TEL-AVIV UNIVERSITY
RAYMOND AND BEVERLY SACKLER
FACULTY OF EXACT SCIENCES
SCHOOL OF MATHEMATICAL SCIENCES

Generators of S_n and A_n

Thesis submitted in partial fulfillment of the requirements
for the M.Sc. degree of Tel-Aviv University
Department of Pure Mathematics

by

Shay Dekel

The research for this thesis has been carried out at
Tel-Aviv University
Under the direction of
Professor Marcel Herzog

July 1994

I deeply thank Professor Herzog for his generous help in the preparation of the thesis.

I would like to thank the creators of GAP (Groups, Algorithms and Programming) for making their tools public domain.

Thank you Tal for your constant support.

Contents

Abstract

Netto, in his book published last century, conjectured that almost all pairs of permutations from the symmetric group over n letters will generates either the Alternating group (A_n) or the Symmetric group (S_n). Since 3/4 of all such pairs contain at least one odd permutation it would follow that the probability of generating S_n is roughly 3/4. Netto's conjecture remained open until Dixon [1] proved the conjecture. Dixon proved that the probability that a random pair (x, y) $x, y \in S_n$ generates S_n approaches 3/4 as $n \to \infty$. Also, the probability that a pair (x, y), $x, y \in A_n$ generates A_n approaches 1 as $n \to \infty$. Dixon also stated a conjecture that generally for any finite simple group G, the probability approaches 1 as $|G| \to \infty$. Lately [2] the proof to this conjecture was completed using the classification of the finite simple groups.

These statistical results indicate that it is, in a sense, "easy" to find generators of S_n and A_n (or any finite simple group). Indeed, the main result of this work shows that except for a very special case, for every permutation x in S_n (A_n) there exists a permutation y in S_n (A_n) so together they generate S_n (A_n).

In Chapter 1 we give some preliminaries, definitions and general results on generators in finite groups. We pay special attention to groups with rank 2 (as is the case with S_n, A_n for $n \geq 4$), and observe the connection between the Frattini subgroup of a finite group and the non-generators of the group.

In Chapter 2 we concentrate on the groups S_n. We explore the combinatorial structure of the conjugacy classes, and present methods for calculating their number and sizes. The main result of this Chapter is a recursive algorithm that calculates the *Number theoretical function* $p(n)$, and thus, the number of conjugacy classes in S_n.

The main result is presented in Chapter 3. We explicitly find a complement for every permutation is S_n (A_n), such that together they generate S_n (A_n). Also, as an example, we find all the complements of a transposition in S_n.

Chapter 1

Preliminaries

In this Chapter we present some basic definitions and general results on generators in finite groups. Throughout the Chapter G is a *finite* group, unless stated otherwise.

1.1 Generators of a group

Generators. We say $\{g_i | g_i \in G\}$ are generators of G if $\langle g_i \rangle = G$.

Rank of a group. The rank of a group is defined:

$$\mathrm{rk}(G) = \min\{|X| : X = \{x_i\},\ x_i \in G,\ \langle x_i \rangle = G\}$$

Base. A set $X = \{x_i\}_{i \in I}\ x_i \in G$, is called a base (of G) if $|X| = \mathrm{rk}(G)$ and $\langle X \rangle = G$.

Independent Set. An Independent set $\{g_i\}_{i \in I}\ g_i \in G$, is a set of elements in G, such that $\forall i_0 \in I\ \ \langle g_j : j \neq i_0 \rangle < \langle g_i : i \in I \rangle$.

Complement set. A complement set $Y = \{y_i\}\ y_i \in G$, for a given set $X = \{x_i\}\ x_i \in G$, is a set of elements of G such that

$$\langle X, Y \rangle = \langle g : g \in X \vee g \in Y \rangle = G$$

Examples

1. For any cyclic group G, $\mathrm{rk}(G) = 1$ by definition. Thus, any subset of G can be complemented by the generator of G.

   If we identify $G \cong \mathcal{Z}/n\mathcal{Z}$, then the only bases for G are the the elements $[k]$, $(k, n) = 1$, $k \neq 1$.

2. Let G be a free group over S symbols. Then $\mathrm{rk}(G) = |S|$, but G is not finite. Each subset of the symbols can be complemented to a base by the other symbols. But if for example G is a free group over the two symbols $\{a, b\}$, then the element a^2 can not be complemented to a base of G.

3. Let $G = S_4$. Then $\mathrm{rk}(G) = 2$ and it is easy to verify that the permutation $(1,2)(3,4)$ can not be complemented to a base of S_4. In Chapter 3 we will show that the example of S_4 and the conjugacy class of $(1,2)(3,4)$ is exceptional.

1.2 Generators of groups with rank 2

Let G be a finite group with $\mathrm{rk}(G)= 2$.

2–generator. We say $x \in G$ is a 2–generator if it can be complemented to a base of G.

Lemma 1.1 *Let $x \in G$, $x \neq 1$. Then x is a non 2–generator iff*

$$G = \bigcup\{M_i : M_i \text{ max } G,\ x \in M_i\}$$

Proof: Let x be a non 2–generator. The set of maximal subgroups of G containing x is not empty, otherwise $\langle x\rangle = G$, which is a contradiction to $\mathrm{rk}(G) = 2$. Suppose $y \in G\backslash\bigcup\{M_i : M_i \text{ max } G,\ x \in M_i\}$. Then $\langle x, y\rangle = G$, otherwise y is in some maximal subgroup M_{i_0} that contains both x and y. This is a contradiction to x being a non 2–generator. Thus, $G\backslash\bigcup\{M_i : M_i \text{ max } G,\ x \in M_i\} = \emptyset$. From the above it is easy to see that if for an element x of G, $\bigcup\{M_i : M_i \text{ max } G,\ x \in M_i\} = G$ then x is a non 2–generator. ∎

Lemma 1.2 *Let $X = \{x_i\}$ be the set in G of non 2–generators. Then*

$$X = \bigcup\{\bigcap M_i : M_i \max G,\ \cup M_i = G\} \tag{1.1}$$

Proof: Let $x \in X$. By Lemma 1.1, $\bigcup\{M_i : M_i \text{ max } G,\ x \in M_i\} = G$. Thus $x \in \bigcap M_i$, where $M_i \max G$, $\bigcup M_i = G$. This means x is in the union defined in (1.1). Also by Lemma 1.1, if an element y of G lies in an intersection of maximal subgroups of G, $\{M_i\}$, $\bigcup M_i = G$, then y is a non 2–generator. ∎

The next Lemma shows a connection between covering of a group G, $\mathrm{rk}(G) = 2$, and the quantity of 2–generators.

Lemma 1.3 *The set of non 2–generators is trivial iff for any covering of G, $G = \cup_{i=1}^m G_i$, $G_i < G$ for all $1 \leq i \leq m$, implies $\cap_{i=1}^m = \{1\}$.*

Proof: Assume X, the set of non 2–generators, is trivial. Let $G = \cup_{i=1}^m G_i$, $G_i < G$ for $1 \leq i \leq m$, be a covering of G. Assume $1 \neq x \in \cap_{i=1}^m G_i$. Let M_i be a maximal subgroup of G, $G_i \leq M_i < G$ for all $1 \leq i \leq m$. As $x \in M_i$, $1 \leq i \leq m$, we have

$G = \cup\{M_i : M_i \text{ max } G,\ x \in M_i\}$. By Lemma 1.1, x is a non 2–generator. This contradicts X trivial. Thus, $\cap_{i=1}^{m} G_i = \{1\}$.

Next we assume that for any covering of G, $G = \cup_{i=1}^{m} G_i$, $G_i < G$ for all $1 \leq i \leq m$, implies $\cap_{i=1}^{m} G_i = \{1\}$. Assume $x \in G$, $x \neq 1$, is a non 2–generator. By Lemma 1.1, $G = \cup\{M_i : M_i \text{ max } G,\ x \in M_i\}$. Thus there exists a covering of G with a non trivial intersection. This contradicts the assumption. Thus, the set of non 2–generators is trivial. ∎

1.3 The Frattini subgroup

It is natural to see the connection between the Frattini subgroup and non 2–generators.

Frattini subgroup. The Frattini subgroup of a group G, Frat(G) is defined

$$\text{Frat}(G) = \bigcap\{M_i : M_i \max G\}$$

The Frattini subgroup is defined in terms of non generators, as the next Lemma shows.

Lemma 1.4 *Frat(G) is generated by the elements x of G such that for any subset X of G, $\langle x, X\rangle = G \Rightarrow \langle X\rangle = G$.*

Proof: Let $x \in \text{Frat}(G)$. Suppose X is a subset of G such that $\langle x, X\rangle = G$, but $\langle X\rangle < G$. Let M be a maximal subgroup of G containing X. $x \notin M$, as this implies, $G = \langle x, X\rangle \leq M$. This is a contradiction to $x \in M$, for all M, M maximal in G.

Let $x \in G$, such that for any subset X of G, $\langle x, X\rangle = G \Rightarrow \langle X\rangle = G$. Suppose $\exists M$ max G, $x \notin M$. This means that $G = \langle x, M\rangle$. But this means M is a subset of G such that $\langle x, M\rangle = G$, $\langle M\rangle = M < G$ and a contradiction. ∎

Lemma 1.5 *Let G be a finite group, with rk(G)=2. Then*

$$\textit{Frat}(G) \leq \{\textit{non 2–generators of } G\}$$

Proof: If $x \in \text{Frat}(G)$ is a 2–generator, then $\exists y \in G$, $\langle x, y\rangle = G$. According to Lemma 1.5 this implies $\langle y\rangle = G$, which is a contradiction to rk(G)=2. ∎

Corollary 1.6 *Let S be the set of non 2-generators of G, with rk(G)=2. Then,*

$$|\textit{Frat}(G)| > 1 \Rightarrow |S| > 1$$

Chapter 2

Conjugacy classes of the symmetric group

In this Chapter we show combinatorial results on the conjugacy classes of the group S_n.

2.1 The conjugacy class

Conjugacy. Let x, y be elements of a group G. We say x, y are conjugate if there exists $z \in G$, such that, $x^z = z^{-1}xz = y$.

It is easy to see that conjugacy is an equivalence relation.

Conjugacy class. For an element x in a group G, the equivalence class of elements that are conjugate to x is called the conjugacy class of x. It is denoted by $\mathrm{Cl}_G(x)$.

C(x). For an element of a group G, the subgroup of elements $y \in G$ such that $[x, y] = x^{-1}y^{-1}xy = 1$ or $xy = yx$, is denoted by $\mathrm{C}(x)$.

Lemma 2.1 *Let x be an element of a finite group G. Then,*

$$[G : C(x)] = |Cl(x)|$$

Proof: Each member $y \in \mathrm{Cl}(x)$ can be represented by a power of x by some element $z \in G$, such that $x^z = y$.

We choose a set of such representatives $Z = \{z_i\}$. Observe that $|Z| = |\mathrm{Cl}(x)|$. We define the natural mapping

$$F : Z \longrightarrow \text{Left cosets of } \mathrm{C}(x)$$

by $F(z) = z\mathrm{C}(x)$.

F is one–to–one mapping, because

$$F(z_1) = F(z_2) \iff z_1\mathrm{C}(x) = z_2\mathrm{C}(x) \iff z_1^{-1}z_2 \in \mathrm{C}(x)$$
$$\iff x^{z_1^{-1}z_2} = x \iff x^{z_1} = x^{z_2} .$$

Also F is onto, as for each coset $y\mathrm{C}(x)$ we choose the representative $z \in Z$ such that $x^z = x^y$. ∎

2.2 Conjugacy classes in S_n

In the symmetric group each permutation can be represented by a product of disjoint cycles.

Decomposition of a permutation. Let $x \in S_n$. Let $x = \prod_{i=1}^{m} C_i$ where C_i, $1 \leq i \leq m$ are disjoint cycles and $|C_i| \leq |C_{i+1}|$ ($|C_i|$ denotes the length of the cycle C_i). This is called the decomposition of x. Sometimes the cycles of length one are omitted from the decomposition, so it is understood that points that are omitted, are fixed under the action of x.

The decomposition is unique up to the order of cycles in the decomposition that have the same length, and the writing order of the points of each cycle.

Example

$(1,2,3)(4,5,6) = (4,5,6)(1,2,3) = (2,3,1)(6,4,5)$

Type of permutation. Let x, y be permutations in S_n, with decompositions

$$x = \prod_{i=1}^{m} C_i, \qquad y = \prod_{j=1}^{l} D_j .$$

including the cycles of length one. If $m = l$, and $|C_i| = |D_i|$ for all $1 \leq i \leq m$, we say that x, y are of the same type. It is easy to prove that two permutations have the same type $\iff$ they are conjugate in S_n.

Usually calculating the conjugacy classes of an arbitrary group is time consuming. All algorithms are polynomial in the size of the group, and some faster algorithms utilize special qualities of the group, such as p–group, solvability, etc.

Due to the combinatorial structure of S_n, calculations are simpler. Namely it is easy to quickly give the number of conjugacy classes, the size of each class, and output a representation of the class.

2.2.1 Sizes of the conjugacy classes in S_n

First we show an equation for $|\mathrm{Cl}(x)|$, for a permutation of a known type.

Lemma 2.2 *Let $x \in S_n$, with a cycle decomposition $x = \prod_{j=1}^{m} C_j$ (Cycles of length one are included). Let k_i be the number of cycles of length i. Then,*

$$|Cl(x)| = \frac{n!}{\prod_{i=1}^{n} i^{k_i} k_i!} \tag{2.1}$$

Proof: There are $n!$ ways of writing the n points $\{1, \ldots, n\}$ as a product of k_1 cycles of length 1, k_2 cycles of length 2, ..., k_n cycles of length n. many of these yields the same permutation. Any i–cycle can be started in any of i places. For example $(1,2,3) = (2,3,1) = (3,1,2)$. So, there are i^{k_i} ways of writing the k_i i–cycles, keeping the i–cycles in the same writing order.

In addition, the k_i i–cycles can be permuted in $k_i!$ ways. For example,

$$\begin{aligned} & (1,2)(3,4)(5,6) = (1,2)(5,6)(3,4) = (3,4)(1,2)(5,6) = \\ = \; & (3,4)(5,6)(1,2) = (5,6)(1,2)(3,4) = (5,6)(3,4)(1,2) \; . \end{aligned}$$

As the above changes are the only permitted, the Lemma follows. ∎

Example

The size of the conjugacy class of $(1,2)(3,4,5)$ in S_7.

We have,

$$\begin{aligned} k_1 &= 2, && \text{as the points } 6,7 \text{ are fixed} \\ k_2 &= 1, \\ k_3 &= 1, \\ k_4 &= k_5 = k_6 = k_7 = 0 \end{aligned}$$

Thus,

$$|\mathrm{Cl}_{S_7}(\,(1,2)(3,4,5)\,)| = \frac{7!}{(1^2 \cdot 2!)(2^1 \cdot 1!)(3^1 \cdot 1!)} = 420$$

Using (2.1) we can conclude the following.

Lemma 2.3 *Let $n \geq 2$. For any $x \in S_n$,*

$$|Cl(x)| \leq |Cl(\,(1,2,\ldots,n-1)\,)| \tag{2.2}$$

Proof: The proof is by induction on n. For $n < 5$, it is easy to verify (2.2). By (2.1) we need only to prove that for any $\{k_i\}_{i=1}^{n}$, such that $\sum_{i=1}^{n} i k_i = n$,

$$\frac{n!}{\prod_{i=1}^{n} i^{k_i} k_i!} \leq \frac{n!}{n-1}$$

or,

$$\prod_{i=1}^{n} i^{k_i} k_i! \geq n-1$$

Assume for all $n' < n$.
Suppose there is an index i_0, $1 \leq i_0 \leq n$ such that $2 \leq i_0 k_{i_0} \leq n-3$. We denote $a = i_0 k_{i_0}$.
By induction,

$$\prod_{i=1}^{m} i^{k_i} k_i! = i_0^{k_{i_0}} k_{i_0}! \prod_{j \neq i_0} j^{k_j} k_j! \geq i_0 k_{i_0}(n - i_0 k_{i_0} - 1) = a(n-a-1)$$

Thus it is sufficient to prove

$$\begin{aligned}
& n-1 \leq a(n-a-1) \\
\Leftrightarrow \quad & a^2 + a - 1 \leq (a-1)n \quad a \geq 2 \\
\Leftrightarrow \quad & \frac{a^2+a-1}{a-1} \leq n \\
\Leftrightarrow \quad & \frac{a^2-1}{a-1} + \frac{a}{a-1} \leq n \\
\Leftrightarrow \quad & a + 1 + \frac{a}{a-1} \leq n
\end{aligned}$$

but,

$$a + 1 + \frac{a}{a-1} \leq n - 3 + 3 = n$$

- We are left with the cases that all positive ik_i, $1 \leq i \leq n$, satisfy either $ik_i = 1$ or $ik_i \geq n-2$.
- If there is an index i_0 such that $i_0 k_{i_0} = n$, then for all other indexes $i \neq i_0$, $k_i = 0$. Thus,

$$\prod_{i=1}^{n} i^{k_i} k_i! = i_0^{k_{i_0}} k_{i_0}! \geq i_0 k_{i_0} = n \geq n-1$$

- If there is an index i_0 such that $i_0 k_{i_0} = n-1$, then we know $i_0 \neq 1$ and,

$$k_i = \begin{cases} 1 & i = 1 \\ k_{i_0} & i = i_0 \\ 0 & i \neq 1, i_0 \end{cases}$$

Again,

$$\prod_{i=1}^{n} i^{k_i} k_i! = (1^1 \cdot 1!)(i_0^{k_{i_0}} k_{i_0}!) = i_0^{k_{i_0}} k_{i_0}! \geq i_0 k_{i_0} = n-1$$

- If there is an index i_0 such that $i_0 k_{i_0} = n-2$, then we are left with an integral part of n of size 2, meaning either $k_1 = 2$, $i_0 \neq 1$ or $k_2 = 1$, $i_o \neq 2$. In either of the cases there is an index i_1, $i_1 \in \{1, 2\}$ and $i_1 k_{i_1} = 2$.
- The case that all positive ik_i equal 1 is clearly impossible.

The Lemma follows. ∎

2.2.2 The number of conjugacy classes, the function $p(n)$

Next we wish to enumerate the conjugacy classes of S_n. That is, to count how many classes there are, and output a representative for each class. As explained above, it is enough to output for each class the type of the class members. First we shall use a well known result from [3] to count the number of classes.

Partition of an integer. Let n be a positive integer. A partition of n is a representation of n as the sum of positive integral parts. For example, all the partitions of 5 are

$$5 = 5 = 4+1 = 3+2 = 3+1+1 = 2+2+1 = 2+1+1+1 = 1+1+1+1+1.$$

$p(n)$. We denote the number of partitions of an integer n by $p(n)$. Thus, $p(5) = 7$.

Clearly, the function $p(n)$ gives exactly the number of conjugacy classes in S_n. Each type is defined by a cycle decomposition, that can be thought of as a partition of n.

Generating formal power series. A generating formal power series of a function $f : \mathcal{Z} \to \mathcal{Z}$, is a series of the form,

$$F(x) = \sum_{n \in \mathcal{Z}} f(n)x^n \quad .$$

The generating formal power series of $p(n)$ was found by Euler and is,

$$F(x) = \frac{1}{\prod_{n=1}^{\infty}(1-x^n)} = \frac{1}{(1-x)(1-x^2)(1-x^3)\cdots} = 1 + \sum_{n=1}^{\infty} p(n)x^n$$

Example

The intuition of the structure of the generating function $F(x)$ can be explained by the following example.

Let us look at a partition of 8, $8 = 1+2+2+3$. We wish to see which elements of the generating function contribute a unit to the coefficient $p(8)$ of x^8, in accordance with this particular partition.

$$\frac{1}{1-x} = 1 + x + x^2 + \ldots \quad \text{contributes} \quad x$$
$$\frac{1}{1-x^2} = 1 + x^2 + x^4 + \ldots \quad \text{contributes} \quad x^4 = x^2 \cdot x^2$$
$$\frac{1}{1-x^3} = 1 + x^3 + x^6 + \ldots \quad \text{contributes} \quad x^3$$

Using the formal power series it can be proved that $p(n)$ obeys the following recursive formula,

$$p(n) - p(n-1) - p(n-2) + p(n-5) + \ldots + \tag{2.3}$$
$$(-1)^k p(n - \frac{1}{2}k(3k-1)) + (-1)^k p(n - \frac{1}{2}k(3k+1)) + \ldots = 0$$

We would like to show another, more intuitive method of calculating $p(n)$, that will also produce the partitions, permutations types and representatives of conjugacy classes.

Actually we show something a little stronger.

Restricted partitions of an integer. Let m, n be two positive integers, with $m \leq n$. We call all the partitions of n, with integral parts $\geq m$, restricted partitions of n by m.

We denote their number by $\tilde{P}(n, m)$.

Examples

1. Clearly $p(n) = \tilde{P}(n, 1)$.
2. $\tilde{P}(7, 2) = 4$, because $7 = 2+2+3 = 2+5 = 3+4 = 7$.

$\boldsymbol{P(i,j)}$. Next we define the following function, which is recursive in two variables. For any two non-negative integers i, j,

$$P(i,j) = \begin{cases} 0 & 0 < i < j \\ 1 & i = 0 \\ \sum_{k=j}^{i} P(i-k, k) & \text{otherwise} \end{cases} \tag{2.4}$$

Lemma 2.4 *For any two positive integers m, n such that $m \leq n$,*

$$\tilde{P}(n, m) = P(n, m)$$

Proof: As promised, the proof is very intuitive. We need to explain the logic involved in a single traversal down the recursion tree, and the stop mechanism that determines the leaves of the recursion tree.

First we observe that at no time during the recursive process, the variables i, j are negative integers. This is because we start off at the root with integers m, n, $m \leq n$, and by the definition of $P(i, j)$ in (2.4) this case is not possible.

Suppose we arrive at a node of the recursive process with $0 < i < j$. As there is no way to partition i with integral parts $\geq j$, we conclude that the path we traveled from the root to this node (= the partition) is illegal. Therefore we return 0.

Suppose we arrive at a node with $i = 0$. This means the path from the root to this node defines a perfect partition of the integer n. Therefore, the node is a leaf, and we return a unit that symbolize the legal partition.

The last case is the case of $j \leq i$. This case explains the logic of $P(i,j)$. Suppose we decide to count all the partitions of i that have at least one integral part of size j. This means we take "off" i a part of the size j, and recursively calculate $P(i-j,j)$.

Suppose $i > j$. To calculate the number of partitions of i that have integral parts of size $\geq j+1$, and have at least one part of size $j+1$, we recursively calculate $P(i-(j+1),j+1)$.

Summing up over all integers $j \leq k \leq i$, we have for $j \leq i$

$$P(i,j) = \sum_{k=j}^{i} P(i-k,k)$$

This concludes the proof. ∎

Corollary 2.5 *The recursive algorithm described in Lemma 2.4 calculates all the conjugacy classes of S_n.*

Proof: If we observe carefully the structure of the recursive process defined by $P(i,j)$, we see that during the process we are able to calculate not only the number of partitions, but output them explicitly. Each partition is described by "legal" traversal down the recursive tree, and the nodes of the traversal contain the integral parts of the partition. As a partition of n represents a type of permutation, which in turn represents a conjugacy class of S_n, representatives of the classes can be listed by the algorithm. ∎

Examples

1. As we have shown, $p(5) = 7$. Using $P(i,j)$ we have

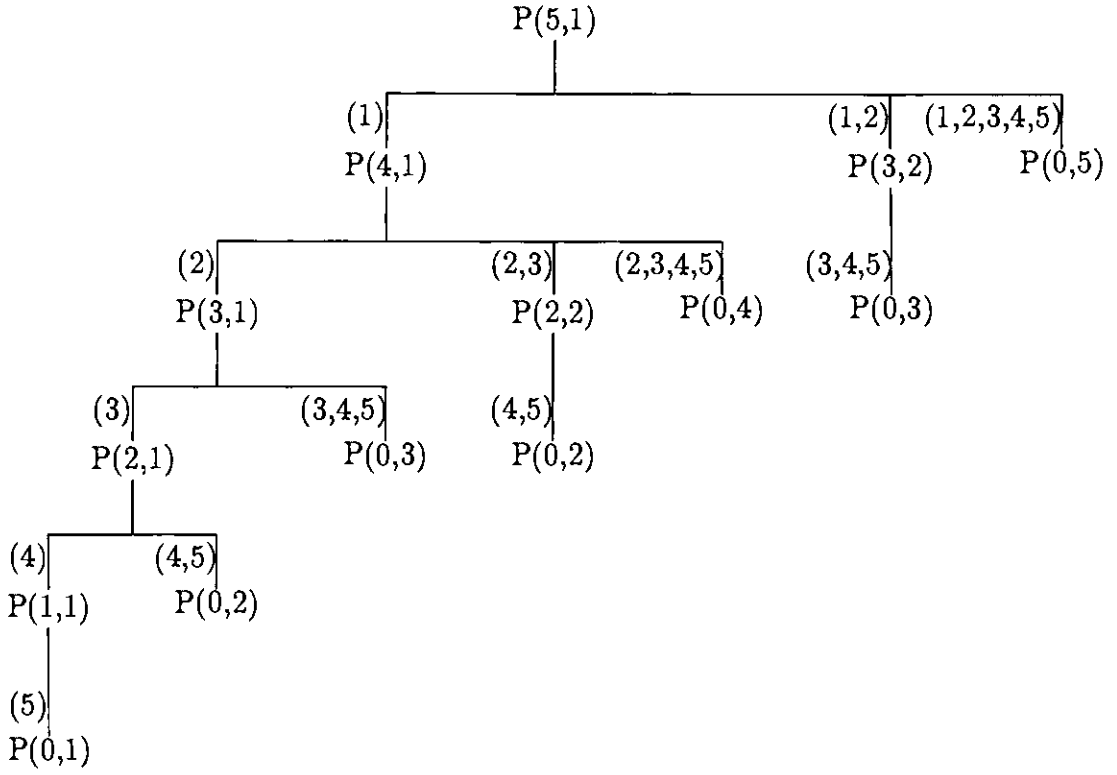
$$\begin{aligned}
p(5) &= \tilde{P}(5,1) = P(5,1) \\
&= P(4,1) + P(3,2) + P(2,3) + P(1,4) + P(0,5) \\
&= P(4,1) + P(3,2) + 1 \\
&= [P(3,1) + P(2,2) + P(1,3) + P(0,4)] + [P(1,2) + P(0,3)] + 1 \\
&= [P(2,1) + P(1,2) + P(0,3)] + P(0,2) + 3 \\
&= P(2,1) + 5 \\
&= P(1,1) + P(0,2) + 5 \\
&= P(1,1) + 6 \\
&= P(0,1) + 6 \\
&= 7
\end{aligned}$$

2. We have shown that $\tilde{P}(7,2) = 4$.

$$\begin{aligned}
\tilde{P}(7,2) &= P(7,2) \\
&= P(5,2) + P(4,3) + P(3,4) + P(2,5) + P(1,6) + P(0,7)
\end{aligned}$$

$$
\begin{aligned}
&= P(5,2) + P(4,3) + 1 \\
&= [P(3,2) + P(2,3) + P(1,4) + P(0,5)] + [P(1,3) + P(0,4)] + 1 \\
&= P(3,2) + 3 \\
&= P(1,2) + P(0,3) + 3 \\
&= 4
\end{aligned}
$$

3. As stated before in Corollary 2.5, using the recursive algorithm of Lemma 2.4, we can list all the conjugacy classes of S_n. We show this for $n = 5$:



Collecting all the above legal traversals down the recursion tree, we list representatives for each of the seven conjugacy classes of S_5:

$$
\begin{aligned}
&(1)(2)(3)(4)(5) \\
&(1)(2)(3)(4,5) \\
&(1)(2)(3,4,5) \\
&(1)(2,3)(4,5) \\
&(1)(2,3,4,5) \\
&(1,2)(3,4,5) \\
&(1,2,3,4,5)
\end{aligned}
$$

The function $p(n)$ can be shown [3] to have an upper bound of the form:

$$p(n) < e^{k\sqrt{n}}, \quad k = \pi\sqrt{\tfrac{3}{2}}$$

Using any one of the recursive equations of $p(n)$, (2.3) or (2.4), the following values of $p(n)$ can be calculated:

$$\begin{aligned} p(1) &= 1 \\ p(5) &= 7 \\ p(10) &= 42 \\ p(20) &= 627 \\ p(50) &= 204,226 \\ p(100) &= 190,569,292 \\ p(200) &= 3,972,999,029,388 \end{aligned}$$

Chapter 3

Generators of S_n and A_n

The main theorems we will prove in this Chapter are,

Theorem 3.1 *For every permutation $x \in S_n$, $x \neq 1$ there exists a permutation $y \in S_n$ such that $\langle x, y \rangle = S_n$, except for the case when x is in the Klein subgroup of S_4.*

Theorem 3.2 *For every permutation $x \in A_n$, $x \neq 1$, there exists a permutation $y \in A_n$ such that $\langle x, y \rangle = A_n$.*

Using Lemma 1.3, we have an interesting application of the above Theorems.

Corollary 3.3 *Let $n \geq 4$. Let $G = A_n$ or S_n, $G \neq S_4$. Let $G = \cup_{i=1}^{m} G_i$, $G_i < G$ for all $1 \leq i \leq m$, be a covering of G. Then $\cap_{i=1}^{m} G_i = \{1\}$.*

3.1 Preliminaries

Before we prove the above theorems, it is required to prove a series of small Lemmas. The following Lemmas prove that some combinations of cycles generate S_n or A_n. Some of the Lemmas are well known.

Transposition. A cycle of length two is called a *transposition.*

Lemma 3.4 *The transpositions in S_n together generate S_n.*

Proof: As explained in Chapter 2, each element of S_n can be written as a product of disjoint cycles. Therefore it is sufficient to show that each cycle can be written as a product of transpositions, all defined over the points of the cycle.

Let $x = (a_1, a_2, \ldots, a_k) \in S_n$. We can write

$$x = (a_1, a_2, \ldots, a_k) = (a_1, a_2)(a_1, a_3)(a_1, a_4) \cdots (a_1, a_k)$$

∎

Lemma 3.5 *The transpositions* $(1,2),(1,3),\ldots,(1,n)$ *together generates* S_n.

Proof: Using Lemma 3.4, it is sufficient to show that any transposition (i,j) can be generated.

$$(i,j) = (1,i)^{(1,j)} = (1,j)(1,i)(1,j)$$

∎

Lemma 3.6 *The transpositions* $(1,2),(2,3),\ldots,(n-1,n)$ *together generate* S_n.

Proof: Using Lemma 3.5 it is sufficient to show that any transposition $(1,i)$, $2 \leq i \leq n$ can be generated.

$$(1,i) = (i-1,i)\cdots(3,4)(2,3)(1,2)(2,3)(3,4)\cdots(i-1,i)$$

∎

Lemma 3.7 *The transposition* $(1,2)$ *and the cycle* $(1,2,\ldots,n)$ *together generate* S_n.

Proof: By Lemma 3.6 we need only write each transposition of the form $(i,i+1)$ as a word in $(1,2),(1,2,\ldots,n)$. This is achieved as follows:

$$(2,3) = (1,2)^{(1,2,3,\ldots,n)}$$

and generally,

$$(i,i+1) = (1,2)^{(1,2,\ldots,n)^{(i-1)}} \quad \text{for } 1 \leq i < n-1$$

∎

Lemma 3.8 *The transposition* $(1,2)$ *and the cycle* $(2,3,\ldots,n)$ *together generate* S_n.

Proof: By Lemma 3.5 we need only write each transposition of the form $(1,i)$ as a word in $(1,2),(2,3,\ldots,n)$. This is achieved as follows:

$$(1,3) = (1,2)^{(2,3,\ldots,n)}$$

and generally,

$$(1,i) = (1,2)^{(2,3,\ldots,n)^{(i-2)}} \quad \text{for } 2 \leq i < n.$$

∎

Next we prove similar results for the Alternating Group (A_n)

Lemma 3.9 *The 3–cycles (cycles of length 3) together generate A_n.*

Proof: Let $x \in A_n$. As in Lemma 3.4, x can be written as a product of transpositions. Because $x \in A_n$, the number of transpositions in the product is even. Thus, it is sufficient to show that each product of an adjacent pair of transpositions can be written as a product of 3–cycles.

Let i, j, k, l be integers, $i \neq j$, $k \neq l$, $1 \leq i, j, k, l \leq n$. We look at the product of the two transpositions (i, j), (k, l).
If $i = k$, $j = l$ then $(i, j) \cdot (k, l) = ()$.
If $i \neq k$, $j = l$ then $(i, j) \cdot (k, j) = (i, k, j)$.
The last case is $i \neq k$, $j \neq l$. In this case we can write

$$(i, j) \cdot (k, l) = (i, j) \cdot (j, k) \cdot (j, k) \cdot (k, l) = (i, k, j) \cdot (j, l, k)$$

∎

Lemma 3.10 *The cycles of the form (i, j, k), $i < j < k$, together generate A_n.*

Proof: For any 3–cycle $x = (i, j, k)$ we can assume $i < j, k$. Otherwise, we simply rewrite the 3–cycle in that form. Next, if $j > k$, then $x^2 = (i, k, j)$, has the required property. As $(x^2)^2 = x$ for 3–cycles, the Lemma follows. ∎

Lemma 3.11 *The 3–cycles $(1, 2, 3), (2, 3, 4), \ldots, (n-2, n-1, n)$ together generate A_n.*

Proof: Let $H \leq A_n$ be the subgroup that is generated by the 3–cycles of the form $(i, i+1, i+2)$, $1 \leq i \leq n-2$.

1. First we prove that each 3–cycle $x = (i, i+1, k)$, $i+2 \leq k \leq n$, is in H: Observe that for $i \leq n-4$,

   $$(i, i+1, i+2)^{(i+2, i+3, i+4)} = (i, i+1, i+3),$$

   and generally,

   $$(i, i+1, j)^{(j, j+1, j+2)} = (i, i+1, j+1), \text{ for } i+2 \leq j \leq n-2.$$

   This means that for $i \leq n-4$, all the 3–cycles $(i, i+1, k)$, $i+2 \leq k \leq n-1$, are in H. But for $i \leq n-4$ we can also generate $(i, i+1, n)$ by

   $$(i, i+1, n-1)^{(n-2, n-1, n)} = (i, i+1, n).$$

   We are left with the case of $n-3 \leq i \leq n-2$. For $i = n-2$, $(n-2, n-1, n) \in H$, by definition.

   So, we are left with the case $i = n-3$. We have to prove that $(n-3, n-2, n) \in H$. In the case of $n \leq 5$, it is easy to verify that the lemma holds, so we can assume $n > 5$.

But $(n-4,n-2,n-3) = (n-4,n-3,n-2)^2 \in H$, because $(n-4,n-3,n-2) \in H$. Also $(n-5,n-4,n) \in H$, as we already proved. Therefore,

$$(n-2,n-3,n) = (n-4,n-2,n-3)^{(n-5,n-4,n)} \in H.$$

$$(n-3,n-2,n) = (n-2,n-3,n)^2 \in H$$

2. Using Lemma 3.10, we need only prove that each 3–cycle (i,j,k), $i<j<k$, belongs to H.

   If $j = i+1$, $k = i+2$, we are done.

   Otherwise, we know that the 3–cycles $(i,i+1,j),(i,i+1,k) \in H$. So $(i+1,i,j)$, $(i+1,i,k) \in H$ too. Using these two 3–cycles,

$$(i,k,j) = (i+1,i,j)^{(i+1,i,k)} \in H, \text{ and } (i,k,j)^2 = (i,j,k).$$

   Therefore $(i,j,k) \in H$.

This conclude the proof. ∎

Lemma 3.12 *Let n be odd, $n \geq 3$. The cycles $(1,2,3),(1,2,3,\ldots,n)$ together generate A_n.*

Proof: If $n = 3$ we are done. Else, observe that

$$(1,2,3)^{(1,2,3,\ldots,n)} = (2,3,4)$$

and generally,

$$(1,2,3)^{(1,2,3,\ldots,n)^i} = (i+1,i+2,i+3) \text{ for } 1 \leq i \leq n-3.$$

By Lemma 3.11, the 3-cycles $(i+1,i+2,i+3)$ generate A_n. ∎

Lemma 3.13 *Let n be even, $n \geq 4$. The cycles $(1,2,3),(2,3,\ldots,n)$ together generate A_n.*

Proof: We have

$$(1,2,3)^{(2,3,\ldots,n)} = (1,3,4)$$

$$(1,3,4)^{(1,2,3)^2} = (1,3,4)^{(1,3,2)} = (2,4,3)$$

And $(2,3,4) = (2,4,3)^2$ is generated.

By Lemma 3.12, all 3–cycles $(i,i+1,i+2)$, $2 \leq i \leq n-2$, are generated using $(2,3,4),(2,3,\ldots,n)$. The Lemma follows. ∎

Lemma 3.14 *Let n be odd, $n \geq 5$. The cycles $(1,2,3),(3,4,\ldots,n)$ together generate A_n.*

Proof: We have

$$(1,2,3)^{(3,4,\ldots,n)} = (1,2,4)$$
$$(1,3,2)^{(1,2,4)} = (2,3,4)$$

If we look at the cycles $(2,3,4),(3,4,\ldots,n)$ acting on the letters $\{2,\ldots,n\}$, we can use Lemma 3.13 to conclude that these two cycles generate the Alternating group over the points $\{2,\ldots,n\}$. Particularly, all the 3–cycles $(i,i+1,i+2)$, $2 \leq i \leq n-2$, are generated. Thus, the cycles $(1,2,3),(3,4,\ldots,n)$ generate all the 3–cycles $(i,i+1,i+2)$, $1 \leq i \leq n-2$. Using lemma 3.11, we conclude that $(1,2,3),(3,4,\ldots,n)$ generate A_n. ∎

Theorem 3.1 says we can find a complement for any $1 \neq x \in S_n$, except for a very special case. To prove the theorem, we will first find complement for permutations that have special qualities, and use that in the theorem.

But before we proceed to look for complements for every permutation in S_n, it is important to ask if it is necessary. The answer is that we need only to find a complement for one representative of each conjugacy class in S_n. In other words, if a permutation x has a complement y in S_n, such that $\langle x,y\rangle = S_n$, then any permutation z that is of the same type as x can be complemented to a base of S_n.

For the case of A_n, it is not true that a conjugacy class is determined by the type of the permutation. For example, $(1,2,3,4,5)$ and $(1,2,3,5,4)$, are not in the same conjugacy class in A_5. They are only conjugate in S_5.

The following lemma shows conjugacy in S_n is sufficient.

Lemma 3.15 *Let G be S_n or A_n. Let $x \in G$. Let $y \in Cl_{S_n}(x)$. Then x has a complement in G iff y has a complement in G.*

Proof: Let c be a complement to x in G. Since y is conjugate to x in S_n, there exists $z \in S_n$, such that $x^z = y$. Then, because $G \lhd S_n$,

$$G = G^z = \langle x,c\rangle^z = \langle x^z, c^z\rangle = \langle y, c^z\rangle$$

So, c^z is a complement to y. This concludes the proof. ∎

For the case $x = y$, in Lemma 3.15, observe that we can also say something about the quantity of complements for x:

Corollary 3.16 *Let $G = S_n$ or A_n. If $c \in G$, is a complement to $x \in G$. then $\forall z \in C_G(x)$, c^z is also a complement.*

Examples

As we proved earlier, the transposition $(1,2)$ has as a complement in S_5, the cycle $(1,2,3,4,5)$.

1. $(2,3)$ is of the same type as $(1,2)$ and so in the same conjugacy class. They conjugate using $(1,3)$, $(1,2)^{(1,3)} = (2,3)$. Therefore, $(1,2,3,4,5)^{(1,3)} = (1,4,5,3,2)$ is a complement to $(2,3)$.

2. $(3,4) \in C_{S_5}((1,2))$, therefore, $(1,2,3,4,5)^{(3,4)} = (1,2,4,3,5)$ is also a complement for the transposition $(1,2)$ in S_5.

We shall frequently use the following result.

Lemma 3.17 *Let G be a group. Let $x,y,z \in G$ with the following conditions: $x = yz$, $(O(y),O(z)) = 1$, $[y,z] = 1$. Then $y,z \in \langle x \rangle$.*

3.2 Generators of S_n

First we find complements for permutations with special qualities:

Lemma 3.18 *For every cycle $x \in S_n$, there exists a complement $y \in S_n$, such that $\langle x,y \rangle = S_n$.*

Proof: By Lemma 3.15 we can assume that $x = (1,\ldots,k)$, $2 \leq k \leq n$.
We will divide the proof to case analysis:

$k = n$
We simply choose $y = (1,2)$, and use Lemma 3.7.

$k = n-1$
We choose $y = (n-1,n)$ and use Lemma 3.8.

$k = 2$
We choose $y = (1,2,\ldots,n)$ and use Lemma 3.7.

$n-k$ is even and $2 < k < n-1$
We choose $y = (1,2)(k,k+1,\ldots,n)$.

Because $n-k$ is even, the cycle $(k,k+1,\ldots,n)$ has odd order. So $y^{(n-k+1)} = (1,2)$. Also

$$xy = (1,\ldots,k)\cdot(1,2)(k,k+1,\ldots,n) = (2,3,\ldots,k-1,k+1,\ldots,n-1,n,k)$$

By Lemma 3.8 and Corollary 3.16 we have,

$$S_n = \langle (1,2),(2,3,\ldots,k-1,k+1,\ldots,n-1,n,k)\rangle = \langle y^{(n-k+1)},xy\rangle \leq \langle x,y\rangle$$

so, $\langle x,y \rangle = S_n$.

$n-k$ is odd and $2 < k < n-1$
We choose $y = (1,n)(k,k+1,\ldots,n-1)$.

Again, because $n-k$ is odd the cycle $(k, k+1, \ldots, n-1)$ has odd order. So $y^{(n-k)} = (1, n)$. Also

$$\begin{aligned} xy &= (1, \ldots, k) \cdot (1, n)(k, k+1, \ldots, n-1) \\ &= (1, 2, \ldots, k-1, k+1, \ldots, n-1, k, n) \end{aligned}$$

By Lemma 3.7 and Corollary 3.16 we have,

$$S_n = \langle (1, n), (1, 2, \ldots, k-1, k+1, \ldots, n-1, k, n) \rangle = \langle y^{(n-k)}, xy \rangle \leq \langle x, y \rangle$$

so $\langle x, y \rangle = S_n$.

This completes the proof of Lemma 3.18. ∎

Lemma 3.19 *For every permutation $x \in S_n$, of* prime *order $p > 2$, there exists a complement y, such that $\langle x, y \rangle = S_n$.*

Proof: By Lemma 3.15 we can assume that

$$x = (1, 2, \ldots, p)(p+1, \ldots, 2p) \cdots (rp+1, \ldots, (r+1)p) \text{ for } r \geq 0.$$

We use case analysis:

$x = (1, 2, \ldots, p)$
was proved in Lemma 3.18.

$n - p$ is even
We choose $y = (1, 2)\langle p, p+1, \ldots, n \rangle$. Then $y^{n-p+1} = (1, 2)$, and

$$xy^{n-p+1} = x(1, 2) = (2, \ldots, p)(p+1, \ldots, 2p) \cdots \langle rp+1, \ldots, \langle r+1)p)$$

As the cycle $\langle 2, \ldots, p)$ is of even order, $p-1$, we have

$$(\, x(1, 2)\,)^{p-1} = (\, (p+1, \ldots, 2p) \cdots (rp+1, \ldots, (r+1)p)\,)^{p-1}$$

Thus,

$$x\,(x(1, 2))^{p-1} = \langle 1, \ldots, p)$$

We conclude using the case analysis in Lemma 3.18,

$$S_n = \langle (1, \ldots, p), y \rangle \leq \langle x, y \rangle.$$

$n - p$ is odd and $(r+1)p < n$

We choose $y = (1,n)(p,\ldots,n-1)$. Then $y^{n-p} = (1,n)$.

$$\begin{aligned} x(1,n) &= (1,2,\ldots,p,n)(p+1,\ldots,2p)\cdots(rp+1,\ldots,(r+1)p) \\ \text{By Lemma 3.17,} \quad & (1,2\ldots,p,n),(p+1,\ldots,2p)\cdots(rp+1,(r+1)p) \in \langle x(1,n)\rangle. \\ \text{Thus,} \quad & (1,\ldots,p) \in \langle x,y\rangle \end{aligned}$$

Using the case analysis in Lemma 3.18,

$$S_n = \langle (1,\ldots,p), y\rangle \leq \langle x,y\rangle.$$

$n - p$ is odd and $(r+1)p = n$

We choose $y = (1,2)(p,\ldots,n-1)$. Then $y^{n-p} = (1,2)$.

As in the previous cases it is easy to see that $(1,\ldots,p) \in \langle x,y\rangle$. This time we can only use Lemma 3.18 to conclude that,

$$S_{n-1} = \langle (1,\ldots,p)\,,\,(1,2)(p,\ldots,n-1)\rangle \leq \langle x,y\rangle.$$

But since S_{n-1} is maximal in S_n and $x \notin S_{n-1}$ (it moves the point $\{n\}$), we can conclude that $\langle x,y\rangle = S_n$.

Lemma 3.19 follows. ∎

In the next Lemma, which deals with the case of a permutation of order two, we can see that the special case of the conjugacy class of $(1,2)(3,4)$ in S_4 is not covered. Indeed, as we stated before, in this special case, a complement does not exist.

Lemma 3.20 *For every permutation $x \in S_n$ of order two, there is a complement y, except for the case $n = 4$, and x is a member of the* Klein subgroup.

Proof: By Lemma 3.15 we can assume $x = (1,2)(3,4)\cdots(k,k+1)$. As in the previous Lemma, we use case analysis. We can assume $n \geq 4$.

$x = (1,2)$

was proved in Lemma 3.18.

n odd and $k \geq 3$

We choose $y = (1,n)(2,3,\ldots,n-1)$.

$$\begin{aligned} y^{n-1} &= (2,3,\ldots,n-1) \\ y^{n-2} &= (1,n) \\ xy^{n-2} &= (1,2)(3,4)\cdots(k,k+1)\cdot(1,n) = (1,2,n)(3,4)\cdots(k,k+1) \\ \text{so,} & \\ (xy^{n-2})^3 &= (3,4)\cdots(k,k+1). \\ \text{Thus,} & \\ (1,2) &= x\cdot(3,4)\cdots(k,k+1) \in \langle x,y\rangle. \\ S_{n-1} &= \langle (1,2),(2,3,\ldots,n-1)\rangle \leq \langle x,y\rangle \end{aligned}$$

Finally, since $(1,n) \in \langle x,y \rangle$, we have by lemma 3.8,

$$S_n = \langle (1,n), (1,2,\ldots,n-1) \rangle \leq \langle x,y \rangle$$

n even and $3 \leq k \leq n-3$

For $3 \leq k \leq n-3$ we must have $n \geq 6$. We choose $y = (1,n)(2,4,\ldots,n-1)$.

$$\begin{aligned} y^{n-3} &= (1,n) \\ y^{n-2} &= \langle 2,4,\ldots,n-1) \\ xy^{n-3} &= \langle 1,2,n)\langle 3,4)\cdots\langle k,k+1) \\ \langle xy^{n-3})^3 &= \langle 3,4)\cdots\langle k,k+1) \end{aligned}$$

So, as in the previous case, $(1,2) \in \langle x,y \rangle$.

We will show now how we can "climb" from S_{n-2} to S_n using the permutations we know that are in $\langle x,y \rangle$.

By Lemma 3.8, $\langle (1,2), (2,4,\ldots,n-1) \rangle \cong S_{n-2}$. Thus $(1,2,4,\ldots,n-1) \in \langle x,y \rangle$.

As $(1,n), (1,2,4,\ldots,n-1) \in \langle x,y \rangle$, again using Lemma 3.8, they generate a subgroup of $\langle x,y \rangle$ which is isomorphic to S_{n-1}, over the points $\{1,2,4,\ldots,n\}$.

But, as x moves the point $\{3\}$, and S_{n-1} is maximal in S_n, we have, $\langle x,y \rangle = S_n$.

Finally, to complete the proof of the Lemma:

n even, $n > 4$ and $k = n-1$

We choose $y = (1,n-1)(2,3,\ldots,n-2)$.

Observe that in the case $n = 4$, this choice degenerates to $y = (1,3)$, which is why the proof does not hold for $x = (1,2)(3,4)$ in S_4.

$$\begin{aligned} y^{n-3} &= (1,n-1) \\ y^{n-2} &= (2,3,\ldots,n-2) \\ xy^{n-3} &= (1,2)(3,4)\cdots(n-1,n)\cdot(1,n-1) \\ &= (1,2,n-1,n)(3,4)\cdots(n-3,n-2) \\ (xy^{n-3})^2 &= (1,n-1)(2,n) \end{aligned}$$

Thus, $(2,n) = (1,n-1)\cdot(1,n-1)(2,n) \in \langle x,y \rangle$.

From the above calculation, and by Lemma 3.8, the group generated by $(2,n)$, $(2,3,\ldots,n-2)$, over the points $\{2,3,\ldots,n-2,n\}$, is isomorphic to S_{n-2}, and is in $\langle x,y \rangle$.

From the above we know

$$(3,4)(5,6)\cdots(n-3,n-2)\ ,\ (2,3) \in \langle x,y\rangle$$
$$x(3,4)(5,6)\cdots(n-3,n-2) = (1,2)(n-1,n)$$
$$(1,2)(n-1,n)\cdot(2,3) = (1,3,2)(n-1,n).$$
Thus $(n-1,n) \in \langle x,y\rangle$

As in previous cases, we can use the transposition $(n-1,n)$ to "climb" to a group isomorphic to S_{n-1}. We have seen that

$$(2,3,\ldots,n-2,n),(n-1,n) \in (x,y)$$

By Lemma 3.8 these permutations generate the symmetric group over the points $\{2,3,\ldots,n\}$. As x moves the point $\{1\}$, and S_{n-1} is maximal in S_n, we can complete the "climbing" process and conclude $\langle x,y\rangle = S_n$.

This conclude the proof of the Lemma. ∎

Using our previous results, we can now prove Theorem 3.1.

Proof of Theorem 3.1: Let $x \in S_n$, $x \neq 1$. It is obvious that there exists an integer $m \geq 1$, such that, x^m is of prime order. Unless x is a member of the Klein subgroup in the case $n = 4$, we can use Lemmas 3.19 and 3.20 to explicitly find y, a complement to x^m in S_n.

Since $\langle x^m,y\rangle \leq \langle x,y\rangle$, the theorem follows. ∎

3.3 Generators of A_n

We now turn to the case of A_n. To prove theorem 3.2, we again prove first a series of Lemmas. The Lemmas constructively find complements for permutations in A_n, with special qualities. Specifically, we again find complements for cycles, and then for permutations of prime order. Then, we use these results, as in Theorem 3.1, to prove Theorem 3.2.

Lemma 3.21 *For every cycle $x \in A_n$, there exists a complement $y \in A_n$, such that $\langle x,y\rangle = A_n$.*

Proof: By Lemma 3.15 we can assume, $x = (1,\ldots,k)$ $3 \leq k \leq n$, k odd.

We now turn to case analysis:

$k = n$ (n is odd)

We choose $y = (1,2,3\rangle$ and use Lemma 3.12.

$k = n-1$ (n is even)

We choose $y = (n-2,n-1,n)$ and use Lemma 3.13.

$k = 3$

Similarly to the previous cases we can choose, $y = (1, 2, \ldots, n)$ for n odd, or $y = (2, 3, \ldots, n)$ for n even.

n odd ($n - k$ is even), $n - k \not\equiv 2 \pmod 3$ and $5 \leq k \leq n - 2$

We choose $y = (1, 2, 3)(k, \ldots, n)$.

First we observe that $y \in A_n$, as a product of two disjoint cycles of odd lengths. By Lemma 3.17, $(1, 2, 3), (k, \ldots, n) \in \langle y \rangle$. We have by Lemma 3.12, $A_k = \langle x, (1, 2, 3) \rangle = \langle (1, \ldots, k), (1, 2, 3) \rangle \leq \langle x, y \rangle$.

Particularly all the cycles $\langle i, i + 1, i + 2 \rangle$, $1 \leq i \leq k - 2$, are in $\langle x, y \rangle$.

In particular $(k - 2, k - 1, k) \in \langle x, y \rangle$. So

$$\langle (k - 2, k - 1, k), (k, \ldots, n) \rangle \leq \langle x, y \rangle$$

and by Lemma 3.14 this group is isomorphic to A_{n-k+3}. Thus, all the cycles $(i, i + 1, i + 2)$, $k - 2 \leq i \leq n - 2$, are in $\langle x, y \rangle$.

Using Lemma 3.11 we conclude that $\langle x, y \rangle = A_n$.

$n = 7$ and $k = 5$

We choose $y = (1, 6, 7)$. By Lemma 3.14, $\langle x, y \rangle = A_7$.

n odd ($n - k$ is even), $n - k \equiv 2 \pmod 3$, $n \geq 9$ and $5 \leq k \leq n - 2$

We choose $y = (1, n - 1, n)(k, k + 1, \ldots, n - 2)$.

Observe that $y \in A_n$, as a product of two disjoint cycles of odd length.

As $O((k, k + 1, \ldots, n - 2)) = n - k - 1 \equiv 1 \pmod 3$, by Lemma 3.17,

$$(1, n - 1, n), (k, k + 1, \ldots, n - 2) \in \langle y \rangle.$$

Therefore the group $\langle x, (1, n - 1, n) \rangle = \langle (1, 2, \ldots, k), (1, n - 1, n) \rangle \leq \langle x, y \rangle$, and by Lemma 3.14 is isomorphic to A_{k+2}.

Particularly, $\langle k, n - 1, n \rangle \in \langle x, y \rangle$, so the group generated by $\langle k, n - 1, n \rangle$ and $(k, k + 1, \ldots, n - 2)$ is in $\langle x, y \rangle$, and by lemma 3.14 isomorphic to A_{n-k+1}.

By rewriting the points $\{1, \ldots, n\}$, in the form $\{1, \ldots, k, n - 1, n, k + 1, \ldots, n - 2\}$ we see that as all the cycles $(i, i + 1, i + 2)$, $1 \leq i \leq n - 2$, are in $\langle x, y \rangle$. So again, using Lemma 3.11 we have, $\langle x, y \rangle = A_n$.

n even ($n - k$ is odd), $n - k \not\equiv 0 \pmod 3$ and $5 \leq k \leq n - 3$

We choose $y = (1, 2, n)(k, \ldots, n - 1)$.

Observe $y \in A_n$ because it is a product of two disjoint cycles of odd length. As $O((k, \ldots, n-1)) = n - k \not\equiv 0 \pmod 3$, By Lemma 3.17, $(1, 2, n)$, $(k, \ldots, n - 1) \in \langle y \rangle$.

The group $\langle x, (1,2,n)\rangle \cong A_{k+1}$, by lemma 3.13. Particularly, the cycle $(k-1,k,n) \in \langle x,y\rangle$, so $\langle (k-1,k,n),(k,\ldots,n)\rangle \leq \langle x,y\rangle$, which by lemma 3.14 is isomorphic to A_{n-k+2}.

By rewriting the points $\{1,\ldots,n\}$ and using similar arguments as in the previous case, $\langle x,y\rangle = A_n$.

n even ($n-k$ is odd), $n-k \equiv 0 \pmod 3$ and $5 \leq k \leq n-3$

We choose $y = (1,2,3)(k-1,k,\ldots,n)$.

Observe $y \in A_n$ as it is a product of two disjoint cycles of odd length.

As $O((k-1,k,\ldots,n))= n-k+2 \equiv 2 \pmod 3$, By Lemma 3.17,

$$(1,2,3),(k-1,k,\ldots,n) \in \langle y\rangle.$$

By Lemma 3.12, $\langle (1,2,3),x\rangle = \langle (1,2,3),(1,\ldots,k)\rangle = A_k$, so $A_k \leq \langle x,y\rangle$. Particularly, $(k-2,k-1,k) \in \langle x,y\rangle$.

This means that $\langle (k-2,k-1,k),(k-1,k,\ldots,n)\rangle \leq \langle x,y\rangle$ and by Lemma 3.12 $\langle (k-2,k-1,k),(k-1,k,\ldots,n)\rangle \cong A_{n-k+3}$.

Thus, all the cycles $(i,i+1,i+2)$, $1 \leq i \leq n-2$ are in $\langle x,y\rangle$, and using Lemma 3.11, $\langle x,y\rangle = A_n$.

The Lemma follows. ∎

Lemma 3.22 *For every permutation $x \in A_n$ of prime order $p > 3$, there exists a complement $y \in A_n$, such that $\langle x,y\rangle = A_n$.*

Proof: By Lemma 3.15 we can assume

$$x = (1,2,\ldots,p)(p+1,\ldots,2p)(rp+1,\ldots,(r+1)p), \text{ for } r \geq 0$$

Again we use case analysis.

$x = (1,\ldots,p)$.

Was proved in Lemma 3.21.

n odd ($n-p$ is even) and $n-p \not\equiv 2 \pmod 3$.

We choose $y = (1,2,3)(p,\ldots,n)$.

By Lemma 3.17, $(1,2,3),(p,\ldots,n) \in \langle y\rangle$.

$$\begin{aligned} x(1,2,3)^2 &= x(1,3,2) \\ &= (1,2,\ldots,p)\cdot(1,3,2)\cdot(p+1,\ldots,2p)\cdots(rp+1,\ldots,(r+1)p) \\ &= (3,4,\ldots,p)(p+1,\ldots,2p)\cdots(rp+1,\ldots,(r+1)p) \end{aligned}$$

By Lemma 3.17,

$$(3,4,\ldots,p),(p+1,\ldots,2p)\cdots(rp+1,\ldots,(r+1)p)\rangle \in \langle x(1,2,3)^2\rangle.$$

So, $(1,\ldots,p) \in \langle x,y\rangle$.

Using the case analysis of Lemma 3.21,

$$A_n = \langle (1,\ldots,p), y\rangle \leq \langle x, y\rangle.$$

n odd ($n-p$ is even), $n-p \equiv 2 \pmod 3$ and $(r+1)p \leq n-2$

We choose $y = (1,n-1,n)(p,\ldots,n-2)$.

By Lemma 3.17, $(1,n-1,n),(p,\ldots,n-2) \in \langle y\rangle$

$$\begin{aligned} x(1,n-1,n) &= (1,2,\ldots,p)\cdot(1,n-1,n)\cdot(p+1,\ldots,2p)\cdots(rp+1,\ldots,(r+1)p) \\ &= (1,2,\ldots,p,n-1,n)(p+1,\ldots,2p)\cdots(rp+1,\ldots,(r+1)p) \end{aligned}$$

By Lemma 3.17,

$$(1,2,\ldots,p,n-1,n),(p+1,\ldots,2p)\cdots(rp+1,\ldots,(r+1)p) \in \langle x(1,2,3)^2\rangle.$$

So, $(1,\ldots,p) \in \langle x, y\rangle$.

Using the case analysis of Lemma 3.21,

$$A_n = \langle (1,\ldots,p),(1,n-1,n)(p,\ldots,n-2)\rangle \leq \langle x, y\rangle$$

n odd ($n-p$ is even), $n-p \equiv 2 \pmod 3$ and $(r+1)p = n-1$

We choose $y = (1,2,n)(p,\ldots,n-2)$.

By Lemma 3.17, $(1,2,n),(p,\ldots,n-2) \in \langle y\rangle$

$$\begin{aligned} x(1,2,n) &= (1,2,\ldots,p)\cdot(1,2,n)\cdot(p+1,\ldots,2p)\cdots(n-p-1,\ldots,n-1) \\ &= (1,n)(2,3,\ldots,p)(p+1,\ldots,2p)\cdots(n-p-1,\ldots,n-1) \\ (x(1,2,n))^{p-1} &= (\,(p+1,\ldots,2p)\cdots(n-p-1,\ldots,n-1)\,)^{-1} \end{aligned}$$

Thus, $(1,\ldots,p) \in \langle x, y\rangle$.

$\langle (1,2,n),(1,\ldots,p)\rangle$ is a group isomorphic to A_{p+1} by Lemma 3.13.

In particular $(p-2,p-1,p) \in \langle x, y\rangle$, so the group $\langle (p-2,p-1,p),(p,\ldots,n-2)\rangle$, which by Lemma 3.14 is isomorphic to A_{n-p+1}, is in $\langle x, y\rangle$. By rewriting the points $\{1,2,\ldots,n-2,n\}$ and using lemma 3.11, it is easy to see that the Alternating group over the points $\{1,2,\ldots,n-2,n\}$ is in $\langle x, y\rangle$.

To complete the proof of this case we use the fact that x moves the point $\{n-1\}$. The cycle $(n-p-1,\ldots,n-1) \in \langle x, y\rangle$, because

$$(n-p-1,\ldots,n-1) = x((1,\ldots,p)\cdots((r-1)p+1,\ldots,rp))^{-1}.$$

We can use the cycles $(n-p-1,n-p,n-p+1),(n-p-1,\ldots,n-1)$ to generate the Alternating group over $\{n-p-1,\ldots,n-1\}$. In particular $(n-3,n-2,n-1) \in \langle x, y\rangle$, and because n is odd, by Lemma 3.14

$$A_n = \langle (n-3,n-2,n-1),(1,n,2,\ldots,n-3)\rangle \leq \langle x, y\rangle$$

n odd ($n-p$ is even), $n-p \equiv 2 \pmod 3$ and $(r+1)p = n$

We choose $y = (1,2,3)(p,\ldots,n-2\rangle$.

Again, $(1,2,3),(p,\ldots,n-2) \in \langle y\rangle$.

$$\begin{aligned} x(1,2,3)^2 &= x(1,3,2) \\ &= (1,2,\ldots,p)\cdot(1,3,2)\cdot(p+1,\ldots,2p)\cdots(n-p,\ldots,n\rangle \\ &= (3,4,\ldots,p)(p+1,\ldots,2p\rangle\cdots(n-p,\ldots,n) \\ \text{By Lemma 3.17,}\quad & (3,4,\ldots,p),(p+1,\ldots,2p\rangle\cdots(n-p,\ldots,n) \in \langle x(1,2,3)^2\rangle. \\ \text{Thus,}\quad & (1,\ldots,p) \in \langle x,y\rangle. \end{aligned}$$

$(1,2,3)$ together with $(1,\ldots,p)$ generate $A_p \leq \langle x,y\rangle$. As in the previous case, using $(p-2,p-1,p)$, $(p,\ldots,n-2) \in \langle x,y\rangle$ it is easy to see, $A_{n-2} \leq \langle x,y\rangle$.

Using the fact that x moves the points $\{n-1,n\}$, and applying similar arguments to those of the previous case, $\langle x,y\rangle = A_n$.

n even ($n-p$ is odd), $n-p \not\equiv 0 \pmod 3$ and $(r+1)p < n$.

We choose $y = (1,2,n)(p,\ldots,n-1)$.

Again, $(1,2,n),(p,\ldots,n-1) \in \langle y\rangle$.

$$\begin{aligned} x(1,2,n\rangle &= (1,2,\ldots,p\rangle\cdot(1,2,n)\cdot(p+1,\ldots,2p)\cdots(rp+1,\ldots,(r+1)p) \\ &= (1,n)(2,3,\ldots,p\rangle(p+1,\ldots,2p\rangle\cdots(rp+1,\ldots,(r+1)p\rangle \\ (x(1,2,n)\rangle)^{p-1} &= (p+1,\ldots,2p\rangle\cdots(rp+1,\ldots,(r+1)p)^{-1} \\ \text{Thus,}\quad & (1,\ldots,p) \in \langle x,y\rangle. \end{aligned}$$

As in the previous cases using the cycles $(1,2,n\rangle,(1,\ldots,p\rangle,(p,\ldots,n-1) \in \langle x,y\rangle$, we can generate the Alternating groups over the points $\{1,\ldots,p,n\}$ and $\{p-2,\ldots,n-1\}$, use rewriting of points and Lemma 3.11 to conclude,

$$\langle x,y\rangle = A_n.$$

n even ($n-p$ is odd), $n-p \not\equiv 0 \pmod 3$ and $(r+1)p = n$

We choose $y = (1,2,3)(p,\ldots,n-1)$

Again, $(1,2,3),(p,\ldots,n-1) \in \langle y\rangle$.

$$\begin{aligned} x(1,2,3\rangle^2 &= x(1,3,2\rangle \\ &= (1,2,\ldots,p)\cdot(1,3,2)\cdot(p+1,\ldots,2p)\cdots(n-p,\ldots,n) \\ &= (3,4,\ldots,p\rangle(p+1,\ldots,2p\rangle\cdots(n-p,\ldots,n) \\ \text{By Lemma 3.17,}\quad & (3,4,\ldots,p\rangle,(p+1,\ldots,2p\rangle\cdots(n-p,\ldots,n) \in \langle x(1,2,3)^2\rangle. \\ \text{Thus,}\quad & (1,\ldots,p) \in \langle x,y\rangle. \end{aligned}$$

Using the cycles $(1,2,3),(1,\ldots,p),(p,\ldots,n-1) \in \langle x,y\rangle$, it is easy to see that $A_{n-1} \leq \langle x,y\rangle$.

It is easy to see that the last cycle of x, $(n-p,\ldots,n)$, belongs to $\langle x,y\rangle$. As the cycle $(n-p,n-p+1,n-p+2)$ belongs to $\langle x,y\rangle$, using Lemma 3.12, $(n-2,n-1,n) \in \langle x,y\rangle$.

Lastly, as n is even, by Lemma 3.13,

$$A_n = \langle (1,\ldots,n-1),(n-2,n-1,n)\rangle \leq \langle x,y\rangle.$$

This completes the case analysis, and concludes the proof. ∎

Lemma 3.23 *For every permutation $x \in A_n$ of order two, there exists a complement y, $y \in A_n$, such that $\langle x,y\rangle = A_n$.*

Proof: By Lemma 3.15 we can assume $x = (1,2)(3,4)\cdots(k,k+1)$ for $3 \leq k \leq n-1$.

Again we use case analysis:

$x = (1,2)(3,4)$ and $n = 4$

We choose $y = (1,2,3)$.

$$\begin{aligned} xy &= (1,3,4) \\ xy^2 &= (2,3,4) \end{aligned}$$

By Lemma 3.13 $A_4 = \langle (1,2,3),(2,3,4)\rangle$. Thus, $\langle x,y\rangle = A_4$.

n even, $n \geq 6$ and $n \not\equiv 0 \pmod 3$

We choose $y = (1,2,3)(4,\ldots,n)$. Observe $(1,2,3),(4,\ldots,n) \in \langle y\rangle$.

If $k \geq 7$ then,

$$\begin{aligned} x\cdot(1,2,3) &= (1,2)(3,4)\cdot(1,2,3)\cdot(5,6)\cdots(k,k+1) \\ &= (1,3,4)(5,6)\cdots(k,k+1) \end{aligned}$$

So for all $k \geq 3$ $(1,2)(3,4)$, $(1,3,4) \in \langle x,y\rangle$. As $(1,2)(3,4)\cdot(1,3,4) = (1,2,3)$, using the arguments of the last case, $A_4 \leq \langle x,y\rangle$.

Using previous methods, it is easy to see $A_n = \langle A_4,(4,\ldots,n)\rangle$. Thus, $\langle x,y\rangle = A_n$.

n even, $n \geq 6$, $n \equiv 0 \pmod 3$ and $k = 3$

We choose $y = (2,\ldots,n)$.

$$\begin{aligned} x^y &= (1,2)(3,4)^{(2,\ldots,n)} = (1,3)(4,5) \\ x^{(1,3)(4,5)} &= (1,2)(3,4)^{(1,3)(4,5)} = (1,5)(2,3) \\ x^{y^{-1}} &= (1,2)(3,4)^{(2,n,n-1,\ldots,3)} = (1,n)(2,3) \\ \text{Thus,}\quad & (1,5)(2,3)\cdot(1,n)(2,3) = (1,5,n) \in \langle x,y\rangle \\ (1,5,n)^x &= (1,5,n)^{(1,2)(3,4)} = (2,5,n) \end{aligned}$$

By Lemma 3.13, $H = \langle (1,5,n),(2,5,n)\rangle$ is a group isomorphic to A_4, over the points $\{1,2,5,n\}$. In particular $(1,5)(2,n) \in H$:

$$(1,5)(2,3)\cdot(1,5)(2,n) = (2,3,n) \in \langle x,y\rangle.$$

$H_1 = \langle H,(2,3,n)\rangle$, is a group isomorphic to A_5, over the points $\{1,2,3,5,n\}$, and $H_1 \leq \langle x,y\rangle$. Using previous methods it is easy to see
$A_n = \langle H_1,(2,\ldots,n)\rangle$. Thus, $\langle x,y\rangle = A_n$.

n even, $n \geq 6$, $n \equiv 0 \pmod 3$ and $k \geq 7$

We choose $y = (1,3,5)(6,\ldots,n)$. Observe $(1,3,5),(6,\ldots,n) \in \langle y\rangle$.

As $k \geq 7$,

$$\begin{aligned} x\cdot(1,3,5) &= (1,2)(3,4)(5,6)\cdot(1,3,5)\cdot(7,8)\cdots(k,k+1) \\ &= (1,2,3,4,5,6)(7,8)\cdots(k,k+1) \\ (x\cdot(1,3,5))^2 &= (1,3,5)(2,4,6). \\ \text{Thus} \quad & (2,4,6) \in \langle x,y\rangle. \end{aligned}$$

$H = \langle (2,4,6),(6,\ldots,n)\rangle$ is a group isomorphic to A_{n-3}, over the points $\{2,4,6,\ldots,n\}$.

As in previous cases, we start a "climbing" process from H to A_n.

$(6,7,8) \in H$. Also $(1,2)(3,4)(5,6)(7,8) \in \langle x,y\rangle$, as it can be written as product of x and a permutation of order two in H. We have,

$$(1,2)(3,4)(5,6)(7,8)\cdot(6,7,8) = (1,2)(3,4)(5,7,6).$$

Thus $(5,6,7) \in \langle x,y\rangle$, and so $H_1 = \langle H,(5,6,7)\rangle$ which is isomorphic to A_{n-2} over the points $\{2,4,5,\ldots,n\}$, is in $\langle x,y\rangle$. It is easy to see that $A_n = \langle H_1,x\rangle$. Thus, $\langle x,y\rangle = A_n$.

n odd

Remark As we stated before, there are usually many complements to a given permutation. Up to this point in the proof, for a given permutation $x \in A_n$, we chose a complement of a particular type. Namely, the complement was composed of two disjoint cycles, one of length three and the other of length l, with conditions: $l \equiv 1 \pmod 2$, $l \not\equiv 0 \pmod 3$. Thus, we were always able to "separate" these two cycle, and show that together with x, they generate A_n. In the case x of order two and n odd there are sometimes no such complements. For example, in the case $x = (1,2)(3,4)$ and $n = 7$, all the complements are of two types: 7–cycles or products of 2–cycle by a 5–cycle.

We choose $y = (1,\ldots,n)$.

We argue $(1,2,n) \in \langle x,y\rangle$. If so, then by Lemma 3.12,

$$A_n = \langle (1,2,n),(1,\ldots,n)\rangle \leq \langle x,y\rangle.$$

Let m be the unique minimal integer such that,

$$x^{y^{2m}} = ((1,2)\cdots(k,k+1))^{(1,\ldots,n)^{2m}} = (n-k+1, n-k+2)\cdots(n-2,n-1)(n,1)$$

Then it is easy to see,

$$\prod_{i=0}^{m} x^{y^{2i}} = (1,2)\cdot(1,n)\cdot z$$

Where z is a permutation of order two over the points $\{3,\ldots,n-1\}$.

Example

$x = (1,2)(3,4)(5,6)(7,8), \quad n = 11.$

$$\begin{aligned} x^{y^2} &= (3,4)(5,6)(7,8)(9,10) \\ x^{y^4} &= (5,6)(7,8)(9,10)(11,1) \end{aligned}$$

Thus $m = 2$ and,

$$x \cdot x^{y^2} \cdot x^{y^4} = (1,2)\cdot(1,11)\cdot(5,6)(7,8)$$

So for this example $z = (5,6)(7,8)$.

From the above it is obvious that

$$\left(\prod_{i=0}^{m} x^{y^{2i}}\right)^4 = (1,2,n)$$

This completes the proof of this case, and the proof of the Lemma.

∎

Lemma 3.24 *For every permutation $x \in A_n$ of order three there exists a complement y, $y \in A_n$, such that $\langle x, y\rangle = A_n$.*

Proof: By Lemma 3.15 we can assume $x = (1,2,3)\cdots(k,k+1,k+2)$ $1 \le k \le n-2$.

Again we use use case analysis:

$\boldsymbol{x = (1,2,3)}$

This case was proved in Lemma 3.21.

$\boldsymbol{n < 6}$

In this case the only possibility is $x = (1,2,3)$.

n is even, $n \geq 6$ and $n \not\equiv 0 \pmod 3$

We choose $y = (1,2,4)(3,5,\ldots,n)$.

Observe $(1,2,4), (3,5,\ldots,n) \in \langle y \rangle$.

If $k \geq 7$ then,

$$\begin{aligned} x(1,2,4) &= (1,2,3)(4,5,6)\cdot(1,2,4)\cdot(7,8,9)\cdots(k,k+1,k+2) \\ &= (1,2,4,5,6)(7,8,9)\cdots(k,k+1,k+2). \\ \text{Thus, } \langle x(1,2,4)\rangle^5 &= \langle (7,8,9)\cdots(k,k+1,k+2)\rangle^{-1} \end{aligned}$$

So for all $k \geq 4$, $(1,2,3)(4,5,6) \in \langle x,y \rangle$.

$$(1,2,4)^{(1,2,3)(4,5,6)} = (2,3,5).$$

By Lemma 3.14, $\langle (1,2,4),(2,3,5)\rangle = A_5 \leq \langle x,y\rangle$. Using previous methods it is easy to see that $A_n = \langle A_5, (3,5,\ldots,n)\rangle$. Thus $\langle x,y\rangle = A_n$.

n is even, $n \geq 6$, $n \equiv 0 \pmod 3$ and $k < n-2$

We choose $y = (1,4,n)(5,\ldots,n-1)$.

Observe $(1,4,n), (5,\ldots,n-1) \in \langle y \rangle$.

If $k \geq 7$ then,

$$\begin{aligned} x(1,4,n) &= (1,2,3)(4,5,6)\cdot(1,4,n)\cdot(7,8,9)\cdots(k,k+1,k+2) \\ &= (1,2,3,4,5,6,n)(7,8,9)\cdots(k,k+1,k+2) \\ \langle x(1,4,n)\rangle^7 &= (7,8,9)\cdots\langle k,k+1,k+2). \end{aligned}$$

So for all $k \geq 4$, $(1,2,3)(4,5,6) \in \langle x,y\rangle$.

$$(1,4,n)^{(1,2,3)(4,5,6)} = (2,5,n).$$

Using previous methods, it is easy to see that

$$A_n = \langle (1,4,n),(2,5,n),(5,\ldots,n-1),(1,2,3)(4,5,6)\rangle.$$

Thus $\langle x,y\rangle = A_n$.

n is even, $n \geq 6$, $n \equiv 0 \pmod 3$ and $k = n-2$

We choose $y = (1,3,4)(5,\ldots,n-1)$.

Observe $(1,3,4), (5,\ldots,n-1) \in \langle y \rangle$.

If $k \geq 7$ then,

$$\begin{aligned} x(1,3,4) &= (1,2,3)(4,5,6)\cdot(1,3,4)\cdot(7,8,9)\cdots(k,k+1,k+2) \\ &= (1,2,4,5,6)(7,8,9)\cdots(k,k+1,k+2). \\ \langle x(1,3,4)\rangle^5 &= ((7,8,9)\cdots\langle k,k+1,k+2)\rangle^{-1}. \end{aligned}$$

So for all $k \geq 4$, $(1,2,3)(4,5,6) \in \langle x, y \rangle$.

$$(1,3,4)^{(1,2,3)(4,5,6)} = (1,5,2).$$

Using Lemma 3.14 twice we have,

$$H = \langle (1,5,2), (5,\ldots,n-1) \rangle \cong A_{n-3}$$

and $A_{n-1} = \langle (1,3,4), H \rangle \leq \langle x, y \rangle$. As the last cycle in the decomposition of x is $(n-2, n-1, n)$ we conclude $A_n = \langle x, y \rangle$.

n is odd, $n \geq 7$ and $n \not\equiv 1 \pmod 3$

We choose $y = (1,2,4)(5,\ldots,n)$.

Observe $(1,2,4), (5,\ldots,n) \in \langle y \rangle$.

By the same analysis of the case "n is even and $n \not\equiv 0 \pmod 3$" $A_5 \leq \langle x, y \rangle$.

Using previous methods it is easy to see $A_n = \langle A_5, (5,\ldots,n) \rangle$. Thus, $\langle x, y \rangle = A_n$.

$n = 7$

In this case the only possibility is $x = (1,2,3)(4,5,6)$. We choose $y = (1,4,7)$.

$$y^x = (1,4,7)^{(1,2,3)(4,5,6)} = (2,5,7)$$

$H = \langle (1,4,7), (2,5,7) \rangle$ is the Alternating group over the points $\{1,2,4,5,7\}$. In particular $(1,2,4) \in \langle x, y \rangle$.

$$(1,2,4)^{(1,2,3)(4,5,6)} = (2,3,5).$$

$H_1 = \langle H, (2,3,5) \rangle$ is the Alternating group over the points $\{2,\ldots,7\}$. Again, it is easy to see that $A_7 = \langle H_1, x \rangle$. Thus $\langle x, y \rangle = A_7$.

n is odd, $n > 7$, $n \equiv 1 \pmod 3$ and $k < n-2$

We choose $y = (1,4,n)(6,\ldots,n)$.

Observe $(1,4,n), (6,\ldots,n) \in \langle y \rangle$.

Using similar analysis to the case "n is even, $n \equiv 0 \pmod 3$ and $k < n-2$" we can conclude $\langle x, y \rangle = A_n$.

n is odd, $n > 7$, $n \equiv 1 \pmod 3$ and $k = n-2$

We choose $y = (1,3,4)(6,\ldots,n-1)$.

Observe $(1,3,4), (6,\ldots,n-1) \in \langle y \rangle$.

$$\begin{aligned}
x(1,3,4) &= (1,2,3)(4,5,6) \cdot (1,3,4) \cdot (7,8,9) \cdots (k,k+1,k+2) \\
&= (1,2,4,5,6)(7,8,9) \cdots (k,k+1,k+2) \\
(x(1,3,4))^5 &= ((7,8,9) \cdots (k,k+1,k+2))^{-1}. \\
\text{Thus} \quad & (1,2,3)(4,5,6) \in \langle x, y \rangle. \\
(1,3,4)^{(1,2,3)(4,5,6)} &= (1,5,2).
\end{aligned}$$

By Lemma 3.14, $A_5 = \langle (1,3,4),(1,5,2)\rangle \leq \langle x,y\rangle$. Using previous results it is easy to see that $A_6 = \langle (1,2,3)(4,5,6), A_5\rangle$ and $A_{n-1} = \langle A_6, (,\ldots,n-1)\rangle \leq \langle x,y\rangle$.

As the last cycle in the decomposition of x is $(n-2,n-1,n)$ we conclude, $\langle x,y\rangle = A_n$.

This concludes the proof. ∎

Using our previous results, we are now able to prove Theorem 3.2.

Proof of Theorem 3.2: Let $x \in A_n$, $x \neq 1$. As in Theorem 3.1, there exists an integer $m \geq 1$ such that x^m is of prime order. Using Lemmas 3.22, 3.23 and 3.24 we can find explicitly $y \in A_n$ which is a complement to x^m.

Since $\langle x^m, y\rangle \leq \langle x,y\rangle$, the theorem follows. ∎

3.4 Complements of transpositions

Up until now we concentrated on the existence of complements. As a simple example we shall now show explicitly all the complements of one particular conjugacy class of S_n, the class of transpositions.

First, a few definitions and general results. Throughout these preliminaries, G is a finite permutation group, $|G| > 1$, acting on a set X, $|X| \geq 2$.

Transitivity. G is said to be transitive if for any two points $x,y \in X$, there exists a permutation $\pi \in G$, such that $x\pi = y$. ($x\pi$ means π acting on x).

From this point on, we also require of G to be transitive (on X).

Domain of imprimitivity. A subset $Y \subset X$, $|Y| \geq 2$, is called a domain of imprimitivity of G, if for every permutation $\pi \in G$, either $Y\pi = Y$ or $Y\pi \cap Y = \emptyset$.

Primitive group. G is primitive if it possess *no* domain of imprimitivity.

Lemma 3.25 *$S_n(A_n)$ is primitive for all $n \geq 1$.*

Proof: The case of $n \leq 2$ is trivial. It is easy to verify that for $n \geq 3$ $S_n(A_n)$ is transitive. Suppose by contradiction there exists a subset $Y \subset \{1,\ldots,n\}$, $|Y| \geq 2$, which is a domain of imprimitivity of $S_n(A_n)$. Let $x \in \{1,\ldots,n\}\setminus Y$, $y,z \in Y$. We can simply choose the 3-cycle $\pi \in S_n(A_n)$, $\pi = (x,y,z)$. $x\pi = y$, $y\pi = z$, $z\pi = x$, so the assumption $Y\pi = Y$ or $Y\pi \cap Y = \emptyset$ does not hold. ∎

Lemma 3.26 *Let $\{\pi_i\}_{i=1}^m$, $\pi_i \in G$, be generators of G. Let $\{M_j\}_{j=1}^l$, $M_j \subset X$, $\cup_{j=1}^l M_j = X$, $M_i \cap M_j = \emptyset$ for $i \neq j$, form a partition of X, such that $M_j\pi_i = M_k$, $1 \leq i \leq m$, $1 \leq j \leq l$, for some $1 \leq k \leq l$. Then each M_j, $|M_j| \geq 2$, is a domain of imprimitivity of G.*

Proof: Let M_{j_0}, $1 \leq j_0 \leq l$, $|M_{j_0}| \geq 2$, be a subset of the partition. Let $\pi_0 \in G$ be an arbitrary element. $\pi_0 = \prod_{k=1}^s \pi_{i_k}^{r_k}$, $r_k = \pm 1$, is an arbitrary representation of π_0 as a word in $\{\pi_i\} \cup \{\pi_i^{-1}\}$. The proof is by induction on s.

If $s = 1$, then $\pi_0 = \pi_{i_{k_0}}^{\pm 1}$, for some $1 \leq i_{k_0} \leq m$. Thus $M_{j_0}\pi_0 = M_{j_0}$ or $M_{j_0}\pi_0 \cap M_{j_0} = \emptyset$. Assume for all $s' < s$. By induction $M_{j_0}(\prod_{k=1}^{s-1} \pi_{i_k}^{r_k}) = M_t$, for some $1 \leq t \leq l$. Thus

$$M_{j_0}\pi_0 = M_{j_0}(\prod_{k=1}^{s} \pi_{i_k}^{r_k}) = M_t\pi_{i_s}^{r_s} = M_u \text{ for some } 1 \leq u \leq l.$$

So $M_{j_0}\pi_0 = M_{j_0}$ if $u = j_0$ or $M_{j_0}\pi_0 \cap M_{j_0} = \emptyset$ if $u \neq j_0$. ∎

A simple use of the the two Lemmas allows us to derive a general restriction on complements of a permutation. This simple restriction is nearly enough to determine all the complements of a transposition in S_n.

Lemma 3.27 *Let $\pi \in S_n(A_n)$, $n \geq 3$. Let $Y \subseteq \{1, \ldots, n\}$ be the subset of points moved by π, $|Y| = k$, $1 \leq k \leq n$. Let $\sigma \in S_n(A_n)$ be a complement to π, such that $\langle \pi, \sigma \rangle = S_n(A_n)$, and let $\sigma = \prod_{i=1}^{m} C_i$ be the cycle decomposition of σ (including cycles of length 1).*

Then the following condition on σ must hold: For any cycle of the decomposition C_i, $1 \leq i \leq m$, if Z_i is the subset of points moved by C_i, then $Y \cap Z_i \neq \emptyset$ (this implies $m \leq k$).

Proof: The proof is simple. Assume there exists a cycle C_{i_0}, $1 \leq i_0 \leq m$, in the decomposition such that $Y \cap Z_{i_0} = \emptyset$. We denote $M_1 = Z_{i_0}$, $M_2 = \{1, \ldots, n\} \setminus Z_{i_0}$. Thus, $|M_1| \geq 2$ or $|M_2| \geq 2$ ($n \geq 3$). Observe that $M_1\pi = M_1$, $M_2\pi = M_2$, $M_1\sigma = M_1$, $M_2\sigma = M_2$. By Lemma 3.26 this implies that either M_1 or M_2 are domains of imprimitivity of $\langle \pi, \sigma \rangle$. But since $\langle \pi, \sigma \rangle = S_n(A_n)$ and by Lemma 3.25 $S_n(A_n)$ is primitive, we have a contradiction. ∎

We now prove the main result of this section and explicitly list all the complements of a transposition. The previous result gives us an important limitation on the form of a complement of a transposition. Namely, such a complement can be composed of at most two disjoint cycles. Adding a few other restrictions we have the following result.

Lemma 3.28 *For any transposition $\pi \in S_n$, $n \geq 3$, $\pi = (a_1, a_2)$, $\sigma \in S_n$ is a complement to π, such that $\langle \pi, \sigma \rangle = S_n$ iff σ has one of the following forms (cycles of length one are omitted):*

The 1–cycle cases

1. *σ is a $(n-1)$-cycle that fixes one of the points $\{a_1, a_2\}$.*
2. *σ is a n-cycle with the following property: Let m be the unique integer, $1 \leq m < n$, such that $\{a_1\}\sigma^m = \{a_2\}$. Then $(m, n) = 1$.*

The 2–cycle case

3. *σ has a cycle decomposition $\sigma = C_1 \cdot C_2$, $|C_i| = m_i$, $1 \leq i \leq 2$, $m_1 + m_2 = n$, $(m_1, m_2) = 1$ and C_i moves the point $\{a_i\}$.*

Proof: By Lemma 3.15 we can assume $\pi = (1, 2)$.

Let $\sigma \in S_n$ have one of the above forms.

1. This case was proved in Lemma 3.8.

2. Let m be the unique integer, $1 \leq m < n$, such that $\{1\}\sigma^m = \{2\}$. As $(m,n) = 1$, σ^m is also a n–cycle. By rewriting the points $\{3,\ldots,n\}$ we can assume $\sigma^m = (1,2,3,\ldots,n)$. Thus, by Lemma 3.7, $S_n = \langle (1,2), \sigma^m \rangle \leq \langle (1,2), \sigma \rangle$.

3. By rewriting the points $\{3,\ldots,n\}$ we can assume $\sigma = (1,3,\ldots,j)(2,j+1,\ldots,n)$ with $(j-1, n-j+1) = 1$. σ^{n-j+1} is is a $(j-1)$–cycle, so by Lemma 3.8,

$$S_j = \langle (1,2), \sigma^{n-j+1} \rangle \leq \langle (1,2), \sigma \rangle.$$

   Also, σ^{j-1} is a $(n-j+1)$–cycle so it clear the symmetric group over the points $\{1,2,j+1,\ldots,n\}$ is in $\langle (1,2), \sigma \rangle$. As this implies all the transpositions $(1,i)$, $2 \leq i \leq n$, are in $\langle (1,2), \sigma \rangle$, by Lemma 3.5, $\langle (1,2), \sigma \rangle = S_n$.

This conclude the first part of the proof.

Next, we assume $\sigma \in S_n$ is a complement to $\pi = (1,2)$, such that $\langle (1,2), \sigma \rangle = S_n$. Let $\sigma = \prod_{i=1}^{k} C_i$ be the cycle decomposition of σ (cycles of length one are omitted). By Lemma 3.27, $k \leq 2$, otherwise there exists a domain of imprimitivity of $\langle (1,2), \sigma \rangle$.

We now use case analysis:

$k = 1$ and $|C_1| \leq n-2$

In this case there are only two possibilities:

1. $(1,2)$ and σ both fix a point $\{j\}$, $3 \leq j \leq n$. This implies $\langle (1,2), \sigma \rangle \neq S_n$.
2. σ fixes the points $\{1,2\}$. This implies $\{1,2\}$ is a domain of imprimitivity for $\langle (1,2), \sigma \rangle$.

We conclude this case is not possible.

$k = 1$ and $|C_1| = n-1$

If the fixed point of σ is not $\{1\}$ or $\{2\}$ it is easy to see $\langle (1,2), \sigma \rangle \neq S_n$. Otherwise, σ has the form (1) of the Lemma.

$k = 1$ and $|C_1| = n$

Let m be the unique integer, $1 \leq m < n$, such that $\{1\}\sigma^m = \{2\}$. Assume by contradiction $(m,n) \neq 1$. Let $\sigma^m = \prod_{j=1}^{l} D_j$ be the cycle decomposition of σ^m. We denote by M_j the subset of the points moved by the cycle D_j, $1 \leq j \leq l$. Observe that $l = (m,n)$ and $2 \leq |M_j| = n/l < n$, $1 \leq j \leq l$. Obviously, $M_j(1,2) = M_j$ for all $1 \leq j \leq l$. Also, it is easy to see that for each j, $1 \leq j \leq l$, there exists an index r, $1 \leq r \leq l$, such that $M_j\sigma = M_r$. Thus, we have the conditions of Lemma 3.25 and each M_j, $1 \leq j \leq l$ is a domain of imprimitivity of $\langle (1,2), \sigma \rangle$. This contradicts $\langle (1,2), \sigma \rangle = S_n$. Thus $(m,n) = 1$ and σ has the form (2).

$k = 2$ and $|C_1| + |C_2| < n$

In this case we know there is at least one point $\{j\}$, $1 \leq j \leq n$, that σ fixes. If $j \geq 3$, then $\langle (1,2), \sigma \rangle$ fixes the point $\{j\}$, and so $\langle (1,2), \sigma \rangle \neq S_n$. If $j \leq 2$, then at least one of the cycles C_1, C_2 fixes the points $\{1,2\}$, say C_1. Thus the subset of points moved by C_1 is a domain of imprimitivity of $\langle (1,2), \sigma \rangle$. This is a contradiction to S_n being primitive. We conclude this case is not possible.

$k = 2$ and $|C_1| + |C_2| = n$

If one of the cycles C_1,C_2 moves both points $\{1,2\}$, then it is easy to see the subset of points moved by the other cycle is a domain of imprimitivity of $\langle (1,2), \sigma \rangle$. Thus, we can assume $\sigma = (1, 3, \ldots, j)(2, j+1, \ldots, n\rangle$ for some $3 \leq j \leq n-1$. Assume $g = (j-1, n-j+1\rangle \neq 1$. Observe that for any two elements x, y of an arbitrary group, $\langle x, y \rangle = \langle x, x \cdot y \rangle$. In this case $\langle (1,2), \sigma \rangle = \langle (1,2), (1,2) \cdot \sigma \rangle = \langle (1,2), \sigma_1 \rangle$, where $\sigma_1 = (1, j+1, \ldots, n-1, n, 2, 3, \ldots, j)$ is a cycle of length n. Observe $\{1\}\sigma_1^{n-j+1} = \{2\}$. Because $g|j-1$, $g|n-j+1$, we have $g|n$. Thus $(n-j+1, n) \neq 1$. We see this case can be reduced to the case $k = 1$, $|C_1| = n$ with $m = n-j+1$ as the unique integer such that $\{1\}\sigma^m = \{2\}$. In this case $S_n \doteq \langle (1,2), \sigma_1 \rangle$ was not possible. Thus, $S_n = \langle (1,2), \sigma \rangle$ is not possible. We conclude $(j-1, n-j+1) = 1$ and so σ has the form $(3\rangle$ of the Lemma.

∎

Bibliography

[1] J. D. Dixon. *The probability of generating the symmetric group*. Math Z. 110 (1969) 199–205.

[2] M. W. Liebeck, A. Shalev. *The probability of generating a finite simple group.* — to appear.

[3] T. M. Apostol. *Introduction to Analytic Number Theory.* Springer – Verlag (1976).

[4] D. J. Robinson. *A course in the theory of groups.* Springer – Verlag (1987).

[5] *GAP (Groups, Algorithms and Programming) Version 3 Release 3.* A public domain Computational Algebra System.

Index

אוניברסיטת תל־אביב
הפקולטה למדעים מדויקים
ע"ש ריימונד ובברלי סאקלר
בית הספר למדעי המתימטיקה

יוצרים של S_n ו A_n

חיבור זה הוגש כחלק מהדרישות לקבלת התואר
"מוסמך אוניברסיטה" M.Sc. באוניברסיטת תל־אביב
החוג למתימטיקה עיונית

על ידי

שי דקל

העבודה הוכנה באוניברסיטת תל־אביב
בהדרכתו של
פרופסור מרצל הרצוג

יולי 1994

תודתי העמוקה לפרופסור הרצוג על עזרתו הרבה והמשמעותית לכתיבת חיבור זה.

ברצוני להודות ליוצרי GAP (Groups, Algorithms and Programming) על שהפכו את המערכת לנחלת הכלל.

תודה לך טל על התמיכה המתמדת.

תקציר

נטו, בספרו מהמאה הקודמת, הניח כי כמעט כל צמד תמורות מתוך החבורה הסמטרית מעל n אותיות יוצר את החבורה האלטרנטית (A_n) או את החבורה הסימטרית (S_n). מאחר ו 3/4 מכל הזוגות הללו מכילים לפחות תמורה אי־זוגית אחת, יוצא שההסתברות שזוג יצור את S_n היא בקרוב 3/4. ההנחה של נטו נותרה בעיה פתוחה עד שדיקסון [1] הוכיח כי ההסתברות שזוג מקרי (x,y), $x,y \in S_n$, יצור את S_n שואפת ל 3/4 כאשר $n \to \infty$. כמו כן ההסתברות שזוג מקרי (x,y), $x,y \in A_n$, יצור את A_n שואפת ל 1 כאשר $n \to \infty$. דיקסון ניסח הנחה שבכל חבורה פשוטה סופית ההסתברות שואפת ל 1 כאשר $|G| \to \infty$. לאחרונה [2] ההוכחה להנחה זו הושלמה בעזרת המיון של החבורות הפשוטות הסופיות.

תוצאות סטטיסטיות אלו מראות כי במובן מסוים "יקלי" למצוא יוצרים של S_n ו A_n (או כל חבורה פשוטה סופית). אכן, התוצאה המרכזית של חיבור זה היא שפרט למקרה מיוחד, לכל תמורה x ב $S_n(A_n)$ קיימת תמורה y ב $S_n(A_n)$, כך שיחדיו הן יוצרות את $S_n(A_n)$.

הפרק הראשון משמש הקדמה ובו הגדרות ותוצאות כלליות על יוצרים בחבורות סופיות. אנו מתמקדים בחבורות מדרגה 2 (זהו המקרה של S_n ו A_n עבור $n \geq 4$) ומבחינים בקשר שבין תת החבורה של פרטיני והלא יוצרים של החבורה.

בפרק השני אנו מתמקדים בחבורות S_n. נחקור את המבנה הקומבינטורי של מחלקות הצמידות ונציג שיטות לחישוב מספר המחלקות וגודלן. התוצאה המרכזית של פרק זה היא אלגוריתם רקורסיבי שמחשב את $p(n)$, פונקציה מתורת המספרים, ובכך את מספר מחלקות הצמידות ב S_n.

התוצאה המרכזית מוצגת בפרק 3. אנו מוצאים במפורש משלים לכל תמורה ב $S_n(A_n)$, כך שיחדיו הם יוצרים את $S_n(A_n)$. כמו כן, כדוגמה, נמצא את כל המשלימים של טרנספוציזיה ב S_n.