the ancestry of \( u \) is the set of vertices in \( V_k \) adjacent to \( u \). Since \( X \) has valence \( d \), every ancestry has cardinality at most \( d \). Recall the classification of edges in \( E_k \) into types and their grouping into families: Let \( (w,v) \in E_k \).

If \( (w,v) \) is a cross edge, then the edge has the type \( t_{0,2} \). Otherwise, let \( w \in V_{k+1}, v \in V_k \). Then the type of the edge \( (w,v) \) is \( t_{i,j} \), where \( j \) is the cardinality of the ancestry of \( w \), and \( i-1 \) is the number of vertices in \( V_{k+1} \) with the same ancestry as \( w \). Since \( X \) has valence \( d \), note that \( j \leq d \) and \( i \leq d-1 \). Next, if \( (w,v) \) has type \( t_{0,2} \), then its family is \( \{(w,v)\} \). Otherwise, if \( (w,v) \) has type \( t_{i,j} \), \( i > 0 \), then the family of this edge is the set \( \{(w,v), (w,v_2), \ldots, (w,v_j), (w_2,v), \ldots, (w_l,w_j)\} \), consisting of the \( ij \) edges in \( E_k \) connecting the vertices \( w, w_2, \ldots, w_i \) in \( V_{k+1} \) with their common ancestry, the vertices \( v, v_2, \ldots, v_1 \) in \( V_k \).

If \( F \) is a family of edges of type \( t_{i,j} \), then \( (F)_k \) denotes the set of \( j \) vertices of \( V_k \) incident to the family and \( (F)_{k+1} \) denotes the set of \( i \) vertices in \( V_{k+1} \) incident to the family. We observe that Lemmata 1 and 2 and Corollary 2 of Chapter IV are true for arbitrary graphs, thus in particular for graphs of fixed valence.

Let \( W \) be the collection of all subsets of \( V_k \) of size not exceeding \( d \). Consider the group \( G \) defined by the induced action of \( \tilde{A} \) on \( W \). We label the points \( z \) in \( W \) with \( t_{i,j} \), where \( 0 \leq i \leq d-1, 1 \leq j \leq d \). Here \( z \) is labelled \( t_{i,j} \) if \( z = (F)_k \) for some family \( F \) of
edges in $E_k$ of type $t_{i,j}$. The remaining, unlabelled points of $W$ are now labelled $t_{0,0}$. Observe that any point in $W$ can have at most two labels; that is, the only multiple labels possible are $t_{i,2}$ and $t_{0,2}, 1 \leq i \leq d-2$. (Since $X$ has valence $d$ it is not possible that $i > d-2$.) Such points with two labels may be labelled $t_{0,i,2}$ instead. Note that we have used up to $d^2$ distinct labels. Let $H$ be the subgroup of $G$ consisting of all elements in $G$ which (setwise) stabilize the subsets of equally labelled points of $W$. Let $\bar{H}$ be the subgroup of $\bar{A}$ corresponding to the subgroup $H$ of $G$. By Lemmata 1 and 2 of Chapter IV, $\bar{H}$ is the subgroup of $\bar{A}$ consisting of all permutations of $V_k$ which may be extended to an automorphism in $\text{Aut}_c(X_{k+1})$.

Because of the presence of singletons in $W$, it is easy to obtain generators for $\bar{H}$ from generators of the subgroup $H$ of $G$. Furthermore, we can use the same method as in Chapter IV for extending these generators to elements of $\text{Aut}_c(X_{k+1})$.

As a consequence of Lemma 3 of Chapter IV, we now have a way of finding generators of the group $H$ and a way of extending these generators to elements in $\text{Aut}_c(X_{k+1})$. Thus, we have an algorithm for Step one. We assume here, of course, that there is an efficient method for computing the setwise stabilizer in the groups $G$.

We now turn to Step two, the determination of $A^{(k)}(X_{k+1})$, the group of those automorphisms in $\text{Aut}_c(X_{k+1})$ which pointwise stabilize the vertices in $V_0 \cup \cdots \cup V_k$.

By Corollary 2 of Chapter IV, every automorphism in $A^{(k)}(X_{k+1})$ must setwise stabilize the vertex sets $(F)_{k+1}$, $F$ the families of $E_k$ and these sets are the blocks of a partition of $V_{k+1}$. Clearly, if $F$ is any family, then the vertices in $(F)_{k+1}$ may be permuted arbitrarily, thus $A^{(k)}(X_{k+1})$ must be the direct product of the symmetric groups of these sets. Since $X$ has valence $d$, no set $(F)_{k+1}$ has cardinality exceeding $d-1$, thus $A^{(k)}(X_{k+1})$ is the direct product of symmetric groups of degree at most $d-1$.

1.2. The Algorithm

Algorithm 1 below formally specifies the method outlined above. The main loop successively determines generating sets for the groups $\text{Aut}_c(X_k)$ given a connected graph $X$ of valence $d$. Note that the algorithm is nearly identical to Algorithm 1 of Chapter IV. Because of this, we can be brief in our comments and the subsequent analysis.
**Algorithm 1 (Automorphism of Graphs of Valence d)**

**Input**  
A connected graph \( X = (V,E) \) of valence \( d > 3 \) and an edge \( e = (v_1,v_2) \) of \( X \).

**Output**  
A generating set for \( \text{Aut}_e(X) \).

**Method**

1. \textbf{begin}
2. Using breadth-first search, determine the vertex sets \( V_0, ..., V_h \) and the edge sets \( E_0, ..., E_h \);
3. Determine \( K_0 \), a generating set for \( \text{Aut}_e(X_0) \);
4. \textbf{for} \( k := 0 \) \textbf{to} \( h \) \textbf{do begin}
5. From the set \( K_k \), construct the set \( \overline{K} \), generating the group \( \overline{A} \) which is the restriction of \( \text{Aut}_e(X_k) \) to \( V_k \);
6. Construct \( W \), the set of all subsets of \( V_k \) of size at most \( d \);
7. From \( \overline{K} \), construct \( D \), a generating set for the group \( G \) defined by the induced action of \( \overline{A} \) on \( W \);
8. Classify the edges in \( E_k \) by type and group them into the families \( F_1, ..., F_r \);
9. Partition \( W \) into the blocks \( J_1, ..., J_s \), \( s \leq d^2 \), according to the types of the families \( F \) and the sets \( (F)k \);
10. Find a generating set for \( H \), the setwise stabilizer of the blocks \( J_1, ..., J_s \) in the group \( G \);
11. From the generating set for \( H \), construct \( \overline{D} \), a generating set for \( \overline{B} \), the restriction of \( \text{Aut}_e(X_{k+1}) \) to \( V_k \);
12. Construct a representation matrix for \( A = \text{Aut}_e(X_k) \), where the vertices in \( V_k \) are stabilized first;
13. Initialize \( K_{k+1} \), the generating set for \( \text{Aut}_e(X_{k+1}) \), to contain the generators of the pointwise stabilizer of \( V_k \) in \( \text{Aut}_e(X_k) \);
14. \textbf{for each} generator \( \pi \) in \( \overline{D} \) \textbf{do begin}
15. find \( \varphi \in A \) whose restriction to \( V_k \) is \( \pi \);
16. if \( k < h \) then begin
17. find \( \chi \), the extension of \( \varphi \) to an automorphism of \( X_{k+1} \);
18. add \( \chi \) to \( K_{k+1} \);
19. end
20. else add \( \varphi \) to \( K_{k+1} \);
21. \textbf{end}
22. \textbf{end}
21. end;
22. for each set $(F)_{k+1}$ do
23. if $(F)_{k+1} = \{u_1, \ldots, u_t\}$, where $t \geq 2$, then add $\pi_1 = (u_1, u_2, \ldots, u_t)$ and $\pi_2 = (u_1, u_2)$ to $K_{k+1}$;
 comment Note that $t < d$;
24. end;
25. output($K_{h+1}$);
26. end.

We analyze Algorithm 1 without accounting for the exact bound on Step 10. As in Section 2 of Chapter IV, we assume that Step 10 requires $T(m)$ steps, where $m$ is the degree of $G$, assuming further that $G$ is presented by a generating set of size $O(m^2)$ and that the generating set determined for $H$ is also of size $O(m^2)$.

Assume that $X$ has $n$ vertices, and observe that $X$ cannot have more than $d-\frac{n}{2}$ edges. Let $n_k$ be the cardinality of $V_k$, and note that $E_k$ is $O(d,(n_k+n_{k+1}))$ in size.

We begin by estimating the time required in each iteration of the for-loop extending through Lines 4-24, assuming that $K_k$ has cardinality $O(n^2)$ and that the constant of proportionality in this bound does not depend on $d$. Arguing as in Chapter IV, it is clear that Lines 5 and 6 require $O(n^3)$ and $O(n^2)$ steps, respectively. Line 7 requires $O(n^2 n_k^2 + n_k^6 + n_k^{d+2})$ steps if we first reduce $K$ to $O(n_k^2)$ permutations. Line 8 can be implemented in $O(d,(n_k+n_{k+1}))$ steps, and Line 9 in $O(n_k^2)$ steps.

By assumption, Line 10 requires $T(n_k^3)$ steps and delivers a generating set of size at most $n_k^{2d}$, since $H$ has degree $O(n_k^d)$.

For Lines 11-21, the dominating steps are Line 11 $(O(n_k^{3d})$ steps) and Line 12 $(O(n^6)$ steps). Since $n \geq d \geq 4$ and $n \geq n_k+n_{k+1}$, Lines 11-21 require a total of $O(n^6+n_k^{3d})$ steps.

The loop in Lines 22 and 23 takes no more that $O(n-(n_k+n_{k+1}))$ steps. In summary, therefore, Lines 5-23 can be implemented in $O(n^6+n_k^{3d}+T(n_k^d))$ steps. Clearly the set $K_{k+1}$ contains $O(n^2)$ permutations of degree $n$. Since $h \leq n$, the for-loop of Lines 4-24 requires a total of $O(n^{3d}+\sum_{k=1}^{h} T(n_k^d))$ steps.

Under the assumption that $T(m)$ increases monotonically with $m$ and at least as fast as linearly in $m$, we obtain $\sum_{k=1}^{h} T(n_k^d) = T(n^d)$. Clearly, the running time of the loop
dominates all other steps. Therefore, in summary, we have just shown Theorem 1 below. Note that Theorem 2 of Chapter IV is a special case of this theorem.

**Theorem 1**

Let \( X \) be a connected graph of valence \( d \) with \( n \) vertices. Assume given a procedure for Step 10 which determines setwise stabilizers in the groups \( G \) which arise, and that for a group of degree \( m \) a generating set of \( O(m^2) \) permutations is found in \( T(m) \) steps. Then a generating set for \( \text{Aut}_e(X) \) can be found in \( O(n^3d + T(n^d)) \) steps.

2. Properties of the Automorphism Group

In Section 1 we have reduced Problem 1 to the problem of determining setwise stabilizers \( H \) in permutation groups \( G \) homomorphic to \( \text{Aut}_e(X_k) \). It is not known whether there exists a polynomial time algorithm for finding setwise stabilizers in arbitrary permutation groups. Therefore, we have to derive results about structural properties of the groups \( G \) which are helpful for finding setwise stabilizers. These results are best developed introducing new concepts from Group Theory. The main result to be established in this section is that the groups \( \text{Aut}_e(X_k) \), and therefore also the groups \( G \), possess subgroup towers in which each subgroup is normal in the preceding one and is of small index. The group-theoretic consequences of this property will be explored in Section 3 and exploited in the design of a polynomial time algorithm for determining the required setwise stabilizers in Section 4.

**Definition 1**

A nontrivial group \( G \) is **simple** if \( G \) contains no proper normal subgroup, except the trivial group \( I \).

For example, the cyclic group \( C_p \) of prime order \( p \) is a simple group. The **alternating** group \( A_n \), \( n \geq 3 \), is the subgroup of \( S_n \) of index 2 consisting of all permutations in \( S_n \) which may be written as the product of an even number of transpositions. It is a standard result from Group Theory that the alternating group \( A_n \) is simple provided that \( n = 3 \) or \( n > 4 \). The alternating group \( A_4 \) is not a simple group (see also Lemma 4b below).

**Definition 2**

Let \( G \) be a finite group. A subgroup tower
I = G^{(m)} \triangleleft G^{(m-1)} \triangleleft \cdots \triangleleft G^{(1)} = G

eq

of G is called a subnormal series of G. Furthermore, if every $G^{(i+1)}$ is a proper normal subgroup of $G^{(i)}$ and the factor groups $G^{(i)}/G^{(i+1)}$ are all simple, then the series is a composition series.

In a subnormal series $G^{(i+1)} = G^{(i)}$ is permitted but not in a composition series. Note that $G^{(i)}$ need not be a normal subgroup of G, even in composition series.

It is well known that every finite group has at least one composition series: If N is a normal subgroup of G, then the subgroups K of G which contain N are in 1-1 correspondence with the subgroups K/N of G/N. As a consequence, the trivial subnormal series $I < G$ may be refined to a composition series by inserting, if necessary, additional subgroups such that the resulting factor groups are all simple. If G is a simple group, then $I < G$ is its only composition series.

The p-step central series of a p-group $G$ (cf. Chapter III, Definition 10) is a composition series of G with the additional properties that the $G^{(i)}$ are normal in G, and that the factor groups $G^{(i)}/G^{(i+1)}$ are subgroups of the center of $G/G^{(i+1)}$ and are of order p (hence are Abelian).

We will use the following two standard results from Group Theory.

**Theorem 2 (Jordan-Hölder)**

Let $I = G^{(r)} \triangleleft \cdots \triangleleft G^{(1)} = G$ and $I = H^{(s)} \triangleleft \cdots \triangleleft H^{(1)} = G$ be two composition series of G. Then $r = s$ and there is a permutation $\pi$ of $\{1, \ldots, r\}$ such that $G^{(i)}/G^{(i+1)}$ is isomorphic to $H^{(j)}/H^{(j+1)}$, where $j = \pi(i)$.

Note that the theorem is usually stated and proved in greater generality than is needed here.

**Theorem 3**

Let $H$ be a subgroup of $G$, $I = G^{(r)} \triangleleft \cdots \triangleleft G^{(1)} = G$ a subnormal series for $G$. Then there is a subnormal series $I = H^{(s)} \triangleleft \cdots \triangleleft H^{(1)} = G$ for $H$ such that each factor group $H^{(i)}/H^{(i+1)}$ is isomorphic to a subgroup of $G^{(j)}/G^{(j+1)}$ for a suitable j (depending on i).

We give several elementary consequences of the above theorems and definitions.

**Lemma 1**

Let $N < G$ where $N$ has a composition series $I = N^{(r)} \triangleleft \cdots \triangleleft N^{(1)} = N$ and $G/N$ has a composition series $I = H^{(r)} \triangleleft \cdots \triangleleft H^{(1)} = G/N$. Let $\overline{H}^{(i)}$ be the subgroup of $G$ containing $N$ whose image under the homomorphism from $G$ onto $G/N$ is $H^{(i)}$. Then $G$ has the
composition series

\[ 1 = N^{(0)} \triangleleft \cdots \triangleleft N^{(1)} = N = H^{(r)} \triangleleft H^{(r-1)} \triangleleft \cdots \triangleleft H^{(1)} = G \]

If \( G = H \times K \), then both \( H \) and \( K \) are normal subgroups of \( G \), and we have \( G/H \) isomorphic to \( K \), \( G/K \) isomorphic to \( H \). With the help of Lemma 1 we can construct a composition series for \( G \) from composition series for \( H \) and \( K \).

**Definition 3**

The group \( H \) is a section of the group \( G \) if \( H \) is the homomorphic image of a subgroup of \( G \).

That is, there is a subgroup \( G' \) of \( G \) containing a normal subgroup \( K \) such that \( G'/K \) is isomorphic to \( H \) (cf. Chapter II, Section 1.2).

**Example 1**

Consider the group \( G = \langle (1,2), (1,3,5)(2,4,6), (3,5)(4,6) \rangle = C_2 \leq S_3 \). \( G \) has order 48 and contains the subgroup \( G' = \langle (1,2), (1,3)(2,4) \rangle \) of order 8. \( G' \) contains the normal subgroup \( K = \langle (1,2)(3,4) \rangle \) of order 4 (here \( K \) is actually the center of \( G' \)), and so the factor group \( G'/K \) has order 4. One verifies easily that \( G'/K \) is isomorphic to the group \( H = \langle (a,b)(c,d), (a,c)(b,d) \rangle \), where the isomorphism is established by the following correspondence:

\[
\begin{align*}
(1,2) & \leftrightarrow [(1,2)(3,4)] \\
(a,b)(c,d) & \leftrightarrow [(1,3), (3,4)] \\
(a,c)(b,d) & \leftrightarrow [(1,4,2,3), (1,3,2,4)] \\
(a,d)(b,c) & \leftrightarrow [(1,3)(2,4), (1,4)(2,3)]
\end{align*}
\]

Therefore, \( H \) is a section of \( G \). The group \( H \) is called Klein's 4-group. \( \square \)

For each natural number \( b \) we define the class \( \Gamma_b \) consisting of those finite groups \( G \) which have a composition series in which each quotient group has order at most \( b \). Equivalently, \( G \) is in \( \Gamma_b \) if \( G \) has a composition series for which each subgroup has index at most \( b \) in the preceding group. Note that \( \Gamma_b \subset \Gamma_{b+1} \). We will prove below that \( \text{Aut}_c(X_b) \) is in \( \Gamma_b \) where \( b \) is a constant depending on the valence of the graph \( X \) only.

**Lemma 2**

A finite group \( G \) is in \( \Gamma_b \) iff every simple section of \( G \) has order at most \( b \).

**Proof** If every simple section of \( G \) has order at most \( b \), then, in particular, so do the simple sections \( G^{(i)}/G^{(i+1)} \) in a composition series of \( G \), thus \( G \in \Gamma_b \). Conversely, let \( G \in \Gamma_b \) and let \( H_1 \triangleleft H \triangleleft G \) be subgroups such that \( H/H_1 \) is nontrivial and simple.
We refine $\mathcal{I} \triangleleft H_1 \triangleleft H$ to a composition series of $H$ and note that $H/H_1$ is a composition factor. By Theorems 2 and 3 and by simplicity, $H/H_1$ is isomorphic to some factor in every composition series of $G$, thus has order at most $b$. □

**Lemma 3**

(a) If $G$ is in $\Gamma_b$, then so is every subgroup of $G$.

(b) If $G$ is in $\Gamma_b$, then so is every homomorphic image of $G$.

(c) If $N \triangleleft G$ and both $N$ and $G/N$ are in $\Gamma_b$, then so is $G$.

**Proof** (a) follows from the proof of Lemma 2. For (b), note that a homomorphic image of $G$ is isomorphic to $G/N$ for some normal subgroup $N$ of $G$. Finally, (c) follows from Lemma 1. □

We need the following examples of groups in $\Gamma_b$:

**Lemma 4**

(a) For $n > 4$, the symmetric group $S_n$ is in $\Gamma_b$, where $b = \frac{n!}{2}$.

(b) $S_4$ and $S_3$ are in $\Gamma_3$.

(c) $S_2$ is in $\Gamma_2$.

**Proof** (a) For $n > 4$, $I \triangleleft A_n \triangleleft S_n$ is a composition series of $S_n$. Since $|A_n| = \frac{n!}{2}$ and $(S_n:A_n) = 2$, $S_n$ is in $\Gamma_b$. (b) $S_4$ has the composition series $I \triangleleft M \triangleleft N \triangleleft A_4 \triangleleft S_4$. Here $M = \langle(1,2)(3,4)\rangle$, $N = \langle M, (1,3)(2,4)\rangle$, $|M| = 2$ and $|N| = 4$. Thus, the largest index in the series is 3. (c) is trivial. □

We now have all the relevant tools to establish the major result concerning the structure of the groups which Algorithm 1 determines.

**Theorem 4 (Luks)**

Let $X = (V,E)$ be a connected graph of valence $d > 3$, $e$ an edge of $X$. Then $\text{Aut}_e(X) \in \Gamma_b$, where $b = 3$ if $d$ is 4 or 5, and $b = \frac{(d-1)!}{2}$ otherwise.

**Proof** Let $X_0, \ldots, X_{n+1}$ be the subgraphs of $X$ defined in Section 1. We will show by induction that $\text{Aut}_e(X_k) \in \Gamma_b$, $0 \leq k \leq h+1$.

**Base Case:** Since $\text{Aut}_e(X_0)$ has order 2 it must be in $\Gamma_2 \subset \Gamma_b$.

**Induction Step:** Let $A = \text{Aut}_e(X_k)$, $A' = \text{Aut}_e(X_{k+1})$, and assume that $A$ is in $\Gamma_b$. Let $B$ be the subgroup consisting of all permutations of $A$ which may be extended to automorphisms in $A'$. By Lemma 3a, $B$ is in $\Gamma_b$. Let $C$ be the pointwise stabilizer of the vertices of $X_k$, and recall that $C$ is the direct product of symmetric groups of degree at most $d-1$. By Lemmata 1 and 4, $C$ is also in $\Gamma_b$. Now the factor group $A'/C$ is iso-
morphic to \( B \) and is therefore in \( \Gamma_b \) (Lemma 3b). Hence by Lemma 3c, so is \( A' = \text{Aut}_e(X_{k+1}) \).

We observe that the group \( G \) considered by Step 10 of Algorithm 1 is a homomorphic image of \( \text{Aut}_e(X_k) \). Therefore, by Lemma 3b and the proof of Theorem 4, \( G \) is in \( \Gamma_b \), where \( b \) is as in Theorem 4. It follows that Problem 1 can be solved in polynomial time provided we have a polynomial time algorithm for determining setwise stabilizers in groups in \( \Gamma_b \), where \( b \) is a constant. We design such an algorithm in the next section.

Note that \( \Gamma_2 \) is the class of all finite 2-groups. Therefore, Theorem 4 generalizes Theorem 1 of Chapter IV.

If \( G \) is a group in \( \Gamma_b \), then the order of \( G \) is only divisible by primes no larger than \( b \). This follows from Theorem 6 of Chapter III and from Lemma 2 above. However, if the largest prime dividing the order of a group \( G \) is \( p \), then it does not follow that \( G \) is in \( \Gamma_p \). For example, the Mathieu group \( M_{11} \) has order \( 7290 = 11 \cdot 5 \cdot 3^2 \cdot 2^4 \). Since \( M_{11} \) is simple, it cannot be in \( \Gamma_{11} \), yet 11 is the largest prime dividing its order.

3. Setwise Stabilizers in the Class \( \Gamma_b \)

In Section 1, we have given a basic algorithm for determining the automorphism group of a graph of fixed valence. The algorithm is not complete since we have not yet shown how to determine setwise stabilizers in the groups occurring in Step 10 of Algorithm 1. In Section 2, we have shown that the group \( \text{Aut}_e(X) \) belongs to the class of groups which have a composition series in which successive factor groups have order at most \( b \) for some constant \( b \) depending on the valence of the graph \( X \) only. We have denoted this class of groups by \( \Gamma_b \). Now we will design a polynomial time algorithm for computing setwise stabilizers in groups in \( \Gamma_b \) and we consider the following

**Problem 2**

Given a generating set \( K \subset S_n \) of a group \( G = \langle K \rangle \) which is in \( \Gamma_b \), where \( b \) is a constant, and given a subset \( Y \) of \( \{1, \ldots, n\} \). Find a generating set for \( G_Y \), the setwise stabilizer of \( Y \) in \( G \).
The algorithm to be designed is very similar to Algorithm 2 of Chapter IV. However, the class $\Gamma_3$ contains permutation groups which have a more complicated structure than $p$-groups and so we will need both further group-theoretic results about the structure of these groups as well as new algorithmic techniques to cope with the additional complications.

3.1. Outline of the Method

We give an informal outline of the setwise stabilizer algorithm to be developed. The outline is intended to convey an intuitive grasp of the techniques used by the algorithm and of the group-theoretic results which are exploited.

Recall Algorithm 2 of Chapter IV. The algorithm contains a recursive procedure for computing the setwise stabilizer $(G\pi)_Y$ of a set $Y$ in the right coset $G\pi$ of the $p$-group $G$. More precisely, given a subset $Z$ of the permutation domain setwise stabilized by $G$, the procedure computes the set $S_Y(G\pi,Z)$ of all elements in $G\pi$ which map $Z \cap Y$ into $Y$ and map $Z - Y$ into $X - Y$. This is accomplished by the following two steps:

1. If $G$ acts intransitively on $Z$ with the orbits $\Delta_1, ..., \Delta_s$, then the procedure considers successively the sets $Y \cap \Delta_1, Y \cap \Delta_2, ..., Y \cap \Delta_s$. Thus the problem is split into $s$ subproblems concerning the sets $\Delta_i$ of smaller cardinality.

2. If $G$ acts transitively on $Z$, then we find a subgroup $H$ of index $p$ in $G$ which is intransitive on $Z$. If $G = H\varphi_1 + \cdots + H\varphi_p$, then we consider $p$ subproblems concerning the cosets $H\varphi_1 \pi$ and the set $Z$, on which $H$ now acts intransitively.

The critical part of this approach is Step (2): Since $p$-groups $G$ have a rich structure of imprimitivity, one can always find a suitable subgroup $H$ of index $p$ in $G$.

Now consider the case of arbitrary permutation groups $G$. Here Step (2) runs into the following difficulties: $G$ may act imprimitively on $Z$, but the subgroup $H$ of $G$ which stabilizes each set of imprimitivity need not have small index in $G$. Worse yet, $G$ may act primitively on $Z$ (cf. Chapter III, Section 3.3). In that case one would have to choose $H = I$, the trivial group, which means that then Step (2) exhaustively searches through the elements of $G$. So we will need group-theoretic results which show us how to overcome these problems. Recall

**Definition 4**

A system $B = \{B_1, ..., B_s\}$ of imprimitivity for $G$ is called **maximal** if it contains more
than one set of imprimitivity and there is no other nontrivial system $B'$ of imprimitivity for $G$ of which $B$ is a proper refinement.

If $G$ is a primitive group, then we choose for $B$ the trivial system consisting of singletons only. With the latter convention we depart from tradition, since it endows primitive groups with a maximal system of imprimitivity, but it allows us to uniformly treat the primitive and the imprimitive case in the algorithm.

If $B$ is a maximal system of imprimitivity for $G$ and if $H$ is the setwise stabilizer of each set of imprimitivity in $B$, then it is clear that $H$ is normal in $G$ and that $G/H$ is primitive on the blocks in $B$.

Note that a permutation group does not have to possess a unique maximal system of imprimitivity as demonstrated by

**Example 2**

Consider the group $G = \langle (1,2,3)(4,5,6), (1,4)(2,5)(3,6) \rangle$ which has order 6 and is isomorphic to $S_3$, the symmetric group of degree 3. One verifies easily that

$$B_1 = \{\{1,2,3\}, \{4,5,6\}\}$$

is a maximal system of imprimitivity for $G$. However,

$$B_2 = \{\{1,4\}, \{2,5\}, \{3,6\}\}$$
is also a maximal system of imprimitivity. Therefore, there need not be a unique block size for maximal systems of imprimitivity.

In overcoming the difficulties with Step (2) the following result (Corollary 8 below) will play a central role:

Let $G < S_n$ be a primitive group in $\Gamma_b$. Then $G$ contains a Sylow $p$-subgroup $P$ of index $(G:P) \leq n^c$, where $c$ is a constant depending only on $b$.

This result will be proved later. If $G$ acts primitively on $Z$, then the theorem may be exploited as follows:

(2.1) Find a Sylow $p$-subgroup $P$ of $G$ such that $G = P\varphi_1 + \cdots + P\varphi_r$, $r \leq n^c$. Now consider the $r$ subproblems concerning the cosets $P\varphi_i\pi$, $i \leq r$, and the set $Z$ on which $P$ acts as a $p$-group.

The significance of this step is that by passing to the subgroup $P$ we lock into the setwise stabilizer algorithm for $p$-groups. Thus, for primitive groups $G$ in $\Gamma_b$ we run Algorithm 2 of Chapter IV at most $n^c$ times. Since $c$ is a constant depending only on $b$, we now have a polynomial time procedure for computing setwise stabilizers in primitive
groups in $\Gamma_b$, $b$ a constant, provided that $P$ can be found efficiently.

If $G$ acts imprimitively (but transitively) on $Z$ the situation is slightly more complex, but we will use the same general idea.

Let $G$ act transitively but imprimitively on $Z$ and let $B = \{B_1, ..., B_s\}$ be a maximal system of imprimitivity for the action of $G$ on $Z$. Then $G$ and $B$ induce a permutation group $G^*$ on the blocks of $B$. Since the system $B$ is maximal, $G^*$ is primitive. We observe that $G^*$ has degree $s$. Thus, $G^*$ must contain a Sylow $p$-subgroup $P^*$ of index at most $s^c$ in $G^*$. Corresponding to $P^*$ is a subgroup $P$ of $G$ which acts on the sets $B_i$, $1 \leq i \leq s$, as a $p$-group and contains the setwise stabilizer $H$ of each set $B_i$ as normal subgroup. (Note that $P/H$ is isomorphic to $P^*$). Here we will imitate Step 2.1, that is, we work with $P$ and those of its subgroups which contain $H$:

(2.2) Find $\{B_1, ..., B_s\}$, a maximal system of imprimitivity for the action of $G$ on $Z$.

Find $P$, a subgroup of $G$ acting as $p$-group on the blocks $B_i$, where $G = P\varphi_1 + \cdots + P\varphi_r$, $r \leq s^c < n^c$. Consider the $r$ subproblems concerning the cosets $P\varphi_i n$ and the set $Z$.

Recall that $P$ acts as $p$-group on the blocks $B_i$. So, if $P$ is transitive on $Z$, then there is a maximal system of imprimitivity for the action of $P$ on $Z$ consisting of $p$ new blocks (which are the union of certain sets $B_i$). Furthermore, the setwise stabilizer $P'$ of each of these new blocks has index $p$ in $P$. This situation repeats for $P'$ until we reach $H$, the setwise stabilizer of each set $B_i$, $1 \leq i \leq r$. We will show later that by proceeding in this fashion we ultimately obtain $O(s^2)$ subproblems involving cosets of $H$ and the individual sets $B_i$. This will again lead to a polynomial time performance.

Except for the obvious intransitive case, we have fully outlined how the problem of finding $S_Y(G\pi, Z)$ can be broken up into subproblems concerning sets of smaller cardinality. Aside from a certain amount of house keeping, data structure choices and the timing (all of which will be discussed later), it remains to explain how to determine the subgroups $P$ acting as $p$-groups on the sets of imprimitivity. This problem divides as follows: Selecting the correct prime number $p$, determining generators for a Sylow $p$-subgroup of $G^*$, and determining generators for the corresponding subgroup $P$ of $G$.

We will prove below that $p$ can be found in one of two ways: Either $s$, the degree of $G^*$, is $p^r$ for some prime number $p$ and then $p$ is the prime number to be used, or $s$ is a composite number, and then any prime $p$ may be chosen. In either case, the necessary computations can be carried out in time polynomial in $s \leq n$. 
Finding generators for \( P \) is a variant on the techniques of Chapter II and combines Algorithms 3 and 5 of that chapter. The difficulty to overcome is that we have no precise definition for \( P \) since \( G^* \) will in general contain more than one Sylow \( p \)-subgroup. Thus we lack a membership test for \( P \).

For simplicity, we first outline the technique for the case where \( G \) is primitive, i.e., \( P \) is a \( p \)-group.

Throughout the computation determining \( P \), we maintain a list \( L \) of right coset representatives for \( P \) in \( G \) and a list \( K \) of generators for a subgroup \( P' \) of \( P \). Eventually, \( P' \) will be \( P \) and \( L \) will be a complete right transversal for \( P \) in \( G \). We exploit Theorem 7c of Chapter III, which asserts that for every \( p \)-group \( P' < G \) there is a Sylow \( p \)-subgroup \( P \) of \( G \) containing \( P' \) as subgroup.

Consider an element \( \psi \) of \( G \). We test whether \( \psi \) lies in a coset with known representative \( \pi \in L \) by testing whether \( \pi\psi^{-1} \) lies in a \( p \)-group containing \( P' \). That is, we test whether \( \langle K, \pi\psi^{-1} \rangle \) is a \( p \)-group using Algorithm 3 of Chapter II by determining whether the order of \( \langle K, \pi\psi^{-1} \rangle \) is a power of \( p \). If so, then \( \psi \) and \( \pi \) are in the same right coset of a Sylow \( p \)-subgroup of \( G \) containing \( P' = \langle K, \pi\psi^{-1} \rangle \) as subgroup. In this case we add \( \pi\psi^{-1} \) as new generator to \( K \) provided that \( \langle K \rangle \) is a proper subgroup of \( \langle K, \pi\psi^{-1} \rangle \). Note that \( \pi\psi^{-1} \in \langle K \rangle \) is a special case of this test.

If \( \langle K, \pi\psi^{-1} \rangle \) is not a \( p \)-group, then there is no Sylow \( p \)-subgroup \( P \) of \( G \) containing \( K \) for which \( \psi \in P\pi \). Consequently, if this is the case for every \( \pi \in L \), then we have discovered a new coset of \( P \) and add \( \psi \) to the list \( L \).

Initially, we so process every generator of \( G \). Thereafter, maintaining the list \( L \) and a representation matrix for \( \langle K \rangle \), we process all pair products formed with entries in the representation matrix for \( \langle K \rangle \) and the list \( L \). Termination of the algorithm is obvious. It requires polynomial time since all operations involved do so and \( L \) contains at most \( n^c \) entries, \( c \) a constant. Correctness follows easily from Theorem 11 and Lemma 6 of Chapter II.

We now generalize this method to imprimitive groups \( G \). Here the trick is to obtain \( P \) rather than the Sylow \( p \)-subgroup \( P^* \) of \( G^* \), where \( G^* \) denotes the action of \( G \) on the sets of imprimitivity. Let \( H \) be the setwise stabilizer of each set of imprimitivity for \( G \). It is clear that we have a membership test for \( H \) and the pointwise stabilizers in \( H \). We proceed as above, maintaining a list \( L \) of right coset representatives for the subgroup \( P \) to be determined and maintaining a representation matrix for \( P \). In order to test whether \( \pi\psi^{-1} \) extends the known subgroup \( P' \) of \( P \) to a larger group still
acting on the sets of imprimitivity as a p-group, we must test that \( \langle P', \pi \psi^{-1} \rangle \) respects the given system of imprimitivity and that the index of the setwise stabilizer of these sets in the group is a power of p. If so, then the group induced on the blocks is a p-group. It is clear that this can be done in polynomial time.

3.2. Group-Theoretic Preliminaries

The algorithm sketched above is based on structural properties of primitive groups. These properties can be shown using completely elementary means, and we prepare the ground in this subsection by giving a miscellany of basic results from Group Theory for the benefit of the reader with little background on the subject. The selection of these results is made according to an overall proof strategy which first shows how to embed (a point stabilizer of) a primitive group \( G \) into the automorphism group of a suitable normal subgroup \( N \) of \( G \). Then properties of \( N \) and resultant properties of its automorphism group are analyzed, which in turn permit conclusions about the structure of \( G \).

If \( G \) is a primitive group, then one can always find a (not necessarily proper) normal subgroup \( N \) of \( G \) which is of one of two types: Either \( N \) is nonabelian with a trivial centralizer in \( G \). In this case \( G \) is represented by its action on \( N \) through conjugation (Proposition 3 and Corollary 1 below). Otherwise \( N \) is elementary abelian and regular. In this case \( G_x \), the stabilizer of \( x \) in \( G \), will be represented by its action on \( N \) through conjugation (Theorem 6 below).

In the first case one then exploits the fact that \( N \) will be the direct product of isomorphic nonabelian simple groups. In the second case, \( N \) may be identified with the additive group of the \( d \)-dimensional vector space over the field of integers modulo the prime \( p \).

We now give the required basic results. The first few results below relate normality and direct products of permutation groups. Note that if \( H \) and \( K \) are normal subgroups of \( G \), then so are \( H \cap K \) and \( HK \).

**Lemma 5**
Let \( H \) and \( K \) be normal subgroups of \( G \). If \( H \cap K = 1 \), then \( HK = H \times K \).
Proof Let \( \varphi \in H, \psi \in K \). Since \( H \triangleleft G \), \( \varphi^{-1}\psi^{-1}\varphi\psi = \varphi^{-1}\varphi \in H \). Furthermore, since \( K \triangleleft G \), \( \varphi^{-1}\psi^{-1}\varphi\psi = (\psi^{-1})^{-1}\psi = K \). So \( \varphi^{-1}\psi^{-1}\varphi \psi \in H \cap K \). Since \( H \cap K = 1 \), it follows that \( \varphi \) and \( \psi \) commute. Thus, \( (\varphi_1\psi_1)(\varphi_2\psi_2) = (\varphi_1\varphi_2)(\psi_1\psi_2) \). Now let \( \varphi_1\psi_1 = \varphi_2\psi_2 \), where \( \varphi_1, \varphi_2 \in H, \psi_1, \psi_2 \in K \). Since \( H \cap K = 1 \), \( \varphi_2^{-1}\varphi_1 = \psi_2\psi_1^{-1} = 1 \), i.e., the map \( \varphi\psi \rightarrow (\varphi, \psi) \) is a bijection. Hence \( HK = H \times K \).

The group \( HK \) of Lemma 5 is called the internal direct product of \( H \) and \( K \). The proof of the lemma establishes that the internal and the external direct product are isomorphic. Of course, the fact that the elements of \( H \) commute with the elements of \( K \) does not imply that either group is commutative.

Example 3

Let \( H \) be the group

\[
\{(1,2,3)(4,5,6), (1,3,2)(4,5,6), (1,4)(2,5)(3,6), (1,5)(2,6)(3,4), (1,6)(2,4)(3,5)\},
\]

and let \( K \) be

\[
\{(1,2,3)(4,5,6), (1,2,3)(4,5,6), (1,4)(2,6)(3,5), (1,5)(2,4)(3,6), (1,6)(2,5)(3,4)\}.
\]

It is easily verified that both \( H \) and \( K \) are nonabelian groups of order six, and that for every \( \pi \in H, \psi \in K \), \( \pi\psi = \psi\pi \) is true. For instance, for the permutations \( \pi = (1,4)(2,5)(3,6) \in H \) and \( \psi = (1,3,2)(4,6,5) \in K \), we have \( \pi\psi = \psi\pi = (1,6,2,4,3,5) \).

Consider \( G = \langle H, K \rangle \). Since \( \pi \in H \) commutes with \( \psi \in K \) both groups are normal in \( \langle H, K \rangle \). Therefore, every element \( \varphi \in G \) may be written as a product \( \varphi = \pi\psi \), where \( \pi \in H, \psi \in K \). Thus \( G = HK \). Finally, since \( H \cap K = 1 \), \( G = H \times K \) by Lemma 5, i.e., the factorization of \( \varphi \in G \) is unique.

Note that if \( N \) is a normal subgroup of \( H \) and \( G = H \times K \), then \( N \) is also normal in \( G \). This follows from the fact that the elements of \( H \) commute with the elements of \( K \).

Definition 5

Let \( G = G_1 \times G_2 \), \( H \) a subgroup of \( G \). The \( G_1 \)-component of \( H \) is the subgroup \( H_1 \) of \( G_1 \) consisting of all elements \( \pi_1 \in G_1 \) for which there is a \( \pi_2 \in G_2 \) such that \( \pi_1\pi_2 \in H \).

The \( G_1 \)-component is also called the projection of \( H \) into \( G_1 \). Note that \( H \cap G_1 \) is not necessarily the \( G_1 \)-component of \( H \), but \( H \cap G_1 \) is always a subgroup of the \( G_1 \)-component.

Example 4

Let \( G = \langle (1,2), (3,4) \rangle = C_2 \times C_2 \), and consider the subgroup \( H = \langle (1,2)(3,4) \rangle \) of \( G \). The \( G_1 \)-component of \( H \) is \( H_1 = \langle (1,2) \rangle \), but the subgroup \( H \cap G_1 \) is the trivial group \( 1 \).
**Proposition 1.**

Let $G = G_1 \times G_2$, and let $H$ be a subgroup of $G$. Let $H_1$ be the $G_1$-component of $H$ and let $k = |H \cap G_2|$. Then every element $\pi_1 \in H_1$ occurs in exactly $k$ elements of $H$ as the $G_1$-component.

**Proof** Let $\pi = \pi_1 \pi_2 \in H$ be a fixed element, where $\pi_1 \in G_1$ and $\pi_2 \in G_2$. Let $\varphi \in H$ be an element with the $G_1$-component $\pi_1$. Then $\pi \varphi^{-1} \in G_2$ since $\pi_1$ commutes with $\pi_2$, and so $\pi \varphi^{-1} \in H \cap G_2$. Now let $\psi \in H \cap G_2$. Clearly $\pi \psi \in H$ and $\pi \psi$ has the $G_1$-component $\pi_1$. $
$
We now give a few results which relate the structure of a group to the structure of its automorphism group in an elementary way.

Recall that conjugation with a fixed element $\pi \in G$ induces an inner automorphism of $G$ (cf. Chapter II, Subsection 1.2). In general, $G$ also has automorphisms not so obtained. Such automorphisms are called outer automorphisms of $G$. The group of all automorphisms of $G$ is denoted $\text{Aut}(G)$ and the subgroup of all inner automorphisms $\text{Inn}(G)$. Note that an abelian group has no nontrivial inner automorphisms.

**Definition 6**

Let $G, H \subseteq S_n$. The centralizer in $G$ of $H$ is the set

$$C_G(H) = \{ \pi \in G \mid (\forall \psi \in H)(\pi \psi = \psi \pi) \}$$

That is, the centralizer of $H$ in $G$ consists of all elements in $G$ which commute with every element of $H$. It is easy to show that $C_G(H)$ is always a group, even when $H$ is not.

The centralizer in $G$ of $G$ is called the center of $G$. $C_{S_n}(G)$ will be called the centralizer of $G$ without explicit reference to $S_n$, the containing symmetric group of degree equal to the degree of $G$.

**Definition 7**

Let $G, H \subseteq S_n$. The normalizer of $H$ in $G$ is the subgroup

$$N_G(H) = \{ \pi \in G \mid H^\pi = H \}$$

of $G$.

It is easily verified that $N_G(H)$ is a group even when $H$ is not. If $K < N_G(H)$, then we say that $K$ normalizes $H$ or that $H$ is $K$-invariant. Note that $K$ does not have to
contain \( H \) in this case.

We will call \( N_{S_n}(H) \) the \textit{normalizer} of \( H \) without explicit reference to \( S_n \), the containing symmetric group of degree equal to the degree of \( G \). Note that the centralizer of \( H \) in \( G \) is always a normal subgroup of the normalizer of \( H \) in \( G \).

\textbf{Proposition 2}

\( \text{Inn}(G) \) is a normal subgroup of \( \text{Aut}(G) \).

\textbf{Proof} Let \( \alpha \in \text{Aut}(G) \) be an automorphism of \( G \), \( \gamma \in \text{Inn}(G) \) an inner automorphism obtained by conjugation with \( \pi \in G \). Let \( \psi \) be any element of \( G \). Then

\[ \psi^{(\alpha^{-1}\gamma)} = (\pi^{-1}\psi\alpha^{-1}\pi)^{\alpha} = (\pi^{-1})^{\alpha}\psi^{\alpha} = \varphi^{-1}\psi, \]

where \( \pi^{\alpha} = \varphi \). ■

\textbf{Lemma 6}

Let \( G = G_1 \times G_2 \). Then \( \text{Inn}(G) \cong \text{Inn}(G_1) \times \text{Inn}(G_2) \).

\textbf{Proof} Let \( \pi = \pi_1\pi_2 \) and \( \psi = \psi_1\psi_2 \) be elements of \( G \), where \( \pi_1, \psi_1 \in G_1, \pi_2, \psi_2 \in G_2 \). Since the elements of \( G_1 \) commute with the elements of \( G_2 \), \( \pi^\psi = \pi_1^{\psi_1}\pi_2^{\psi_2} \), so \( \text{Inn}(G) \) is isomorphic to \( \text{Inn}(G_1) \times \text{Inn}(G_2) \). ■

\textbf{Proposition 3}

Let \( N \) be normal in \( G \). Then \( \text{Inn}(G) \) acts faithfully on the elements of \( N \) iff \( C_G(N) \) is trivial.

\textbf{Proof} Let \( \varphi, \psi \in G \), where \( \varphi \neq \psi \). \( \text{Inn}(G) \) acts faithfully on \( N \) iff there is a \( \pi \in N \) such that \( \pi^{\varphi\psi^{-1}} \neq \pi \). Now \( \pi^{\varphi\psi^{-1}} = \pi \) for all \( \pi \in N \) iff \( \varphi\psi^{-1} \) is in the centralizer \( C_G(N) \) of \( N \) in \( G \), hence the conclusion follows. ■

An immediate corollary of Proposition 3 is

\textbf{Corollary 1}

\( \text{Inn}(G) \) is isomorphic to \( G \) iff \( G \) has a trivial center.

If \( G \) is a primitive group with no abelian normal subgroup, then the above results can be exploited for finding a normal subgroup \( N \) of \( G \) such that \( G \) is isomorphic to a subgroup of \( \text{Aut}(N) \).

Next, we give some results which concern specific means of representing abstract groups as transitive permutation groups. These results will be needed when studying certain nonabelian normal subgroups of primitive groups.
DEFINITION 8
Let $G$ be a finite group. The right regular representation of $G$ is a permutation group $G^* < \text{Sym}(G)$ with $G$ as its permutation domain, such that $g \in G$ corresponds to the permutation $g^* \in \text{Sym}(G)$ which maps $h \in G$ to $h \cdot g \in G$. The left regular representation of $G$ is a permutation group $^*G < \text{Sym}(G)$ with $G$ as its permutation domain, where $g \in G$ corresponds to the permutation $^g \in \text{Sym}(G)$ which maps $h \in G$ to $g^{-1} \cdot h \in G$.

It is easy to verify that both $G^*$ and $^*G$ are permutation groups isomorphic to $G$. Furthermore, both groups are regular (cf. Definition 9 below). Note that the degree of these permutation representations of $G$ is equal to the order of $G$.

EXAMPLE 5
In Example 3 above, $H$ is the right regular and $K$ the left regular representation of $S_3$ with the following identification of its elements:

1 $\leftrightarrow ()$
2 $\leftrightarrow (a,b,c)$
3 $\leftrightarrow (a,c,b)$
4 $\leftrightarrow (a,b)$
5 $\leftrightarrow (b,c)$
6 $\leftrightarrow (a,c)$

DEFINITION 9
A permutation group $G$ is semiregular if $G_x = 1$ for every point $x$ in the permutation domain. If $G$ is semiregular and transitive, then $G$ is regular.

The following lemma explains Definition 9 above:

LEMMA 7
Let $G < S_n$ be a regular group. Then $G$ is the right regular (left regular) representation of a group $H$ of order $n$.

Proof Let $H = \{1, \ldots, n\}$, and define $i \cdot j = k$ iff, for some $\pi \in G$, $1^n = j$ and $i^n = k$. Since $G$ is regular, this defines a map from $H \times H$ onto $H$. Furthermore, the bijection $\kappa$ from $G$ onto $H$ which maps $\pi$ to $j$ iff $1^n = j$ satisfies $\pi^\kappa = (\pi \kappa)^\kappa$. Therefore, $H$ is a group and is isomorphic to $G$. Now it is clear that the right regular representation $H^*$ of $H$ is just $G$. Similarly one proves that $G$ is the left regular representation of a group $H'$ of order $n$.  

THEOREM 5

If $G < S_n$ is a transitive permutation group, then $C_{S_n}(G)$ is a semiregular group.

Proof Let $H = C_{S_n}(G)$, where $G$ is transitive, and let $\psi \in H_x$ be any element of the stabilizer of $x$ in $H$. For an arbitrary point $y \neq x$ in the permutation domain let $\pi$ be an element of $G$ such that $x^\pi = y$. Since $G$ is transitive, such an element $\pi$ exists. Since $\psi$ is in the centralizer of $G$, $\pi^{-1}\psi\pi = \psi$. Consequently, $y^\psi = y^{\pi^{-1}\psi\pi} = x^{\psi\pi} = x^\pi = y$. It follows that $\psi$ is the identity permutation, i.e., $H_x = 1$. 

Of course, if $G, H < S_n$, then $C_{H}(G)$ is also a semiregular group, since $C_{H}(G)$ is obtained by intersecting the centralizer (in $S_n$) of $G$ with $H$.

PROPOSITION 4

Let $G < S_n$ be a regular group. Then $C_{S_n}(G)$ is isomorphic to $G$.

Proof Let $G' = C_{S_n}(G)$. Since $G$ is transitive, $G'$ is semiregular. By Theorem 3 of Chapter II, therefore, the order of $G'$ divides $n$. Now let $H$ be a group of which $G$ is the right regular representation. Consider $G_1 < S_n$, the left regular representation of $H$. Since the group operation of $H$ is associative, $G_1$ centralizes $G$, thus $G_1 < G'$. Since the order of $G_1$ is $n$, $G_1 = G'$. Therefore $G'$ is isomorphic to $G$.

If $G^*$ is the right regular representation of an abelian group, then it is a subgroup of its own centralizer. Thus, for an abelian group $G$, $G^*$ and $G^*$ are the same permutation group.

PROPOSITION 5

Let $G_1$ and $G_2$ be the left and the right regular representation of a group $H$ with trivial center. Then $G_1G_2 = G_1 \times G_2$. Furthermore, if $h \in H$, then the $G_1$-component and the $G_2$-component of the stabilizer $G_h$ are both isomorphic to $H$.

Proof If $G_1 \cap G_2 \neq 1$, then there are $h_1, h_2 \in H$ such that, for all $g \in H$, $h_1^{-1}g = gh_2$. This is true in particular for the identity $e$ of $G$, hence $h_1 = h_2^{-1}$. But $h_2g = gh_2$ holds for all $g \in H$ iff $h_2 \in C_H(H)$. So, by Lemma 5 and Proposition 4, $G_1G_2 = G_1 \times G_2$.

Now let $h$ be a fixed element of $H$, and consider the elements $k \in H$ and $k^h \in H$. Since $k^{-1}hk^h = h$, it follows that $g = *k(k^h)^* \in G_h$. Conversely, if $g = *k(k^h)^* \in G_h$, then $k^{-1}hk' = h$, i.e., $k' = k^h$. Hence the $G_1$-component of $G_h$ is $^*H$ and the $G_2$-component of $G_2$ is $(^h)^*$. 

We now give a result which allows one to represent the stabilizer $G_2$ in the automorphism group of a regular normal subgroup $N$ of $G$. In contrast to the method of
Proposition 3 and Corollary 1 above, N need not have a trivial centralizer.

**Theorem 6**

Let N be a regular normal subgroup of \( G \leq \text{Sym}(X) \), and let A be the group of automorphisms of N induced by conjugation with elements of \( G_x \), the stabilizer of x in G. Then \( G_x \) as permutation group on \( X - \{x\} \) is isomorphic to A as permutation group on \( N - \{(), x\} \).

**Proof** Since N is regular, the correspondence between \( y \in X - \{x\} \) and \( \pi \in N - \{(), x\} \), where \( x^\pi = y \), is a bijection. We need to show that if \( \varphi \in G_x \), \( y^\varphi = z \) and \( y \neq x \), then \( \pi^\varphi = \psi \) where \( x^\pi = y \) and \( x^\psi = z \).

Now \( x^{\varphi^{-1}\pi} = x^{\pi\varphi} = y^\varphi = z \). By normality, \( \pi^\varphi = \chi \in N \). Since \( x^\varphi = z \) and since N is regular, therefore, \( \chi = \psi \).

### 3.3. The Socle of Primitive Groups

We have indicated above that a proof of the existence of large Sylow p-subgroups in primitive groups G can be argued by embedding the group G or a point stabilizer \( G_x \) into the automorphism group of a suitable normal subgroup N of G, followed by exploiting special properties of Aut(N). We now develop the first part of this argument and investigate specifically the normal subgroup \( S(G) \) generated by all minimal normal subgroups of G. This subgroup is called the socle of G and has a number of important properties which we prove below.

The main result of this section is Theorem 8 below which states that a primitive group G has a socle which is the direct product of isomorphic simple groups. As a consequence of this result, the proof of the main theorem about primitive groups reduces to the consideration of just two cases:

1. G is primitive and its socle is the direct product of isomorphic nonabelian simple groups, and
2. G is primitive and its socle is the direct product of isomorphic abelian simple groups (i.e., G has an elementary abelian socle).

We also give some structural results concerning the automorphism group of direct products of isomorphic simple groups.

**Definition 10**

A subgroup \( H \) of G is **characteristic** in G if every automorphism of G setwise stabilizes H.
That is, $H$ is characteristic in $G$ if it is an invariant subgroup under all automorphisms of $G$. If $H$ is characteristic in $G$, then it is also normal in $G$ since normality means invariance under inner automorphisms. However, a normal subgroup of $G$ need not be characteristic:

**Example 6**

Consider $G = \langle (1,2), (3,4) \rangle = C_2 \times C_2$. The subgroup $K = \langle (1,2) \rangle$ is normal in $G$. $G$ has an outer automorphism $\alpha$ obtained by conjugation with $(1,4)(2,3)$, a permutation which is not in $G$. Since $K^\alpha$ is not $K$, $K$ cannot be characteristic in $G$. 

**Definition 11**

A group $G$ is **characteristically simple** if $G$ contains no proper characteristic subgroup except $I$.

A characteristically simple group need not be simple:

**Example 7**

Consider the group $G$ of Example 6. $G$ is abelian and has three nontrivial normal subgroups: $K_1 = \langle (1,2) \rangle$, $K_2 = \langle (3,4) \rangle$, and $K_3 = \langle (1,2)(3,4) \rangle$. In Example 6, we demonstrated that $K_1$ and $K_2$ are not characteristic in $G$. To see that $K_3$ is not characteristic, consider the automorphism $\beta$ which fixes the elements $(1)$ and $(3,4)$ of $G$ and exchanges the element $(1,2)$ with $(1,2)(3,4)$. Here $K_3^\beta = K_1$, thus $K_3$ is not characteristic. Consequently, $G$ is characteristically simple, but it is evidently not a simple group. 

**Definition 12**

A normal subgroup $F \neq I$ of $G$ is **minimal** if no proper subgroup of $F$ (except $I$) is normal in $G$. If $G$ is a simple group, then $G$ is the only minimal normal subgroup of itself.

Note that a minimal normal subgroup $F$ of $G$ need not be a simple group. However, if $F$ has a proper normal subgroup $N$, then $N$ is not normal in $G$.

**Proposition 6**

If $F$ is a minimal normal subgroup of $G$, then $F$ is characteristically simple.

**Proof** If $H < F$ is a nontrivial proper characteristic subgroup of $F$, then $H$ is normal in $G$, a contradiction to the minimality of $F$. 

**Definition 13**

Let $F_1, ..., F_r$ be the minimal normal subgroups of the group $G$. The subgroup $S(G) = F_1F_2 \cdots F_r$ of $G$ is the **socle** of $G$.

That is, the socle of $G$ is the subgroup generated by the minimal normal subgroups of $G$. 
**Proposition 7**

$S(G)$ is a characteristic subgroup of $G$.

**Proof** If $F$ is a minimal normal subgroup of $G$, $\alpha$ any automorphism of $G$, then $F^\alpha$ is again a minimal normal subgroup of $G$. $\blacksquare$

**Corollary 2**

If $F$ is a minimal normal subgroup of $G$, then $S(F) = F$.

**Proof** By Proposition 7, the socle $S(F)$ of $F$ is characteristic in $F$. By Proposition 6, $F$ is characteristically simple. By definition, $S(F) \neq I$, therefore, $S(F) = F$. $\blacksquare$

We now prove the first major result about the structure of $S(G)$:

**Theorem 7**

The socle $S(G)$ of $G$ is the direct product of certain minimal normal subgroups of $G$.

**Proof** Let $F_1, ..., F_r$ be the minimal normal subgroups of $G$. Let $H_1 = F_1$, and assume inductively that $H_j = F_1 \times F_2 \times \cdots \times F_j$, where the minimal normal subgroups of $G$ have been enumerated suitably. Let $F$ be any minimal normal subgroup of $G$ which is not contained in $H_j$. Then $N = H_j \cap F$ is normal in $G$. If $N \neq I$ and $N \neq F$, then $N$ is a proper subgroup of $F$, contradicting the minimality of $F$. Thus, either $F < H_j$ or $F \cap H_j = I$. In the latter case, let $H_{j+1} = H_j F = H_j X F$. Since $H_j < S(G)$, the theorem follows. $\blacksquare$

We apply the theorem to the minimal normal subgroups of the group $G$. Now the following is easy:

**Corollary 3**

If $F$ is a minimal normal subgroup of $G$, then $F$ is the direct product of isomorphic simple groups.

**Proof** By Corollary 2 and Theorem 7, $F = N_1 \times \cdots \times N_k$, where the $N_i$ are minimal normal subgroups of $F$. If $N_i$ contained a nontrivial normal subgroup $N'$, then $N'$ would also be normal in $F$ contradicting the minimality of $N_i$. Each direct factor $N_i$ is therefore a simple group. Consider the subgroup $M$ of $F$ generated by all subgroups $N$ such that, for some automorphism $\alpha$ of $F$, $N_1^\alpha = N$. Then $M \neq I$ is a characteristic subgroup of $F$. By Proposition 6, therefore, $M = F$, i.e., all direct factors of $F$ are isomorphic simple groups. $\blacksquare$

As a consequence, the socle of any finite group $G$ is a direct product of simple groups. In general, we cannot conclude that these simple groups are isomorphic since we have no assurance that distinct minimal normal subgroups of $G$ are isomorphic. In the case of primitive groups $G$, however, we can show this and obtain
stronger results which we now give.

Recall Theorem 11 of Chapter III. It says that the transitive permutation group $G$ is primitive iff the stabilizer $G_x$ of every point $x$ in the permutation domain is a maximal subgroup of $G$. That is, if $G_x < H < G$, then either $H = G_x$ or $H = G$. We exploit this theorem to prove

**Proposition 8**

If $K$ is a nontrivial normal subgroup of the primitive permutation group $G$, then $K$ is transitive.

**Proof** Let $G$ be primitive (hence transitive) and assume that $K \neq I$ is a nontrivial normal subgroup of $G$. If $K$ is not transitive, then we can find an orbit $x^K = \Delta$ of some point $x$ in $K$ which is neither $\{x\}$ nor the entire permutation domain. We consider the subgroup $H = G_xK$ of $G$. Since every element of $H$ can be written as $\pi \psi$, where $\pi \in G_x$ and $\psi \in K$, the orbit of $x$ in $H$ is $\Delta$. Since $\Delta$ has length greater than 1, $G_x$ is a proper subgroup of $H$. Since $\Delta$ is a proper subset of the permutation domain, $H$ is not transitive, hence it is a proper subgroup of $G$. Therefore, $G_x$ is not a maximal subgroup of $G$ contradicting that $G$ is primitive. Hence $K$ must be transitive. 

We wish to prove that the socle $S(G)$ of the primitive permutation group $G$, when factored into minimal normal subgroups of $G$, has at most two direct factors and that these factors are isomorphic. To do so, we will consider centralizers of minimal normal subgroups since in a direct product the direct factors centralize each other.

**Lemma 8**

Let $F$ be a minimal normal subgroup of the primitive group $G$. If $C_G(F)$ is not trivial, then $C_G(F)$ is a regular group. Furthermore, $C_G(F)$ is also a minimal normal subgroup of $G$.

**Proof** Let $H = C_G(F)$. Since $F$ is transitive, $H$ is semiregular. If $\pi$ is any element of $G$, then $H^\pi$ centralizes $F^\pi$. Since $F^\pi = F$, it follows that $H$ is normal in $G$. Hence, by Proposition 8, $H$ is regular. Next, since $H$ is regular and by Theorem 3 of Chapter II, its order is equal to its degree. Therefore, $H$ cannot properly contain transitive subgroups, and so, again by Proposition 8, $H$ is a minimal normal subgroup.

In conjunction with Proposition 4 we now have established all the tools needed to prove the main result of this section:
Theorem 8

Let $G$ be a primitive permutation group, $S(G) = F_1 \times \cdots \times F_k$ a direct factorization of the socle of $G$ into minimal normal subgroups of $G$. Then $k \leq 2$. Furthermore, if $k = 2$, then $F_1$ and $F_2$ are isomorphic groups.

Proof. If $k > 1$, let $S(G) = F_1 \times H$, where $H = F_2 \times \cdots \times F_k$ and the $F_i$ are minimal normal subgroups of $G$. Since $H$ centralizes $F_1$, $H$ is a subgroup of $H' = C_G(H)$. By Lemma 8, therefore, $H = H' = F_2$.

Now assume that $S(G) = F_1 \times F_2$. Since $F_1$ and $F_2$ centralize each other and are transitive, both are regular groups. By Proposition 4, $F_1$ and $F_2$ are isomorphic. ■

As a corollary of Theorem 8 we now know that the socle of a primitive permutation group is the direct product of isomorphic simple groups. In particular, either $S(G) = F$ and $F$ is the only minimal normal subgroup of $G$, or $S(G) = F_1 \times F_2$ and $F_1$ and $F_2$ are the left and the right regular representation of a nonabelian group $H$, respectively, where $H$ is also a direct product of isomorphic simple groups.

We conclude this subsection with some results concerning direct products of isomorphic simple groups and the structure of their automorphism group. Let $G = T_1 \times T_2 \times \cdots \times T_m$, where the $T_i$ are isomorphic simple groups. We distinguish the case where the $T_i$ are abelian from the case where the $T_i$ are nonabelian, and we begin with the abelian case.

Recall that an abelian group is simple iff it is cyclic of prime order. Hence in the abelian case we must discuss direct products of cyclic groups each of order $p$, where $p$ is prime.

Definition 14

A group $G$ is elementary abelian if it is the direct product of cyclic groups $C_p$ of order a fixed prime $p$.

It follows that an elementary abelian group $G$ has order $p^m$, where $p$ is the order and $m$ the number of its direct factors. We first show how to identify $G$ with a vector space.

It is clear that we can find elements $\pi_1, \ldots, \pi_m \in G$ of order $p$ such that $G = \langle \pi_1 \rangle \times \cdots \times \langle \pi_m \rangle$. Then every element $\varphi \in G$ can be expressed as a unique product

$$\varphi = \pi_1^{k_1} \pi_2^{k_2} \cdots \pi_m^{k_m},$$
where 0 ≤ k_i < p. The correspondence of \( \varphi \) to the exponent vector \((k_1, ..., k_m)\) is now easily seen to be an isomorphism from \( G \) onto the additive group of the \( m \)-dimensional vector space \( V \) over the field of integers modulo \( p \).

We consider \( \text{Aut}(G) \), the group of all automorphisms of the elementary abelian group \( G \) of order \( p^m \). Clearly, every \( \alpha \in \text{Aut}(G) \) is in 1-1 correspondence with a nonsingular linear transformation of \( V \), and this correspondence defines an isomorphism.

**Definition 15**

The group of all nonsingular linear transformations of the \( m \)-dimensional vector space \( V \) over the field of integers modulo \( p \), \( p \) a prime, is called the general linear group of \( V \) and is denoted \( \text{GL}(m,p) \).

We will determine the order of \( \text{GL}(m,p) \) and thus determine the order of \( \text{Aut}(G) \) where \( G \) is an elementary abelian group of order \( p^m \).

**Proposition 9**

The order of \( \text{GL}(m,p) \) is \( \prod_{i=0}^{m-1} (p^m - p^i) \).

**Proof** Let \( \{v_1, ..., v_m\} \) be a basis of \( V \), the \( m \)-dimensional vector space over the field of integers modulo \( p \). Every nonsingular linear transformation \( A \) of \( V \) is completely determined by the image \( \{v_1^A, ..., v_m^A\} \) of the basis vectors, and this image must consist of linearly independent vectors. Let \( \langle u_1, ..., u_j \rangle \) denote the vector space spanned by the linearly independent vectors \( u_1, ..., u_j \), and observe that this space has cardinality \( p^j \). Because of nonsingularity, the image vectors \( \{v_i^A\} \) must satisfy

- \( v_i^A \neq \bar{0} \) (the zero vector of \( V \)),
- \( v_2^A \not\in \langle v_1^A \rangle \),
- \( ... \)
- \( v_m^A \not\in \langle v_1^A, ..., v_{m-1}^A \rangle \).

Therefore, \( |\text{GL}(m,p)| = (p^m - 1)(p^m - p) \cdots (p^m - p^{m-1}) \).

We now analyze groups \( G \) which are the direct product of isomorphic nonabelian simple groups.

**Proposition 10**

Let \( G = T_1 \times T_2 \times \cdots \times T_m \), where the groups \( T_i \) are isomorphic nonabelian simple groups. Then the groups \( N = \prod_{i \in B} T_i \), where \( B \subseteq \{1, ..., m\} \), are the only normal subgroups of \( G \).
Proof Let $N$ be a normal subgroup of $G$, $\pi = \pi_1\pi_2 \cdots \pi_m$ an element of $N$ whose $T_i$-component $\pi_i$ is not the identity. We will show that $T_i$ is then a subgroup of $N$, from which the conclusion follows.

Since $T_i$ is nonabelian and simple, it has a trivial center, hence there is some $\psi_i \in T_i$ which does not commute with $\pi_i$. We form the commutator $\psi_i^{-1}\pi_i^{-1}\psi_i\pi_i = \varphi_i$. Since $\psi_i$ and $\pi_i$ do not commute, $\varphi_i \neq ()$. Clearly $\varphi_i \in T_i$. Since $\varphi_i = (\pi_i^{-1})^{\psi_i}\pi_i$ and since $N$ is normal in $G$, $\varphi_i \in N \cap T_i$. Since $N \cap T_i$ is normal in $T_i$ and since $T_i$ is simple, it follows that $N \cap T_i = T_i$, i.e., $T_i < N$. $\blacksquare$

In particular, Proposition 10 implies that the groups $T_i$ are the only minimal normal subgroups of $G$. Hence every minimal normal subgroup of $G$ occurs as direct factor. Note that this is not true for direct products of isomorphic abelian simple groups.

**Corollary 4**

Let $G = T_1 \times T_2 \times \cdots \times T_m$, where the $T_i$ are isomorphic nonabelian simple groups. Then $\text{Aut}(G) \cong \text{Aut}(T_i) \cap S_m$.

**Proof** Since the $T_i$ are the only minimal normal subgroups of $G$, an automorphism $\alpha$ of $G$ must map $T_i$ onto $T_j$, $1 \leq i, j \leq m$. Hence $\text{Aut}(G)$ is isomorphic to a subgroup of $\text{Aut}(T_i) \cap S_m$. Conversely, since the $T_i$ are isomorphic, $\alpha \in \text{Aut}(T_i) \cap S_m$ induces an automorphism of $G$. $\blacksquare$

### 3.4. Primitive Groups with Nonabelian Socle

Having established that the socle of a primitive group is the direct product of isomorphic simple groups, we now argue that a primitive group in $\Gamma_b$ with nonabelian socle cannot be of very large order. The main result to be shown is Corollary 5 below which states that if $G$ is a primitive group in $\Gamma_b$ of degree $n$, and if $G$ has a nonabelian socle, then the order of $G$ is at most $n^c$, where $c$ is a constant which depends only on $b$.

This result is established as follows: Let $G$ be a primitive permutation group of degree $n$ with the nonabelian socle $S(G)$. We first show that $G$ is isomorphic to a subgroup of $\text{Aut}(S(G))$. Since $S(G) = T_1 \times \cdots \times T_m$, where the $T_i$ are isomorphic nonabelian simple groups, this shows that $G$ is a subgroup of $\text{Aut}(T_i) \cap S_m$. As a consequence, we will be able to prove that the order of such primitive groups in $\Gamma_b$ is at most $a^m$, where $a$ is a constant.
Next, we will consider the stabilizer of \( x \) in the socle \( S(G) \). Since \( S(G) \) is transitive, the index of \( S(G)_x \) in \( S(G) \) is \( n \). Since \( G \) is primitive, \( S(G)_x \) will inherit a certain maximality property from the maximality of \( G_x \) in \( G \). This property is used to prove that \( S(G)_x \) is the direct product of sections of the simple factors of \( S(G) \), and this leads to a correlation of \( n \), the degree of \( G \), and \( m \), the number of direct factors of \( S(G) \). As a final consequence, we then can prove that primitive groups in \( \Gamma_b \) with nonabelian socle are of order polynomial in their degree (assuming \( b \) is a constant).

**Proposition 11**

If \( G \) is primitive with nonabelian socle \( S(G) \), then \( G \) is isomorphic to a subgroup of \( \text{Aut}(S(G)) \).

**Proof** Let \( F \) be a minimal normal subgroup of \( G \). Since \( F \) is nonabelian, by the proof of Theorem 8, either \( C_G(F) = 1 \) and then \( S(G) = F \), or \( C_G(F) = F' \) and then \( S(G) = F \times F' \). For \( S(G) = F \), clearly \( C_G(S(G)) = 1 \). For \( S(G) = F \times F' \), \( C_G(S(G)) = F' \cap F = 1 \). Hence, by Proposition 3, \( G \) is isomorphic to a subgroup of \( \text{Aut}(S(G)) \).

Before exploring the consequences of this proposition for primitive groups in \( \Gamma_b \), we derive structural results about the stabilizer \( S(G)_x \) of \( x \) in the socle \( S(G) \). The following theorem is a crucial link in the argument:

**Theorem 9**

Let \( G \) be primitive with the nonabelian socle \( S(G) = T_1 \times \cdots \times T_m \), where the \( T_i \) are simple groups, and let \( S(G)_x \) be the stabilizer of \( x \) in \( S(G) \). If \( R_i \) is the \( T_i \)-component of \( S(G)_x \), then the subgroups \( R_i \) are isomorphic, \( 1 \leq i \leq m \).

**Proof** Since \( G \) is primitive, \( G_x \) is maximal and \( S(G) \) is transitive. Hence \( G = G_x S(G) \). After suitably enumerating the direct factors of \( S(G) \), let \( T_1, \ldots, T_k \), \( k \geq 1 \), be those factors such that the \( T_i \)-component of \( S(G)_x \), \( 1 \leq i \leq k \), is isomorphic to \( R_1 \). Consider \( F_1 = T_1 \times \cdots \times T_k \), and let \( \pi \in G_x \). \( S(G) \triangleleft G \) and by Proposition 10, \( F_1^\pi = T_1^\pi \times \cdots \times T_k^\pi \), where \( T_j^\pi = T_j \) and \( i_j \in \{1, \ldots, m\} \). Since \( S(G)_x = S(G) \cap G_x \), \( G_x \) normalizes \( S(G)_x \). Hence the subgroups \( R_i \) of \( T_i \), \( 1 \leq i \leq k \) remain setwise stable under conjugation by elements of \( G_x \), i.e., \( G_x \) normalizes \( F_1 \). Moreover, \( F_1 \triangleleft S(G) \). Since every element of \( G \) can be factored \( \pi \psi \) where \( \pi \in G_x \) and \( \psi \in S(G) \), it follows that \( F_1 \) is normal in \( G \).

Now if \( k < m \), then we know that \( S(G) = F_1 \times F_2 \), \( k = \frac{m}{2} \), and \( F_1 \) and \( F_2 \) are the left regular and the right regular representation of a group \( H \), respectively, where \( H \) is the direct product of \( k \) isomorphic nonabelian simple groups. By Proposition 5, the \( F_1 \)-
component and the \( F_2 \)-component of \( S(G)_x \) are isomorphic to \( H \). Hence, if \( k < m \), then \( R_i = T_i \), contradicting that not all \( T_i \)-components of \( S(G)_x \) are isomorphic. Hence \( k = m \).

As a consequence of Theorem 9, we need to investigate the following two cases: (1) Either each \( T_i \)-component of \( S(G)_x \) is \( T_i \), or (2), each \( T_i \)-component is a proper subgroup \( R_i \) of \( T_i \) and is isomorphic to \( R_i \). We consider the first case in Lemma 10 and the second in Lemma 11 below.

**Definition 16**

Let \( G = G_1 \times G_2 \times \cdots \times G_m \) be the direct product of isomorphic groups \( G_i \), and let \( H \) be a subgroup of \( G \). Then \( H \) is a **full diagonal subgroup** of \( G \) if every \( G_i \)-component of \( H \) is \( G_i \) and the order of \( H \) is \( |G_1| \).

Intuitively, full diagonal subgroups are obtained from \( G_1 \) by forming

\[
H = \{ \pi_1 \pi_2 \cdots \pi_m | \pi_i \in G_i, \pi_i = \pi_i^{a_i} \},
\]

where \( a_i \) is a fixed isomorphism from \( G_1 \) onto \( G_i \). For instance, the group \( K_3 \) of Example 7 is a full diagonal subgroup of the group \( G \) of Example 6.

**Lemma 9**

Let \( G = T_1 \times \cdots \times T_m \), where the \( T_i \) are isomorphic nonabelian simple groups. If \( D \) is a full diagonal subgroup of \( G \), then \( N_G(D) = D \).

**Proof**

Let \( D = \{ \pi = \pi_1^{a_1} \cdots \pi_m^{a_m} | \pi_i \in T_i, \pi_i^{a_i} \in T_1 \} \). Clearly \( D < N_G(D) \). Let \( \overline{\psi} = \psi \psi_2 \cdots \psi_m \in G-D \) where \( \psi \in T_1, \psi_i \in T_i \). Since \( \overline{\psi} \notin D \), \( \psi_i \neq \psi_i^{a_i} \) for some \( i \). Consider \( \overline{\phi} = \overline{\psi} \). The \( T_i \)-component of \( \overline{\phi} \) is \( \varphi_i = \pi_i^{\psi_i} = (\pi_i^{a_i})^{\psi_i} \). If \( \overline{\psi} \in N_G(D) \), it follows that \( \pi_i^{\psi} \in D \) for all \( \pi_i \). Hence

\[
(\pi_i^{a_i})^{\psi_i} \varphi_i = \varphi_i = (\psi_i^{a_i})^{-1} \pi_i^{a_i} \psi_i^{a_i},
\]

since the \( T_i \)-component of \( \overline{\phi} \) is \( \pi_i^{\psi} \). With \( \chi = \psi_i(\psi_i^{a_i})^{-1} \neq () \), therefore, it follows that \( \chi^{-1} \pi_i^{a_i} \chi = \pi_i^{a_i} \) for all \( \pi_i \in T_1 \). Since \( a_i \) is an isomorphism and since \( \chi \in T_i \), it follows that \( \chi \) is in the center of \( T_i \). Since \( T_i \) is nonabelian and simple, this is not possible, hence \( \overline{\psi} \) cannot normalize \( D \). 

**Lemma 10 (Scott)**

Let \( H \neq I \) be a subgroup of \( G = T_1 \times \cdots \times T_m \), where the \( T_i \) are isomorphic nonabelian simple groups. If the \( T_i \)-component of \( H \) is \( T_i \), \( 1 \leq i \leq m \), then there is a partition \( P = \{ B_1, \ldots, B_s \} \) of the set \( \{ 1, \ldots, m \} \), such that \( H = D_1 \times D_2 \times \cdots \times D_s \) and \( D_i \) is a full
diagonal subgroup of the direct product of the \( T_j \), where \( j \in B_i \).

**Proof**  Since \( H \neq \mathbb{I} \), there is a minimal subset \( B \) of \( \{1, \ldots, m\} \), such that \( D = H \cap \prod_{j \in B} T_j \neq \mathbb{I} \). Clearly \( D < H \), so the \( T_i \)-component of \( D \) is normal in the \( T_i \)-component of \( H \). If the \( T_i \)-component of \( D \) were \( \mathbb{I} \), then \( D' = H \cap \prod_{j \in B'} T_j \neq \mathbb{I} \), where \( B' = B - \{i\} \), thus contradicting the minimality of \( B \). Therefore, the \( T_i \)-component of \( D \) is also \( T_i \) for every \( i \in B \). By Proposition 1, the number of elements in \( D \) with a given \( T_i \)-component is \( i \), hence \( D \) is a full diagonal subgroup of \( G_1 = \prod_{j \in B} T_j \).

Next, let \( H_1 \) be the \( G_1 \)-component of \( H \). Clearly \( D < H_1 \). By Lemma 9, \( N_{G_1}(D) = D \), hence \( H_1 = D \). Therefore, \( H = D \times D' \), where \( D' = H \cap \prod_{j \in B} T_j \). Now the lemma follows by induction on \( m \). 

**Lemma 11**

Let \( G \) be a primitive permutation group with the socle \( S(G) = T_1 \times \cdots \times T_m \), where the \( T_i \) are nonabelian simple groups, and assume that the \( T_i \)-component of \( S(G)_x \) is \( R_i \), a proper subgroup of \( T_i \). Then \( S(G)_x = R_1 \times R_2 \times \cdots \times R_m \), where \( R_i \) is a proper subgroup of \( T_i \) isomorphic to \( R_1 \), \( 2 \leq i \leq m \).

**Proof**  Let \( R_i \) be the \( T_i \)-component of \( S(G)_x \), the stabilizer of \( x \) in \( S(G) \), and note that \( S(G)_x < R_1 \times R_2 \times \cdots \times R_m \). By Theorem 9, the groups \( R_i \) are all isomorphic to \( R_1 \). Furthermore, \( S(G)_x \) is invariant under conjugation with elements of \( G_x \). If there is a proper subgroup \( N \) of \( S(G) \) properly containing \( S(G)_x \) which is also \( G_x \)-invariant, then \( N \) cannot be transitive and so the group \( G_xN \) properly contains \( G_x \) and is properly contained in \( G \), contradicting that \( G \) is primitive. Therefore, \( S(G)_x \) is a maximal \( G_x \)-invariant subgroup of \( S(G) \).

Now \( R_1 \) is a \( N_{G(T_1)_x} \)-invariant subgroup of \( T_1 \). Therefore, the direct product \( R_1 \times R_2 \times \cdots \times R_m \) is \( G_x \)-invariant. By maximality, therefore, \( S(G)_x = R_1 \times \cdots \times R_m \). 

We combine the results of Lemmata 10 and 11 and obtain

**Theorem 10 (O'Nan, Scott)**

Let \( G \) be a primitive permutation group of degree \( n \) with a socle \( S(G) = T_1 \times T_2 \times \cdots \times T_m \) which is the direct product of \( m \) isomorphic nonabelian simple groups \( T_i \). Then either \( n = (T_1:R_1)^m \), or \( n = |T_1|^{(k-1)s} \), where \( m = k \cdot s \).

**Proof**  Since \( G \) is primitive, \( S(G) \) is transitive, hence the index \( (S(G):S(G)_x) \) is \( n \). If the \( T_i \)-component of \( S(G)_x \) is \( R_i \), a proper subgroup of \( T_i \), then \( |S(G)_x| = |R_i|^m \) by Lemma 10, hence \( n = r^m \), where \( r = (T_1:R_1) \). Otherwise, the \( T_i \)-component of \( S(G)_x \) is
By Lemma 10, there is a partition $P = \{B_1, ..., B_s\}$ of $\{1, ..., m\}$ such that $S(G)_x = D_1 \times \cdots \times D_s$ and $D_i$ is a full diagonal subgroup of $\prod_{j \in B_i} T_j$. By the proof of Theorem 9, the groups $D_i$ must be isomorphic, hence the blocks $B_i$ are of uniform size $k$ and $k$ divides $m$. Since the order of $D_i$ is $|T_i|$, $S(G)_x$ has order $|T_i|^e$, thus $n = |T_i|^{(k-1)s}$ and $k \cdot s = m$.  

We now apply Proposition 11 and Theorem 10 to primitive groups in the class $\Gamma_b$ and obtain

**COROLLARY 5 (LÜKES)**

Let $G \in \Gamma_b$ be a primitive group of degree $n$ with nonabelian socle. Then $|G| < n^c$, where $c = 2(b \cdot \log_2(3) + (\log_2(b))^2)$. That is, $c$ is a constant which depends only on $b$.

**Proof** Let $S(G) = T_1 \times \cdots \times T_m$, where the $T_i$ are isomorphic nonabelian simple groups. By Proposition 11, $G$ is isomorphic to a subgroup $G'$ of $\text{Aut}(S(G)) = \text{Aut}(T_1) \cup S_m$. Since $G \in \Gamma_b$, $|T_1| \leq b$, hence, by Theorem 5 of Chapter II, $|\text{Aut}(T_1)| \leq b^{\log_2(b)}$, which is a constant depending only on $b$.

Now consider the homomorphic image $H'$ of $G'$ in $S_m$. Since the order of $G$ (and hence of $G'$) is divisible only by primes no larger than $b$, so is the order of $H'$. Since a Sylow $p$-subgroup of $S_m$ has order less than $p^m$, it follows that the order of $H'$ is bounded by the $m$th power of the product of all primes not exceeding $b$. Let $P(b)$ be the set of primes not exceeding $b$. From Number Theory, we obtain the following estimate:

$$e \leq \prod_{p \in P(b)} p < e^{1.001162b} < 3^b,$$

where $e$ denotes Euler's constant. Hence

$$|G| \leq |\text{Aut}(T_1)|^m \cdot |H'| < b^{m \cdot \log_2(b)} \cdot 3^b \cdot m.$$

By Theorem 10, either $m = \log_r(n)$, where $2 \leq r \leq b$, or $m - s = \log_b(n)$, where $1 \leq s \leq \frac{M}{2}$. In either case, $m \leq 2 \cdot \log_2(n)$. Therefore,

$$|G| < b^{2 \cdot \log_2(b) \cdot \log_2(n)} \cdot 3^{2 \cdot \log_2(n)} = n^{2((\log_2(b))^2 + b \cdot \log_2(3))}$$

Therefore, the conclusion follows. $\blacksquare$
3.5. Primitive Groups with Abelian Socle

If $G$ is a primitive group with abelian socle $S(G)$, then $C_G(S(G))$ must contain $S(G)$ as subgroup, hence the socle does not have a trivial centralizer. Therefore, Proposition 11 does not hold for such groups and the arguments of the preceding section do not apply to $G$.

In this subsection, we show that a primitive group $G$ in $\Gamma_b$ with abelian socle must contain a Sylow $p$-subgroup of index at most $n^c$ in $G$, where $c$ is a constant which depends only on $b$ (Corollary 7 below). This constant is different from the constant of Corollary 5. The argument is as follows: Let $S(G)$ be the abelian socle of the primitive group $G$. Since $S(G)$ is the direct product of isomorphic simple abelian groups, it is elementary abelian, hence of order $p^m$, $p$ a prime number. Since $S(G)$ is transitive and self-centralizing, it is regular. Hence the degree $n$ of $G$ is $p^m$ and $G_x$ acts faithfully on $N$ by conjugation. Therefore, $G_x$ is isomorphic to a subgroup of $\text{Aut}(S(G)) = \text{GL}(m,p)$. Let $q$ be a prime other than $p$, and assume that $q^x$ is the highest power of $q$ dividing the order of $\text{GL}(m,p)$. We will show by number-theoretic argument that $x < c_{p,q}m$, where $c_{p,q}$ is a constant depending on $p$ and $q$ only. Since $G \in \Gamma_b$, the order of $G_x$ is divisible only by primes no greater than $b$. Hence we can find a constant $c$ depending only on $b$ such that for any subgroup $G'$ of $\text{GL}(m,p)$ the order $|G'| \leq p^c n^c$, provided the only primes dividing the order of $G'$ are less than or equal to $b$. This means that every Sylow $p$-subgroup of $G'$ has index at most $n^c$ in $G'$.

We begin by showing that $G_x$ is isomorphic to a subgroup of $\text{Aut}(S(G))$:

**Proposition 12**

Let $G \leq S_n$ be a primitive group with abelian socle $S(G)$. Then $S(G)$ is elementary abelian of order $p^m$, the degree of $G$ is $n = p^m$, and $G_x$ is isomorphic to a subgroup of $\text{Aut}(S(G))$.

**Proof** By Theorem 8, $S(G)$ is the direct product of isomorphic simple groups $T_1 \times \cdots \times T_m$. Since $S(G)$ is abelian, the groups $T_i$ are cyclic of prime order, hence $|S(G)| = p^m$ for some prime $p$ and the socle is elementary abelian. By Proposition 8, $S(G)$ is transitive. Since it is abelian, it centralizes itself. So, by Theorem 5, $S(G)$ is regular. Hence the degree of $S(G)$ and of $G$ is $n = p^m$. Finally, by Theorem 6, $G_x$ is isomorphic to a subgroup of $\text{Aut}(S(G))$. •
By the discussion following Definition 14 above, $G_x$ is isomorphic to a subgroup of $GL(m,p)$. For estimating the index of a Sylow $p$-subgroup of $G_x$ in $G_x$, we need some results about congruences modulo prime numbers. In the following, $(a,b)$ denotes the greatest common divisor of the (positive) integers $a$ and $b$. If $(a,b) = 1$, $a$ and $b$ are said to be relatively prime or coprime. If $a$ is congruent to $b$ modulo $p$ we write $a \equiv b \pmod{p}$.

**Definition 17**

Let $p$ be a prime number, $a$ any integer not divisible by $p$. The order of $a$ modulo $p$ is the smallest positive integer $r$ such that $a^r \equiv 1 \pmod{p}$.

Since $p$ is prime and $(a,p) = 1$, such an integer always exists. It is not difficult to see that $r$ is at most $p-1$. Furthermore, it is clear that there is no positive integer $r$ such that $a^r \equiv 0 \pmod{p}$.

**Example 8**

Let $p = 5$, $a = 4$. Then $a = 4 \equiv -1 \pmod{5}$ and $a^2 = 16 \equiv 1 \pmod{5}$, hence 4 has order 2 modulo 5. Similarly, one can see that the order of 3 modulo 5 is 4. The order of 25 modulo 5 is not defined since 5 divides 25.

**Lemma 12**

Let $p$ be a prime, $y$ and $s$ positive integers, where $(y,p) = 1$. If $m > 0$ is not divisible by $p$, then $(1+p^sy)^m = 1+p^su$, where $(u,p) = 1$.

**Proof** \[(1+p^sy)^m = 1+p^{s(m+y+\sum_{i=2}^{m}(p^{i-1}(m)^{p-1}y))} = 1+p^su.\] Here $m \cdot y$ is the only term in $u$ not divisible by $p$. Hence $(u,p) = 1$. 

**Lemma 13**

Let $p$ be a prime, $0 < i \leq p^t$. If $p^r$ is the highest power of $p$ dividing $i$, then $p^{t-r}$ is the highest power of $p$ dividing \(\binom{p^t}{i}\).

**Proof** The lemma certainly holds for $i = p^t$, so we may assume $i < p^t$. Let $E = \prod_{k=0}^{i-1}(p^t-k)$, $D = i!$, and recall that $A = \binom{p^t}{i} = \frac{E}{D}$. We pair the last term of $D$ with the first term of $E$ and pair the $k$th term in $D$ with the $k+1$st term in $E$ for $k < i$. Apart from the first term, the only terms of $E$ divisible by $p$ have the form $(p^t-u \cdot p^j)$, where $(u,p) = 1$ and $j < t$. Furthermore, such terms have been paired with $u \cdot p^j$ in $D$. Note that $\frac{p^t-u \cdot p^j}{p^j}$ is an integer not divisible by $p$. Hence the highest power of $p$ dividing $A$ is equal to the highest power of $p$ dividing $\frac{p^t}{i}$, from which the lemma follows.
Let $p$ be a prime, $y$ and $s$ positive integers such that $(y,p) = 1$. Then $(1+p^s y)^{p^t} = 1+p^{s+t}u$, where $(u,p) = 1$, unless $s = 1$ and $p = 2$.

**Proof**  
\[ A = (1+p^s y)^{p^t} = 1+p^{s+t}y+p^{2s+t}x_1+M, \]  
where  
\[ M = \sum_{i=3}^{n} (p^t_i)^{p^{s_i}y_i} \]  
and  
\[ x_1 = \frac{1}{2}(p^{t-1}-1)y^2. \]  
By Lemma 13, the highest power of $p$ dividing the term $(p^t_i)^{p^{s_i}y_i}$ is $p^{t-j+s_i}$, where $i = p^j$ and $(r,p) = 1$. Since $s \geq 1$, we know that $t-j+i \geq t+s+(i-j-1)$. If $j \geq 2$, then $r \cdot p^j-j-1 \geq 1$. If $j < 2$, then $r \cdot p^j-j-1 \geq 1$ as well, since $r \cdot p^j = i \geq 3$. Therefore, each term in $M$ is divisible by $p^{s+t+1}$.

If $p$ is odd, then $p^t-1$ is even, hence $x_1$ is an integer. Therefore, in this case we may write $A = 1+p^{s+t}(y+u')$, where $u'$ is divisible by $p$, from which the conclusion follows.

Next, if $p = 2$ and $s > 1$, then $p^{2s+t}x_1 = p^{2s+t-1}y^2(p^t-1)$, which is divisible by $p^{s+t+1}$. Hence, in this ease the lemma also follows.

If $y$ is an odd number, then $(1+2y)^{2^t} = 1+2^{s+t}u$, but this does not imply that $u$ is odd. For example,
\[ (1+2y)^2 = 1+4y+4y^2 = 1+4(y+y^2) = 1+2^3u \]
where $u$ is odd. Since both $y$ and $y^2$ are odd, it follows that $s' \geq 3$.

We now combine these results in the following

**Proposition 13**

Let $s$ and $t$ be positive numbers. Then the following is true:

(i) If $p$ is an odd prime and if both $m$ and $y$ are not divisible by $p$, then  
\[ (1+p^s y)^{2^m} = 1+p^{s+t}u, \]  
where $(u,p) = 1$.

(ii) If $s > 1$ and $m$ and $y$ are odd, then $(1+2^s y)^{2^m} = 1+2^{s+t}u$, where $u$ is odd.

(iii) For $m$ and $y$ odd, let $(1+2y)^{2^m} = 1+2^s u_1$, where $u_1$ is odd. Then, for $t > 1$,  
\[ (1+2y)^{2^m} = 1+2^{s+t-1}u, \]  
where $u$ is odd.

**Proof**  In cases (i) and (ii), we have by Lemmata 12 and 14  
\[ (1+p^s y)^{2^m} = (1+p^{s+t}u_1)^m = 1+p^{s+t}u_2, \]  
where $(u_1,p) = (u_2,p) = 1$. In case (iii), observe that $s' > 1$, thus by case (ii) above,  
\[ (1+2y)^{2^m} = (1+2^s u_1)^{2^t-1} = 1+2^{s+t-1}u_2. \]
where \( u_1 \) and \( u_2 \) are odd. ■

We apply these results to the group \( \text{GL}(m,p) \) and prove

**Corollary 6 (Luks)**

Let \( G = \text{GL}(m,p) \), \( q \) a prime different from \( p \). There is a constant \( c \) depending only on \( p \) and \( q \) such that every Sylow \( q \)-subgroup \( Q \) of \( G \) has order at most \( q^{c \cdot m} \).

**Proof** We determine the highest power of \( q \) dividing the order of \( G \). By Proposition 9, the order of \( G \) is

\[
|G| = \prod_{i=0}^{m-1} (p^m - p^i) = p^{m(m-1)/2} \prod_{i=1}^{m} (p^i - 1).
\]

The only terms in this formula which are divisible by \( q \) are

\[
(p^r - 1), \ (p^{2r} - 1), \ldots, \ (p^{kr} - 1),
\]

where \( r \) is the order of \( p \) modulo \( q \) and \( k = \left\lfloor \frac{m}{r} \right\rfloor \). We use Proposition 13 to estimate the highest power of \( q \) which divides \( |G| \), thereby estimating the order of \( Q \).

Let \( p^r = 1 + q^s u_1 \), \( p^{qr} = 1 + q^s u_2 \), where \( u_1 \) and \( u_2 \) are both coprime with \( q \). The highest power of \( q \) which divides \( p^r - 1 \) is \( q^s \). The highest power of \( q \) which divides \( p^{qr} - 1 \) is \( q^{s' + (s' - s)} \) Finally, the highest power of \( q \) dividing \( p^{qr} - 1 \), where \( t > 1 \), is \( q^{s' + t - 1} \). Note that \( s' = s + 1 \) if \( q \) is odd or \( s > 1 \). In all other cases, \( s' > s + 1 \). By Proposition 13, the highest power of \( q \) dividing \( |G| \) is therefore

\[
f(q,m,p) = s \left\lfloor \frac{m}{r} \right\rfloor + (s' - s) \left\lfloor \frac{m}{qr} \right\rfloor + \sum_{i=2}^{\infty} \left\lfloor \frac{m}{q^i r} \right\rfloor.
\]

Observe that the terms in the summation are 0 for \( i > \left\lfloor \log_q \left( \frac{m}{r} \right) \right\rfloor \). We estimate \( f(q,m,p) \) observing that \( s \leq s' - 1 \) and that \( q \geq 2 \):

\[
f(q,m,p) < s \frac{m}{r} + (s' - s) \frac{m}{qr} + \sum_{i=2}^{\infty} \frac{m}{q^i r}
\]

\[
\leq \frac{m}{r} (s' - 1 + \frac{1}{q} + \sum_{i=2}^{\infty} \frac{1}{q^i})
\]

\[
\leq \frac{m}{r} (s' - 1 + 1)
\]

\[
= \frac{s' - m}{r}.
\]
Since both $s'$ and $r$ depend on $p$ and $q$ only, the corollary follows.

We now estimate the index of a Sylow $p$-subgroup of a primitive group $G$ in $\Gamma_b$, where $G$ has the abelian socle $S(G)$ of order $p^m$.

Let $q^t$ be the highest power of the prime $q \neq p$ which divides the order of $G_x$, the stabilizer of the point $x$. Since $G_x$ is isomorphic to a subgroup of $\text{Aut}(S(G)) = \text{GL}(m,p)$, we can find a $q$-group in $\text{GL}(m,p)$ which is isomorphic to a given Sylow $q$-subgroup of $G_x$. Hence, by Corollary 6, $r \leq f(q,m,p)$. Since $G$ is in $\Gamma_b$, its order is divisible only by primes $q \leq b$. Let $P(b)$ denote the set of all primes not greater than $b$ and let $P(b,p) = P(b) - \{p\}$. Then

$$|G_x| \leq p^u \prod_{q \in P(b,p)} q^{f(q,m,p)} < p^{u3b \cdot t}$$

where $t = \sum_{q \in P(b,p)} f(q,m,p)$. Now $f(q,m,p) \leq c_{p,q} \cdot m$, where $c_{p,q}$ is a constant depending only on $p$ and $q$. Thus $t \leq \left( \sum_{q \in P(b,p)} c_{p,q} \right) \cdot m = c' \cdot m$, where $c'$ now depends only on $p$ and $b$. Choosing

$$c = \max \left( \sum_{p \in P(b)} \sum_{q \in P(a,p)} c_{p,q} \right),$$

we obtain

$$|G_x| \leq p^u \left( \prod_{q \in P(b,p)} q \right)^{c \cdot m} < p^{u3b \cdot c \cdot m}.$$ 

By Proposition 12, the degree of $G$ is $n = p^m$, hence $m = \log_p(n)$. Therefore,

$$|G_x| < p^{u \cdot n \cdot c \cdot \log_3(3)} \leq p^{u \cdot n \cdot c \cdot \log_3(3)}.$$ 

Recall that $c$ is a constant which only depends on $b$. Consequently, since a primitive group $G$ is transitive, we have just proved

**Corollary 7 (Luks)**

Let $G$ be a primitive group in $\Gamma_b$ of degree $n$ with an abelian socle of order $n = p^m$. There is a constant $c$ depending only on $b$ such that $|G| \leq p^u \cdot n^c$, i.e., every Sylow $p$-subgroup of $G$ has index at most $n^c$ in $G$. 

3.6. The Algorithm

We summarize the group-theoretic results developed above:

**Corollary 8 (Luks)**

Let $G$ be a primitive group in $\Gamma_b$ of degree $n$. There is a prime number $p$ such that $G$ has a Sylow $p$-subgroup $P$ of index at most $n^c$, where $c$ is a constant depending on $b$ alone. Furthermore, if $n = q^r$, where $q$ is a prime, then $p = q$, otherwise the conclusion holds for arbitrary primes $p$.

The proof of the corollary is straightforward from Corollaries 5 and 7 and Proposition 12. We now develop the details of the setwise stabilizer algorithm for groups in $\Gamma_b$. We do this in two steps: First, we will show how to obtain a Sylow $p$-subgroup $P$ of the action of $G$ on the blocks of a maximal system of imprimitivity. This computation includes the special case where $G$ is primitive, since we may then consider a partition into singletons of the permutation domain a maximal system of imprimitivity. Second, we give the full stabilizer algorithm. Specifically, we first consider the following

**Problem 3**

Given a generating set $K$ for a group $G$ in $\Gamma_b$ of degree $n$, a maximal system of imprimitivity $\{B_1, ..., B_n\}$ for $G$, and a prime number $p$. Find a generating set for a subgroup $P$ of $G$ which acts on the blocks $B_i$ as a Sylow $p$-subgroup of $G/H$, where $H$ is the setwise stabilizer of the blocks $B_i$.

Note that $P$ must contain $H$ as a subgroup, so that $P^* = P/H$ is a Sylow $p$-subgroup of $G^* = G/H$. The basic idea of an algorithm for this problem has been outlined in Section 3.1. In principal, the algorithm is little more than a combination of Algorithms 3 and 6 of Chapter II. It computes a representation matrix $M$ for $P$ and a list $L$ of coset representatives for $P$ in $G$. The union of $M$ and $L$ is clearly a representation matrix for $G$. The reason for maintaining $L$ separately is simply the absence of a direct membership test in $P$ which forces us to resort to the indirect method of testing whether a permutation $\pi$ may be adjoined to $M$ while retaining that the resulting group still acts on the blocks of imprimitivity as a $p$-group.

The algorithm is given below as Algorithm 2. For the sake of simplicity, we make no attempt at optimizing it. It is clear that the algorithm can be improved by better
integrating its computation. However, such an effort soon runs into a complication of details in the maintenance of suitable data structures.

**Algorithm 2 (Subgroup with p-Group Action)**

**Input**
A generating set $K$ for a permutation group $G$ of degree $n$, a system of imprimitivity $B = \{B_1, ..., B_9\}$, and a prime number $p$.

**Output**
A representation matrix $M$ for a subgroup $P$ of $G$ which acts as a Sylow $p$-subgroup of $G/H$ on the blocks $B_i$, where $H$ is the setwise stabilizer of the $B_i$. Furthermore, a list $L$ of coset representatives for $P$ in $G$.

**Comment**
For $\pi \in G$, $\pi^*$ denotes the induced permutation of the blocks $B_i$.

**Method**
1. begin
2. Initialize $M$ to represent the trivial group $I$;
3. $L := \{()\};$
4. $Q := K;$
5. while $Q$ is not empty do begin
6. remove $\pi$ from $Q$;
7. incoset := false;
8. for each $\psi \in L$ while not incoset do
9. if $\pi$ is in the coset represented by $\psi$ then begin
10. incoset := true;
11. sift $\pi \psi^{-1}$ in $M$;
12. if there is now a new entry $\pi_1 \psi$ in $M$ then
13. add to $Q$ all permutations $\pi_1 \varphi$ and $\varphi \pi_1$, where $\varphi$ is an entry in $M$ or in $L$;
14. end;
15. if not incoset then begin
16. add $\pi$ to $L$;
17. add to $Q$ all permutations $\pi \varphi$ and $\varphi \pi$, where $\varphi$ is an entry in $M$ or in $L$;
18. end;
19. end;
20. output $(M, L)$;
21. end.
Step 11 above uses Algorithm 2 of Chapter II. The details of Step 9 are given below. Here, adjoining \( \varphi \) to the matrix \( M \) means sifting \( \varphi \) in \( M \) and closing the resulting matrix under pair product formation.

9.1 \( M_1 := M \);
9.2 Adjoin \( \psi^{-1} \) to \( M_1 \);
9.3 Construct \( K^* = \{ \pi^* \mid \pi \text{ an entry of } M_1 \} \);
9.4 If the order of \( <K^*> \) is a power of \( p \) then \( \pi \) and \( \psi \) are in the same coset, otherwise they are not;

Correctness of this algorithm follows easily from the results of Chapter II. For its analysis we observe first that all operations require time polynomial in \( n \). Therefore, the algorithm requires polynomial time provided that the number of pair products formed and processed is polynomial in \( n \). While the entries of \( M \) cannot result in more than \( O(n^4) \) pair products, this is not necessarily true of \( L \). However, if \( G \) is in \( \Gamma_b \) and \( B \) is a maximal system of imprimitivity, then \( G \) acts primitively on the blocks of \( B \). Hence, with a suitable prime \( p \) by Corollary 8 above, the list \( L \) contains at most \( s^c \) members, where \( c \) is a constant depending only on \( b \). (Note that \( s \leq n \)). Thus, in that case Algorithm 2 requires polynomial time provided that \( b \) is fixed.

We give the details of the analysis of Algorithm 2. Assuming that Corollary 8 applies, a total of at most \( O(|K|+(s^c \cdot n^6)^3) \) permutations is entered into \( Q \) and processed. Consider processing a single permutation \( \pi \in Q \). Line 8 considers up to \( s^c \) members \( \psi \) of \( L \). For each such \( \psi \) we test whether \( \pi \) and \( \psi \) are in the same coset which requires at most \( O(n^6) \) steps by the proof of Proposition 2 of Chapter II. This test dominates all remaining computation steps. Consequently, Algorithm 2 requires a maximum of \( O(|K| \cdot s^c \cdot n^6 + s^{3c} \cdot n^{10}) \) steps. In summary, we have just proved

**Proposition 14**

Let \( G \in \Gamma_b \) be of degree \( n \) with a maximal system \( B \) of imprimitivity consisting of exactly \( s \) blocks. If \( s \) is a power of a prime then let \( p \) be that prime, otherwise assume that \( p \) is an arbitrary prime number. Then there is a constant \( c \) depending only on \( b \) such that Algorithm 2 requires at most \( O(|K| \cdot s^c \cdot n^9 + s^{3c} \cdot n^{10}) \) steps.

We now give the details of the setwise stabilizer algorithm. As in the case of \( p \)-groups, we stabilize the subset \( Y \) of the permutation domain in a group by working
through a tower of intransitive subgroups $G$. The general situation is that a subset $Z$ of the permutation domain is known to be setwise stabilized by the subgroup $G$, and we now determine all elements in the coset $G\pi$ of $G$ which map $Y \cap Z$ into $Y$ and $Z - Y$ into $X - Y$. Let $S_Y(G\pi, Z)$ denote this set. In Chapter IV, we encountered the following three situations for the $p$-group $G$:

1. $G$ stabilizes $Z$ pointwise. This is the base case of the recursion; either $S_Y(G\pi, Z)$ is empty or it is equal to $G\pi$. We have $S_Y(G\pi, Z) = G\pi$ iff $(Y \cap Z)^\pi$ is a subset of $Y$ and $(Z - Y)^\pi$ is a subset of $X - Y$.

2. $G$ acts intransitively on $Z$ with the orbits $\Delta_1, \ldots, \Delta_s$. Here we have $S_Y(G\pi, Z) = S_Y(\cdots S_Y(S_Y(G\pi, \Delta_1), \Delta_2), \cdots, \Delta_s)$.

3. $G$ acts transitively on $Z$. We find a maximal system of imprimitivity for the action of $G$ on $Z$ and the subgroup $H$ setwise stabilizing each block of imprimitivity. We determine a complete right transversal $\{\varphi_1, \ldots, \varphi_r\}$ for $H$ in $G$. (Since $G$ is known to be a $p$-group, we know that $r = p$). Now $S_Y(G\pi, Z) = \bigcup_{i=1}^r S_Y(H\varphi_i, Z)$.

As already outlined in Section 3.1, Case (3) above has to be modified since we have not established an a priori bound on the length $r$ of the transversal for $H$ in $G$ when $G$ is a group in $\Gamma_b$. We handle Case (3) by first finding a subgroup $P$ of $G$ such that $P/H$ is a Sylow $p$-subgroup for $G/H$. Then we use $P$ in place of $H$, followed by a sequence of subgroups of $P$ which form a tower extending from $P$ to $H$. Each factor group of consecutive subgroups in this tower has order $p$. When reaching the subgroup $H$, we have again one of the three cases above. In order to find the subgroup tower between $P$ and $H$, we extend the cases above to consider stabilizing $Y$ in the subset $Z$ subject to a fixed system of imprimitivity partitioning $Z$. This is necessary since maximal systems of imprimitivity are not unique. The above three cases now become six, three in case $Z$ consists of a single block of imprimitivity and three in case $Z$ is partitioned into more than one block. The analogy to the previous method is apparent. Let $S_Y(G\pi, B)$ denote the set of all permutations in the coset $G\pi$ which map $Y \cap Z$ into $Y$ and map $Z - Y$ into $X - Y$, where $B$ is a system of $s$ sets $\Delta_i$ of imprimitivity for the action of $G$ on $Z = \bigcup_{i=1}^s \Delta_i$. The following cases arise:
(1a) \( B \) contains only one block, \( Z = \Delta_i \), and \( G \) pointwise stabilizes \( Z \). Then
\[
S_Y(G\pi,B) = G\pi \text{ iff } (Z \cap Y)^Y \subseteq Y \text{ and } (Z-Y)^Y \subseteq (X-Y); \text{ otherwise } S_Y(G\pi,B) \text{ is empty.}
\]
(1b) \( B \) contains \( r > 1 \) blocks \( \Delta_i \) and \( G \) setwise stabilizes each block \( \Delta_i \). Then
\[
S_Y(G\pi,B) = S_Y(\cdots S_Y(S_Y(G\pi,\{\Delta_1\}),\{\Delta_2\}),\cdots,\{\Delta_i\}).
\]
(2a) \( B \) contains only one block, \( Z = \Delta_1 \), and \( G \) acts intransitively on \( Z \) with the orbits \( \Delta'_1, \ldots, \Delta'_s \). Then
\[
S_Y(G\pi,B) = S_Y(\cdots S_Y(S_Y(G\pi,\{\Delta'_1\}),\{\Delta'_2\}),\cdots,\{\Delta'_s\}).
\]
(2b) \( B \) contains \( r > 1 \) blocks \( \Delta_i \) and \( G \) acts intransitively but as a \( p \)-group on the individual blocks. Let \( \Delta'_1, \ldots, \Delta'_s \) be the orbits of the action of \( G \) on the \( \Delta_i \) and note that each such orbit \( \Delta'_j \) consists of certain blocks \( \Delta_i \). Then
\[
S_Y(G\pi,B) = S_Y(\cdots S_Y(S_Y(G\pi,\{\Delta'_1\}),\{\Delta'_2\}),\cdots,\{\Delta'_s\}).
\]
(3a) \( B \) contains only one block, \( Z = \Delta_1 \), and \( G \) acts transitively on \( Z \). We find a maximal system \( B' = \{\Delta'_1, \ldots, \Delta'_s\} \) of imprimitivity for the action of \( G \) on \( Z \). Let \( H \) be the setwise stabilizer of every block \( \Delta'_j \), \( 1 \leq j \leq s \). We find a subgroup \( P \) of \( G \) containing \( H \) such that \( P/H \) is a Sylow \( p \)-subgroup \( G/H \). We determine a complete right transversal \( \{\varphi_1, \ldots, \varphi_r\} \) for \( P \) in \( G \). Then
\[
S_Y(G\pi,B) = \bigcup_{j=1}^r S_Y(P\varphi_j\pi,B').
\]
(3b) \( B \) contains \( r > 1 \) blocks \( \Delta_i \) and \( G \) acts transitively but as a \( p \)-group on these blocks. We find a maximal system of imprimitivity for the action of \( G \) on the blocks \( \Delta_i \) and find the subgroup \( H \) stabilizing setwise each block of imprimitivity. Since \( G \) acts as a \( p \)-group, we know that \( H \) has index \( p \) in \( G \). We determine a complete right transversal \( \{\varphi_1, \ldots, \varphi_p\} \) for \( H \) in \( G \). Now
\[
S_Y(G\pi,Z) = \bigcup_{i=1}^p S_Y(H\varphi_i\pi,B).
\]
It is clear that this algorithm generalizes Algorithm 2 of Chapter IV. Note the complete analogy of the a-cases to the b-cases. Furthermore, we observe that the Cases (1b) and (2a) can be handled in formally the same manner.

Algorithm 3 below specifies the above algorithm in a more detailed manner. Case (1a) is handled by Lines 8-12, Cases (1b) and (2a) by Lines 14-31, Case (2b) by Lines 68-82, Case (3a) by Lines 33-48, and Case (3b) by Lines 50-66.
ALGORITHM 3 (Setwise Stabilizer in $\Gamma_b$)

Input Generating set $K$ for a group $G \in \Gamma_b$ acting on the set $X$ of size $n$, and a subset $Y$ of $X$. 

Output Generating set $K'$ of $G_Y$, the setwise stabilizer of $Y$ in $G$. In case that $G_Y$ is the trivial group, the set $K'$ contains $\emptyset$ only.

Comment The recursive procedure STABILIZE, Lines 5-90, works through the tower of intransitive subgroups and determines the stabilizer in a coset of the group $<K> \in \Gamma_b$ with respect to a collection of sets of imprimitivity of $<K>$.

Method 
1. begin 
2. STABILIZE( $\emptyset$, $K$, $\{X\}$, 1; $\psi$, $K'$, isempty); 
3. output($K'$); 
4. end.
5. procedure STABILIZE ($\pi$, $K$, $B$, $p$; $\psi$, $K'$, isempty); 
   comment The procedure searches the coset $<K>\pi$ of the group $<K> \in \Gamma_b$. $B$ is a system consisting of $r \geq 1$ blocks of imprimitivity $\Delta_i$ for the action of $<K>$ on the set $Z = \bigcup \Delta_i$. It is known that $<K>$ stabilizes $Z$ as a set. Moreover, if $r > 1$, then $<K>$ acts as a $p$-group on the blocks of $B$. The procedure determines all elements in the coset $<K>\pi$ which map every point in $Y \cap Z$ to a point in $Y$, and map every point in $Z-Y$ to a point in $X-Y$. This set is either empty (and then the variable $isempty$ is true), or it is the coset $<K'>\psi$, where $<K'>$ is the setwise stabilizer of $Z \cap Y$ in $<K>$, (and then $isempty$ is false).
6. begin 
7. $Z := \bigcup_{i=1}^r \Delta_i$, where $B = \{\Delta_1, ..., \Delta_r\}$; 
8. if $<K>$ stabilizes $Z$ pointwise then begin 
   comment Base Case: $<K>$ acts trivially on $Z$; 
9. $K' := K$; 
10. $\psi := \pi$; 
11. $isempty := ((Z \cap Y)^{\psi} \subseteq Y)$ and $((Z-Y)^{\psi} \subseteq (X-Y))$; 
12. end 
13. else
14. if \( r = 1 \) and \(<K>\) is intransitive on \( \Delta_1 \) or \( r > 1 \) and \(<K>\) setwise stabilizes each block \( \Delta_i, 1 \leq i \leq r \) then begin

   comment \(<K>\) acts intransitively on \( Z \);

15. if \( r = 1 \) then
16. determine the orbits \( \Delta'_1, ..., \Delta'_s \) of \(<K>\) in \( Z \)
17. else
18. let \( s = r \) and \( \Delta'_i = \Delta_i, 1 \leq i \leq r \);
19. \( K_0 := K \);
20. \( \pi_0 := \pi \);
21. \( i := 1 \);
22. isempty := false;
23. while \( i \leq s \) and not isempty do begin
24. STABILIZE(\( \pi_{i-1}, K_{i-1}, \{ \Delta'_i \}, p; \pi_i, K_i, \text{isempty} \))
25. \( i := i+1 \);
26. end;
27. if not isempty then begin
28. \( \psi := \pi_s \);
29. \( K' := K_s \);
30. end;
31. end
32. else
33. if \( r = 1 \) then begin

   comment \(<K>\) acts transitively on \( \Delta_1 \), the only block in the system \( B \). We find a maximal system of imprimitivity \( \Delta'_1, ..., \Delta'_s \) for the action of \(<K>\) on \( \Delta_1 \). Next, we find a (maximal) subgroup \( P \) of \(<K>\) which acts on the blocks of imprimitivity \( \Delta'_1 \) as a \( q \)-group (\( q \) a suitable prime number) and determine the stabilizer in the cosets of \( P \) in \(<K>\);
34. factor \( s \) into \( q^j \cdot u \), where \( q \) is prime, \( j > 0 \) and \( (u,q) = 1 \);
35. using Algorithm 2 above, determine a subgroup \( P \) of \( G = <K> \) such that \( P/H \) is a Sylow \( q \)-subgroup of \( G/H \), where \( H \) is the setwise stabilizer of the \( \Delta'_1 \) and \( q \) is as in Step 37 above. Let \( M \) be a generating set for \( P \), \( L = \{ \varphi_1, ..., \varphi_i \} \) a complete right transversal for \( P \) in \( G \);
isempty := true;
i := 1;

while i ≤ t and isempty do begin
    STABILIZE(\varphi_i \pi, M, \{ \Delta_1', ..., \Delta_s' \}, q; \psi, K', isempty);
i := i+1;
end;

while i ≤ t do begin
    STABILIZE(\varphi_i \pi, M, \{ \Delta_1', ..., \Delta_s' \}, q; \psi, K_i, cempty);
    if not cempty then
        K' := K' \cup \{ \psi \psi^{-1} \};
i := i+1;
end;
end
else

if r > 1 and \langle K \rangle acts transitively on the blocks of B then begin
    comment The collection B consists of several sets of imprimitivity on which
    \langle K \rangle acts as a transitive p-group. \langle K \rangle thus has a subgroup \langle \overline{K} \rangle of index p in
    \langle K \rangle which is intransitive on the blocks \Delta_i;

determine a maximal system of imprimitivity \Delta_1', ..., \Delta_p' for the action of \langle K \rangle
    on the blocks \Delta_i, 1 ≤ i ≤ r;

    comment Note that each \Delta_j' is a set of \frac{r}{p} blocks \Delta_i;

determine a generating set \overline{K} for the subgroup of \langle K \rangle which setwise stabil-
    izes each \Delta_j', 1 ≤ j ≤ p;

determine a complete right transversal \{ \varphi_1, ..., \varphi_p \} for \langle \overline{K} \rangle in \langle K \rangle;
isempty := true;
i := 1;

while i ≤ p and isempty do begin
    STABILIZE(\varphi_i \pi, \overline{K}, B, p; \psi, K', isempty);
i := i+1;
end;

while i ≤ p do begin
    STABILIZE(\varphi_i \pi, \overline{K}, B, p; \psi, K_i, cempty);
62. \textbf{if not} cempty \textbf{then}

63. \hspace{1em} K' := K' \cup \{ \psi_i \psi^{-1} \};

64. \hspace{1em} i := i + 1;

65. \hspace{1em} \textbf{end};

66. \textbf{end}

67. \textbf{else}

68. \hspace{1em} \textbf{begin}

69. \hspace{2em} \textbf{comment} The collection $B$ contains more than one set $\Delta_i$ and \(<K>\) acts intransitively on these sets;

70. \hspace{2em} determine the orbits $\Delta'_1, \ldots, \Delta'_s$ for the action of \(<K>\) on the blocks $\Delta_i$,

71. \hspace{2em} $1 \leq i \leq r$;

72. \hspace{2em} \textbf{comment} Note that each $\Delta'_j, 1 \leq j \leq s$, is a set of blocks $\Delta_i$;

73. \hspace{2em} $K_0 := K$;

74. \hspace{2em} $\pi_0 := \pi$;

75. \hspace{2em} $i := 1$;

76. \hspace{2em} isempty := \textbf{false};

77. \hspace{2em} \textbf{while} $i \leq s$ \textbf{and not} isempty \textbf{do begin}

78. \hspace{3em} \textbf{STABILIZE}$(\pi_{i-1}, K_{i-1}, \Delta'_i, p; \pi_i, K_0, \text{isempty})$

79. \hspace{3em} $i := i + 1$;

80. \hspace{3em} \textbf{end};

81. \hspace{2em} \textbf{if not} isempty \textbf{then begin}

82. \hspace{3em} $\psi := \pi_s$;

83. \hspace{3em} $K' := K_s$;

84. \hspace{3em} \textbf{end};

85. \hspace{2em} \textbf{end};

86. \hspace{1em} \textbf{return}$($\psi, K', \text{isempty}$)$;

87. \hspace{1em} \textbf{end.}$
Assume that Algorithm 3 is to compute the setwise stabilizer in a group $G$ in $\Gamma_b$, $b$ a constant, where $G$ has degree $n$. We now prove that this requires only time polynomial in $n$, i.e., we will show that Problem 2 is in $P$.

A precise analysis of the running time requires an exact estimate of the constant $c$ of Corollary 8 as a function of $b$. But this seems somewhat pointless, for even with small values of $b$ the value of $c$ is so large that Algorithm 3 cannot be considered practical. (See also Section 4 below). So, we only show that there is a polynomial in $n$ bounding the running time of Algorithm 3 without determining the degree of this polynomial.

We develop the analysis of Algorithm 3 in the style of Subsection 3.2 of Chapter IV. Except for the cost of the recursive calls, every line of Algorithm 3 can be executed in time polynomial in $n$ (cf. Proposition 14). Therefore, it suffices to derive recurrences which estimate the running time in accordance with the depth of the recursion, that is, with the maximum number of nested recursive calls made in the course of the computation.

First, we reduce the running time analysis to the consideration of Cases (1a), (2a), and (3a). For this we observe that Cases (1b), (2b), and (3b) are only encountered because of Case (3a), and that a sequence of the Cases (2b) and (3b) terminates with the Cases (1b), (1a), (2a), or (3a). In particular, we have the following estimate of the number of consecutive Cases (2b) and (3b):

**Lemma 15**

Let $B' = \{\Delta'_1, ..., \Delta'_s\}$, $s > 1$, be a system of imprimitivity such that $P$ acts on the blocks $\Delta'_i$ as a $p$-group. Then from the problem $S_Y(Pn, B')$ we obtain at most $s^2$ problems of the form $S_Y(H, \{\Delta'_i\})$, $1 \leq i \leq s$, where $H$ is the setwise stabilizer of every block in $B'$.

**Proof** We argue by induction on the depth of recursion needed by Algorithm 3 to break up $S_Y(Pn, B')$ into problems of the required form. Observe that the only relevant situations are Cases (2b) and (3b), for all other cases imply that a recursion is unnecessary.

**Base Case:** $P$ setwise stabilizes each block $\Delta'_i$, i.e., no recursion is needed (Case (1b)). We obtain $s < s^2$ problems of the required form.

**Induction Step:** Assume that breaking up $S_Y(Pn, B')$ requires the recursive depth $d$. We have either Case (2b) or Case (3b).

If $P$ acts transitively on the blocks $\Delta'_i$, we can find a system $\{B'_1, ..., B'_p\}$ of imprimitivity for the action of $P$ on the blocks $\Delta'_i$, where each set $B'_j$ of imprimitivity
consists of exactly \( \frac{s}{p} \) blocks \( \Delta'_j \). Let \( P_1 \) be the subgroup of \( P \) containing \( H \) and setwise stabilizing the sets of blocks \( B'_j \), \( 1 \leq j \leq p \). Then \( P_1 \) has index \( p \) in \( P \), and we obtain \( p^2 \) problems of the form \( S_y(P_1 \psi, B'_j) \), \( 1 \leq j \leq p \). By induction hypothesis, we thus obtain \( p^2(\frac{s}{p})^2 = s^2 \) problems of the form \( S_y(H \psi, \{ \Delta'_j \}) \) from \( S_y(P \psi, B') \).

If \( P \) acts intransitively on \( B' \), then let \( B'_1, ..., B'_r \) be the orbits of \( P \) on the blocks \( \Delta'_j \) with the respective lengths \( m_1, ..., m_r \). By induction hypothesis, we thus obtain \( \sum m_i^2 < s^2 \) subproblems of the form \( S_y(H \psi, \{ \Delta'_j \}) \).

Now consider Case (3a). Here we determine \( S_y(G \psi, \{ \Delta_1 \}) \), where the action of \( G \) on \( \Delta_1 \) possesses the maximal system of imprimitivity \( B' = \{ \Delta'_1, ..., \Delta'_s \} \). Since we allow that \( \Delta'_j \) is a singleton, this case includes the situation where \( G \) acts primitively on \( \Delta_1 \). Let \( H \) be the setwise stabilizer of each block \( \Delta'_j \). (In case \( G \) acts primitively on \( \Delta_1 \) we have of course \( H = I \)). By Corollary 8, \( S_y(G \psi, \{ \Delta_1 \}) \) results in at most \( s^2 \) problems of the form \( S_y(P \psi, B') \), where \( P \) acts on the blocks \( \Delta'_j \) as \( p \)-group. By Lemma 15, each of these subproblems results in at most \( s^2 \) problems of the form \( S_y(H \psi, \{ \Delta'_j \}) \), \( 1 \leq j \leq s \). Consequently, from \( S_y(G \psi, \{ \Delta_1 \}) \) we obtain at most \( s^{s+2} \) problems of the form \( S_y(H \psi, \{ \Delta'_j \}) \). Observe that the cardinality of \( \Delta'_j \) is \( \frac{|\Delta_1|}{s} \).

We have just reduced the analysis of Algorithm 3 to the consideration of the Cases (1a), (2a), and (3a). We now prove the major timing result:

**Proposition 15**

Let \( G \) be a permutation group of degree \( n \) presented by a generating set consisting of at most \( O(n^2) \) permutations. If \( G \) is in \( \Gamma_b \), then there is a polynomial \( p(x) \) whose degree depends only on \( b \) such that Algorithm 3 requires at most \( p(n) \) steps to determine a generating set for \( (G \pi)_y \), the setwise stabilizer of \( Y \) in the coset \( G \pi \).

**Proof** Let \( c \) be the constant of Corollary 8. By Proposition 14, there is a polynomial \( q(x) \) whose degree depends only on \( c \) (and therefore only on \( b \)) such that a single invocation of the procedure STABILIZE can be executed in \( q(n) \) steps, except for the time required to execute the ensuing recursive calls.

Let \( T(n,m) \) be the number of steps required to determine \( S_y(G \pi, \{ Z \}) \), where \( |Z| = m \). We show

\[
T(n,m) \leq 2^{c+3} q(n) \frac{m^{c+2} - 1}{2^{c+2} - 1} + q(n)
\]
by induction on the recursive depth.

**Induction Basis:** No nested recursive calls are needed, i.e., G pointwise stabilizes Z. It is clear that then $S_Y(G,\{Z_i\})$ can be determined in $q(n) < 2^{c+3}q(n) \cdot \frac{m_c+2}{2^{c+2} - 1} + q(n)$ steps.

**Induction Step:** Determining $S_Y(G,\{Z_i\})$ requires a recursive depth $d \geq 1$.

If $G$ acts transitively on $Z$, we have initially Case (3a). By Lemma 15 and Corollary 8, we obtain at most $s^{c+2}$ subproblems of the form $S_Y(H,\{A'j\})$, each requiring a recursive depth at most $d-1$. Here $\{A'_1, ..., A'_s\}$ is a maximal system of imprimitivity for the action of $G$ on $Z$. Thus, at most $$s^{c+2}.T(n, \frac{m_c}{s} - s^{c+2}q(n) + q(n)$$ steps are needed, where $2 \leq s \leq m$. By induction hypothesis,

$$s^{c+2}.T(n, \frac{m_c}{s}) + s^{c+2}q(n) + q(n) \leq$$

$$s^{c+2}(2^{c+3}q(n) \cdot \frac{\frac{m_c}{s}+2}{2^{c+2} - 1} + q(n)) + s^{c+2}q(n) + q(n) =$$

$$q(n) \cdot (2^{c+3}\frac{m_c+2}{2^{c+2} - 1} - 2s^{c+2} + 1) =$$

$$q(n) \cdot (2^{c+3}\frac{m_c+2-2s^{c+2}}{2^{c+2} - 1} + 1) \leq$$

$$2^{c+3}q(n) \cdot \frac{m_c+2}{2^{c+2} - 1} + q(n)$$

The last inequality follows from $s \geq 2$. This establishes the transitive case.

If $G$ acts intransitively on $Z$, let $\{A'_1, ..., A'_s\}$ be the orbits of $G$ on $Z$. We obtain $s$ subproblems of the form $S_Y(G_{j-1},\{A'_j\})$, $1 \leq j \leq s$. Let $m_j$ be the length of $A'_j$. Then we require at most

$$q(n) + \sum_{j=1}^s T(n, m_j) \leq$$

$$q(n) \cdot (1 + s + \frac{2^{c+3}}{2^{c+2} - 1} \sum_{j=1}^s m_j^{c+2} - \frac{s \cdot 2^{c+3}}{2^{c+2} - 1}) \leq$$

$$q(n) \cdot (1 + \frac{2^{c+3}}{2^{c+2} - 1} (m_c^{c+2} - \frac{s}{2} - \frac{s}{2^{c+3}}))$$ steps.

Since $s \geq 2$, we have $\frac{s}{2} + \frac{s}{2^{c+3}} > 1$. Hence

$$q(n) + \sum_{j=1}^s T(n, m_j) < q(n) \cdot (1 + \frac{2^{c+3}}{2^{c+2} - 1} \frac{m_c^{c+2} - 1}{2^{c+2} - 1}).$$
This concludes the induction step.

Note that \( \frac{2^c+3}{2^c+2-1} < 3 \), so the theorem follows from Corollary 8 with
\[ p(n) = 3(n^{c+2}+1)q(n) \]

Now it is obvious that Problem 2 is in \( P \).

4. Remarks

While we have proved that Problem 2 is in \( P \), we have not shown that there exists a practical algorithm for this problem, even for small values of \( b \). To get an impression of the established bounds, we consider testing isomorphism of graphs of valence four and five. Here the groups arising are all in \( \Gamma_3 \) (Theorem 4).

We begin with estimating the constant of Corollary 5. This constant is obtained as
\[ c_{Cor. 5} = 2((\log_2(3))^2+3\log_2(3)) \approx 14.5, \]
since \( \log_2(3) \) is approximately 1.585.

In order to determine the constant of Corollary 7, we need to compute the values of \( c_{p,q} \) where \( p, q \in \{2, 3\} \). By Corollary 6, \( c_{p,q} = \frac{s'}{r} \), where \( r \) is the order of \( p \) modulo \( q \) and \( s' \) is determined from \( p^{q'r} = 1 + q'u \), where \( u \) is not divisible by \( q \). Now \( 2^2 = 3^1 + 1 \). Since 3 is an odd prime, we have
\[ c_{2,3} = \frac{1+1}{2} = 1. \]
Moreover, \( 3^1 = 2^1 + 1 \) and \( 3^2 = 2^3 + 1 \). Hence
\[ c_{3,2} = \frac{3}{1} = 3. \]

Therefore, the constant of Corollary 7 is
\[ c_{Cor. 7} = 3.3\log_2(3) \approx 14.25 \]

Consequently, the constant of Corollary 8 is
\[ c_{Cor. 8} = \max(c_{Cor. 5}, c_{Cor. 7}) \approx 14.5 \]
By Proposition 14, determining a suitable Sylow $p$-subgroup in a primitive group in $\Gamma_3$ requires at most $O(n^{31.5+10}) = O(n^{53.5})$ steps, where $n$ is the degree of the group. Clearly this operation dominates the overhead computation in Algorithm 3, hence we may assume that the polynomial $q(n)$ in the proof of Proposition 15 has degree 53.5. Therefore, we have a bound for Algorithm 3 of $O(n^{14.5+2+53.5}) = O(n^{70})$ steps.

Recall that Line 10 of Algorithm 1 considers permutation groups of degree $n^d \leq n^d$, where $d$ is the graph valence, $n$ the number of vertices, and $n_k$ the number of vertices at distance $k$ from the edge $e$. Hence, by Theorem 1, determining $\text{Aut}_e(X)$, a connected graph of valence four or five, may require up to $O(n^{9+3+70}) = O(n^{219})$ steps, where $n$ is the number of vertices of the graphs. Testing isomorphism, therefore, may take $O(n^{220})$ steps. One should expect that these bounds can be significantly improved.

Theorem 1 and Proposition 15 clearly imply that Problem 1, determining the automorphism group of graphs of fixed valence, is in $P$. Consequently, we may test isomorphism of graphs of fixed valence and of cone graphs of fixed degree in polynomial time. The above comments seem to indicate, however, that one should not expect that these isomorphism tests are practically efficient for valence four or higher.

We can enlarge the class of graphs handled by the methods of this chapter. Consider the following

**Definition 18**

A graph $X = (V,E)$ has *forward connectivity* $d$ if there is an edge $e \in E$ or a vertex $v \in V$ such that a breadth-first search from $e$ or $v$ partitions $V$ into the sets $V_0, \ldots, V_h$, where at most $d$ vertices in $V_{k+1}$ are adjacent to the same vertex in $V_k$ and at most $d$ vertices in $V_k$ are adjacent to the same vertex in $V_{k+1}$, $0 \leq k < h$.

It is not hard to see that cone graphs of degree $d$ and graphs of valence $d$ also have the forward connectivity $d$. Furthermore, there are infinitely many graphs of forward connectivity $d$ which are neither cone graphs of fixed degree nor are graphs of fixed valence.

The class of graphs of fixed forward connectivity is motivated by considering the (direct) applicability of the techniques in this chapter. Algorithm 1 can fail in one of two ways to run in polynomial time:
(1) The set $W$ of all potential ancestries in $V_k$ fails to be polynomially bounded, hence the groups processed by Step 10 of Algorithm 1 are not of degree polynomial in $n$.

(2) The groups considered by Step 10 are not in the class $\Gamma_b$ for a fixed constant $b$.

Failure to bound the size of $W$ polynomially simply means that there is a vertex in $V_{k+1}$ which is adjacent to a number of vertices in $V_k$ not bounded by a fixed constant, whereas (2), by the results of Section 2, implies that there is a vertex in $V_k$ which is adjacent to a number of vertices in $V_{k+1}$ not bounded by a fixed constant. We conclude, therefore, that the graphs of fixed forward connectivity are a natural class to which these techniques generalize, and that they possess a polynomial time isomorphism test.

5. Notes and References

The polynomial isomorphism test for graphs of fixed valence is due to Luks [1980]. The two key observations have been Theorem 4, showing that the automorphism group of a graph $X$ of fixed valence is in the class $\Gamma_b$, $b$ a constant, and Corollaries 4 and 6, showing that primitive groups in $\Gamma_b$ are either small or have Sylow $p$-subgroups of small index. A precursor to Theorem 4 is a theorem of Babai [1979] which states that the order of an edge stabilizer subgroup of the automorphism group of a connected graph of valence $d$ is divisible only by primes smaller than $d$. The theorem can be proved by orbit considerations much like Theorem 1 of Chapter IV.

Luks defines the class $\Gamma_b$ as the set of all finite groups $G$ such that every simple section of $G$ has order at most $b$. Our definition is equivalent (Lemma 2). The Jordan-Hölder Theorem (Theorem 2) can be found in any introductory text. Theorem 3 is from Kochendörffer [1970], p. 46. A proof that $A_n$, $n > 4$, is a simple group can be found in Hall [1959] or in any other introductory text book.

Luks [1980] contains a sparse outline of the material in Sections 2 and 3. Wielandt [1964] contains most of the material from Section 3.2. The term socle (from the German Sockel) was coined by Remak [1930], who investigated its structure in terms of the minimal normal subgroups which he called the feet of the group. Remak's paper contains most of the material in Section 3.3, except for Theorem 8,
which is due to O'Nan and Scott. The theorem is mentioned in a footnote in Scott [1979]. Our proof follows a sketch in Cameron [1981].

The general results about the structure of the (nonabelian) socle in primitive groups are due to O'Nan and Scott, and are mentioned in Scott [1979]. Our development follows largely an outline in Cameron [1981]. Results concerning primitive groups with abelian socle, in contrast, are older and go back to Galois. The application of these results to primitive groups in $\Gamma_b$ is due to Luks [1980]. Lemmata 13, 14 and 15, and Proposition 12 are standard results from Number Theory. Our estimate for the product of all primes not exceeding a fixed integer $b$ is taken from Rosser and Schoenfeld [1975].

The analysis of Algorithm 3 follows the sketch in Luks [1980]. Luks remarks in the same paper on other generalizations of these techniques. Some of these will be discussed in Chapter VI.