SOME TOPICS IN THE REPRESENTATION THEORY OF FINITE GROUPS AND
LINEAR ASSOCIATIVE ALGEBRAS

HONORS THESIS ID 499
BALL STATE UNIVERSITY

ADVISOR: MR. RANDAL P. MILLER

META DARLENE KEIHN
JULY 15, 1966
Acknowledgements

Since mathematical notation and definition are still somewhat a matter of individual whim, I have chosen to use that which Mr. Miller uses in his lectures. I am therefore very grateful to Miss Paula Lovelace and Miss Rebecca Russell for the use of their classnotes taken in Mathematics 411 and Mathematics 512. I am particularly indebted to Mr. Miller himself for his help and guidance.
INDEX

Introduction ..............................................1
I. Basic Definitions ......................................1
II. Cayley's Theorem .....................................7
III. Representations of Groups .........................9
IV. Linear Algebras ....................................15
V. Conclusion ............................................22
Bibliography ............................................23
Some Topics in the Representation Theory of Finite Groups
and Linear Associative Algebras

Introduction

For many years algebra was considered to be merely symbolic arithmetic; a short cut for easier problem solution. Eventually mathematicians became aware that some of the symbolic statements from this generalized arithmetic, which were true when numerals were plugged in, were also true when the symbols were replaced by other objects. Thus algebra evolved into the study of mathematical systems. One of the most fundamental of the systems with "nice" properties is the group. To a large extent this paper will illustrate some methods of analyzing abstract algebraic systems which have been devised by mathematicians. In particular after basic definitions have been given, the emphasis shall be upon representing groups by other groups to facilitate that analysis. However, as abstract as group theory may appear, it must not be forgotten that group theory does have important applications in physics and chemistry.

I. Basic Definitions

In any branch of mathematics one must begin with some undefined terms which are intuitively clear, and build upon these logically to develop some ideas by means of definitions, postulates, and theorems. Our only undefined term necessary for this paper is set. A set is a basic formally undefined noun--intuitively a collection of objects--to which we assign a basic formally undefined predicate, the elementhood predicate. Intuitively, an object either is or is not an element
of a set. The term subset is then formally defined as follows:

**Definition 1.** A set \( T \) is a subset of a set \( S \) if and only if every element of \( T \) is also an element of \( S \). A set \( T \) is a proper subset of a set \( S \) if and only if \( T \) is a subset of \( S \), but \( S \) is not a subset of \( T \).

Other definitions essential for a complete hierarchy of logically developed concepts include:

**Definition 2.** Let \( a \) and \( b \) be sets. By the ordered pair \((a, b)\), we mean

\[
(a, b) = \{(a), (a, b)\}.
\]

a. Remark: This definition implies that \((a, b)\) and \((c, d)\) are equal if and only if \( a = c \) and \( b = d \).

**Definition 3.** Let \( a \) and \( b \) be sets. By the Cartesian product of \( a \) and \( b \) (denoted \( a \times b \) and read "a cross b") we mean the set

\[
a \times b = \{(x, y) | (x \in a) \land (y \in b)\}.
\]

**Definition 4.** Let \( a \) and \( b \) be sets. A relation from \( a \) to \( b \) is any subset of the Cartesian product \( a \times b \).

**Definition 5.** Let \( a \) and \( b \) be sets, and \( R \) be a relation from \( a \) to \( b \). \( R \) is called a functional relation if and only if no two different pairs with the same first entries are elements of \( R \).

**Definition 6.** Let \( X \) and \( Y \) be sets. Then \( f \) is a function from \( X \) to \( Y \) if and only if: 1) \( f \) is a functional relation from \( X \) to \( Y \); and 2) the domain of \( f \) is all of \( X \). That is, the set of all the different first entries of the various ordered pairs in \( f \) is all of \( X \).

a. Notation: The set of all functions from a set \( X \) to a set \( Y \) is denoted by \( Y^X \). Thus \( f \in Y^X \) means \( f \) is a function from \( X \) to \( Y \). **A mapping is a function.**
Definition 7. If $\alpha$ is a mapping of a set $S$ into a set $T$, then $\alpha$ is called a mapping of $S$ onto $T$ if for each $y \in T$, there is some $x \in S$ such that $\alpha x = y$.

Definition 8. A mapping $\alpha$ is called a 1:1 mapping or injection of $S$ into $T$ if and only if any two distinct elements of $S$ have distinct images in $T$.

Definition 9. A permutation on a set $S$ is a 1:1 mapping of $S$ onto itself.

Let $S$ be a set and let $R$ be a relation from $S$ to $S$. That is, $R \subseteq S \times S$. Then certain properties of $R$ may be defined as follows:

Definition 10. $R$ is said to be reflexive iff for every $x \in S$, then $(x, x) \in R$.

Definition 11. $R$ is said to be symmetric iff whenever $(x, y) \in R$, then $(y, x) \in R$.

Definition 12. $R$ is said to be transitive iff whenever $(x, y) \in R$, and $(y, z) \in R$, then $(x, z) \in R$.

Definition 13. Let $E$ be a relation from a set $S$ to $S$. $E$ is called an equivalence relation iff $E$ is reflexive, symmetric, and transitive.

Definition 14. A mathematical system $S$ is a set $S = (E, O, A)$ where $E$ is a nonempty set of elements, $O$ is a set of relations and operations on $E$, and $A$ is a set of axioms concerning the elements of $E$ and $O$.

Having accepted these fourteen definitions, we are now ready to define what is meant by a group.

Definition 15. Let $G$ be a nonempty set (furnished with an equivalence relation) and let $\cdot$ be a binary operation on $G$ (i.e., $\cdot$ is a function from $G \times G$ to $G$). The mathematical system $(G, \cdot)$ is called a group iff $\cdot$ has the following properties:
1) \( \circ \) is associative: for every three elements \( x, y, z \) of \( G \),
\[
x \circ (y \circ z) = (x \circ y) \circ z.
\]

2) There is an element \( e_L \in G \) so that for every \( x \in G \),
\[
e_L \cdot x = x. \quad \text{(Left identity element)}
\]

3) For every element \( x \in G \), there corresponds an element
\[
x^{-1}_L \in G \text{ so that } x^{-1}_L \cdot x = e. \quad \text{(Left inverse.)}
\]

Of course there are other similar definitions possible, but all
are equivalent to the above. Given this definition, what are some ex-
amples? Integers under usual addition, rational numbers under usual
addition, nonzero rational numbers under multiplication, and complex
numbers under usual addition name a few well-known groups. Suppose we
look at arithmetic modulo five. The addition table below shows speci-
fically:

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

In general, \( a + (b + c) = (a + b) + c \)
where \( a, b, \) and \( c \) can be any elements of
the table. The additive identity is 0, and
each element has an inverse: 0-0; 1-4;
2-3; 3-2; and 4-1. Thus we must again
have a group.

**Theorem 1.** If \( (G, \circ) \) is a group and \( a \in G \), then \( a \cdot a^{-1}_L = e \), and
\( a \cdot e_L = a. \)

**Proof:** \( a^{-1}_L \in G \) implies that there exists a "\( v \)" \( \in G \) such that
\[
v \cdot a^{-1}_L = e. \quad \text{Then } a \cdot a^{-1}_L = (e \cdot a) \cdot a^{-1}_L = (v \cdot a^{-1}_L) \cdot a = v \cdot (a^{-1}_L \cdot a) \cdot a^{-1}_L = v \cdot e \cdot a^{-1}_L = v \cdot a^{-1}_L = e. \quad \text{Therefore } a \cdot a^{-1}_L = e. \quad \text{To see that } e_L
\]
is also a right identity, consider:
\[
a \cdot e = a \cdot (a^{-1}_L \cdot a) = (a \cdot a^{-1}_L) \cdot a = e \cdot a = a. \quad \text{Therefore } e \text{ is the identity element. Note that we now have}
\]

no need of the subscript \( L \) and it can be dropped.
There is a group-theoretic analogue for the set-theoretic concept of subset. This is the idea of subgroup, whose definition follows:

Definition 16. Let \((G, *)\) be a group and let \(H\) be a nonempty subset of \(G\). If \(*_H\) is the restriction of \(*\) to \(H\), (i.e., \(*_H = (H \times H \times G) \cap *\)), then the system \((H, *_H)\) is said to be a subgroup of \((G, *)\) if \((H, *_H)\) is a group in its own right.

We denote the statement that \((H, *_H)\) is a subgroup of \((G, *)\) by the notation \(H < G\). It can be shown that \((H, *_H)\) is a subgroup of \((G, *)\) when \(H\) is a nonempty subset of \(G\) iff 1) for every element \(a \in H\) and \(b \in H\), both \(a \cdot b \in H\) and \(a^{-1} \in H\); or 2) if \(a \in H\) and \(b \in H\), then \(a \cdot b^{-1} \in H\).

Of course not every subset of \(G\) will be a subgroup under the defined operation.

Definition 17. Let \((G, *)\) be a group. The order of \(G\), denoted \([G:e]\), is defined to be the cardinal number of the set \(G\). \((G, *)\) is said to be finite iff \([G:e]\) is finite.

Examples: The order of the group \((\mathbb{Z}, +)\) of integers under addition is infinite. The order of the group \(\mathbb{Z}_n\) of integers modulo \(n\) is \(n\).

Definition 18. Let \((G, *)\) be a group and let \(S\) be a nonempty subset of \(G\). Then \(S\) is called a complex of \(G\).

If \(S\) is a complex of the group \((G, *)\), then the smallest subgroup \((H, *_H)\) of \(G\) which contains \(S\) as a subset is called the subgroup generated by \(S\), notated by \((S)\). \((S) = (S, *_S)\) iff \(S < G\).

Definition 19. Let \((G, *)\) be a group. \((G, *)\) is said to be cyclic iff there exists some element \(g \in G\) so that \(G = \langle g \rangle\).

Example: \[
\begin{array}{c|ccc}
+ & 0 & 1 \\
\hline
0 & 0 & 1 \\
1 & 1 & 0
\end{array}
\]

This table gives a cyclic group of order two whose generator is 1.
It is well-known that every subgroup of a cyclic group is cyclic. 1

Definition 20. If $H$ is a subgroup of $(G, \cdot)$, then the set $aH = \{a \cdot h | h \in H\}$, for a fixed element $a$ of $G$, is a left coset of $H$. The element $a$ is called a representative of $aH$. Right cosets are similarly defined.

Example:

<table>
<thead>
<tr>
<th></th>
<th>e</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>f</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td>e</td>
<td>a</td>
<td>b</td>
<td>c</td>
<td>d</td>
<td>f</td>
</tr>
<tr>
<td>a</td>
<td>a</td>
<td>b</td>
<td>e</td>
<td>f</td>
<td>c</td>
<td>d</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>e</td>
<td>a</td>
<td>d</td>
<td>f</td>
<td>c</td>
</tr>
<tr>
<td>c</td>
<td>c</td>
<td>d</td>
<td>f</td>
<td>e</td>
<td>a</td>
<td>b</td>
</tr>
<tr>
<td>d</td>
<td>d</td>
<td>f</td>
<td>c</td>
<td>b</td>
<td>e</td>
<td>a</td>
</tr>
<tr>
<td>f</td>
<td>f</td>
<td>c</td>
<td>d</td>
<td>a</td>
<td>b</td>
<td>e</td>
</tr>
</tbody>
</table>

A subgroup of this group would be:

<table>
<thead>
<tr>
<th></th>
<th>e</th>
<th>a</th>
<th>b</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td>e</td>
<td>a</td>
<td>b</td>
</tr>
<tr>
<td>a</td>
<td>a</td>
<td>b</td>
<td>e</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>e</td>
<td>a</td>
</tr>
</tbody>
</table>

If we let $a$, $b$, or $e$ be the representative, the left cosets are:

$eH = aH = bH = H = \{e, a, b\}$.

If $c$, $d$, or $f$ is the representative, then we have the left cosets:

$cH = dH = fH = \{c, d, f\}$.

Note also that the set $A = \{e, c\}$ is also a cyclic subgroup of $G$ whose generator is $c$. This example implies that if $H$ is a subgroup of $(G, \cdot)$ and $aH$ and $bH$ are cosets of $H$ then 1) $aH = bH$ or 2) $aH$ and $bH$ are disjoint.

Definition 21. The subgroup $H$ of the group $G$ is normal in $G$ if and only if for every $x$ in $G$ the left coset $xH$ equals the right coset $Hx$, or $x^{-1}Hx \subseteq H$. $H$, a normal subgroup of $G$, is denoted by $H \triangleleft G$.

Definition 22. Let $(G_1, \circ_1)$ and $(G_2, \circ_2)$ be groups, and let $\phi \in G_2^{G_1}$. (i.e., $\phi$ is a mapping from $G_1$ to $G_2$.) $\phi$ is said to be a homomorphism iff $(x \circ_1 y) \phi = (x \phi) \circ_2 (y \phi)$ for every $x \in G_1$ and every $y \in G_1$.

---

1 Deskins, Abstract Algebra, pp. 212-213.
A homomorphism which is 1:1 is called a **monomorphism**.

A homomorphism which is onto is called an **epimorphism**.

A homomorphism which is both a monomorphism and an epimorphism is called an **isomorphism**.

II. Cayley's Theorem

If we have a set $S$, as we said before, a permutation of $S$ is any 1:1 onto function from $S$ to $S$. Let $S = \{1, 2, 3\}$. Then the (3!) possible permutations, with appropriate notation, are:

$$
\begin{align*}
(1 & 2 & 3), \\
(1 & 3 & 2), \\
(2 & 1 & 3), \\
(2 & 3 & 1), \\
(1 & 2 & 3), \\
& (3 & 1 & 2).
\end{align*}
$$

A cycle is a shorthand way of writing permutations. The cycles which describe the above are respectively: $(1), (2 3), (1 3), (1 2), (1 2 3), \text{ and } (1 3 2)$. Note we are using left hand notation, reading cycles and products of cycles from right to left.

**Definition 23.** A transposition is a cycle of order two.

Is this set of permutations under operation of composition of functions a group? Composition of functions is associative, the identity is $(1)$, and each permutation has an inverse—the first four are their own inverses, and the last two are inverses of each other. Therefore the system is a group. In general, the group of all permutations of a set with $n$ elements is called the symmetric group on $n$ symbols and is designated $S_n$.

Informally, a representation is a general way of using a homomorphism from abstract systems (in which the elements are unknown and just the set is defined) to concrete systems. If we can exhibit a representation of abstract groups as groups of permutations, it will be a simple matter to
represent permutations as matrices and computation will be greatly simplified. The theorem which says that abstract groups can be represented as groups of permutations is known as Cayley's Theorem. Its formal statement and proof are as follows:

**Theorem 2. (Cayley's Theorem):** Let \( G \) be a group. Then \( G \) is isomorphic to a subgroup of \( S_{[G:e]} \); i.e., every group is isomorphic to a group of permutations.

**Proof:** Let \( g \in G \) and let \( \bar{g} \) be the permutation in \( S_{[G:e]} \) which maps \( x \) onto \( xg \). \( \bar{g} \) really is a permutation of \( G \) since 1) the range of \( \bar{g} \) is \( G \) (since \( G \) is closed under multiplication) and 2) \( \bar{g} \) is 1:1.

Let \( x \) and \( y \) be elements of \( G \) and assume \( x \neq y \). \( \bar{g}(x) \neq \bar{g}(y) \), for if they were equal, then \( xg = yg \), which implies \( x = y \), a contradiction.

3) \( \bar{g} \) is onto. Let \( x \in G \). The \( \bar{g} \) pre-image of \( x \) is \( xg^{-1} \) since \( \bar{g}(xg^{-1}) = (xg^{-1})g = x(gg^{-1}) = xe = x \).

Let \( \phi: G \rightarrow S_{[G:e]} \) be given by \( g \phi = \bar{g} \). We assert that \( \phi \) is a monomorphism. To prove this, we must show that 1) \( \phi \) is a homomorphism, and 2) \( \phi \) is 1:1.

1. **Prove:** \( g_1 \phi g_2 = g_1 g_2 \phi \), where \( g_1 g_2 x = x(g_1 g_2) \).

   **Proof:** \( g_1 \phi = \bar{g}_1 ; \bar{g}_1(x) = xg_1 ; g_2 \phi = \bar{g}_2 ; \bar{g}_2(y) = yg_2 \).

   \[ \therefore \bar{g}_2(\bar{g}_1(x)) = g_2(xg_1) = xg_1 g_2 \] . \( \therefore \phi \) is a homomorphism.

2. **Prove:** \( \phi \) is one-to-one.

   **Proof:** Let \( g_1 \neq g_2 \) be elements of \( G \). Then \( g_1 \phi = \bar{g}_1 \), where \( \bar{g}_1(x) = xg_1 \), and \( \bar{g}_2 \phi = g_2 \), where \( \bar{g}_2(x) = xg_2 \). If \( \bar{g}_1 = \bar{g}_2 \), then \( xg_1 = xg_2 \) for every \( x \in G \). \( \therefore x^{-1}(xg_1) = x^{-1}(xg_2) \) for every \( x \in G \). By associativity, \( (x^{-1}x)g_1 = (x^{-1}x)g_2 \), so \( eg_1 = eg_2 \), which implies \( g_1 = g_2 \); but this is a contradiction. \( \therefore \bar{g}_1 \neq \bar{g}_2 \) and \( \phi \) must be one-to-one.
III. Representations of Groups

Having proven Cayley's Theorem, we are now ready to show that not only can we represent groups by permutations, but that these permutations can be represented as matrices. What is a permutation matrix?

Definition 24. A permutation matrix is an n x n matrix of 1's and 0's in which there is one and only one "1" in each row and column.

Example: The cycle representation of the permutation (1 2 3) is represented in a permutation matrix as follows:

\[
\begin{pmatrix}
0 & 1 & 0 \\
0 & 0 & 1 \\
1 & 0 & 0
\end{pmatrix}
\]

(remember left hand notation is being used, so read the cycle from right to left.)

Theorem 3: Every permutation can be represented as a matrix.

Our proof will be made clearer if we first prove a lemma.

Lemma 1: Every permutation in the symmetric group \( S_n \) of order \( n! \) is a product of transpositions.

Proof: Consider the cycle: \( (a_1, a_2, a_3, \ldots, a_k) \). Observe that

\[
(a_1 a_2 a_3 \ldots a_k) = (a_1 a_k) (a_2 a_k)(a_3 a_k) \ldots (a_{k-1} a_k).
\]

:. Every permutation in \( S_n \) is a product of transpositions.

Example: \( (1 2 3 4 5) = (1 5) (2 5) (3 5) (4 5) \).

Now since any permutation can be written as a product of cycles and each cycle is a product of transpositions, then if we exhibit a homomorphism between permutation matrices and transpositions, this homomorphism is sufficient for proving permutations in general can be represented by matrices.

Proof: Let \((i j)\) and \((k q)\) be two arbitrary transpositions in \( S_n \).
Define a function \( h \) from the set of transpositions of \( S_n \) to the set of 
\( n \times n \) permutation matrices by:
h(i j) = the n x n matrix obtained from the n x n identity matrix $I_n$ by the interchanging of the $i^{th}$ and $j^{th}$ rows.

$$= \sum_{m=1}^{n} A_{mm} + A_{ij} + A_{ji}$$

$m \notin \{i, j\}$

where $A_{rs}$ is the n x n matrix with 1 in the (r, s)$^{th}$ place and 0's elsewhere.

To show that $h$ is a homomorphism, we shall show that

$$h((i j) (k q)) = h(i j) \cdot h(k q).$$

Case 1. \{i, j\} \cap \{k, q\} = \emptyset

Case 2. \{i, j\} \cap \{k, q\} = \{j\}. For definiteness, say $q = j$. Then

$$(i j) (k q) = (i j) (k j) = (i k j).$$

Case 3. \{i, j\} = \{k, q\}. For definiteness, say $i = k$ and $j = q$, so that

$$(i j) (k q) = (i j) (i j) = (1).$$

Case 1. $h((i j) (k q)) = \sum_{m=1}^{n} A_{mm} + A_{ij} + A_{ji} + A_{kq} + A_{qk}$

$m \notin \{i, j, k, q\}$

On the other hand, $h((i j)) = \sum_{m=1}^{n} A_{mm} + A_{ij} + A_{ji}$ and

$$h((k q)) = \sum_{m=1}^{n} A_{mm} + A_{kq} + A_{qk}.$$

Now the matrix basis elements $A_{rs}$ are multiplied according to the formula:

$$A_{rs}A_{tu} = A_{ru} \cdot \delta_{(st)}$$

where $\delta_{(st)}$ is the Kronecker $\delta$-function defined by $\delta_{(st)} = 1$ if $s = t$, and $\delta_{(st)} = 0$ if $s \neq t$.

Therefore, $h((i j)) \cdot h((k q)) = \left(\sum_{m=1}^{n} A_{mm} + A_{ij} + A_{ji}\right) \left(\sum_{m=1}^{n} A_{mm} + A_{kq} + A_{qk}\right)$

$$= \left(\sum_{m=1}^{n} A_{mm}\right) \left(\sum_{m=1}^{n} A_{mm}\right) + \left(\sum_{m=1}^{n} A_{mm}\right) A_{kq} + \left(\sum_{m=1}^{n} A_{mm}\right) A_{qk} + A_{ij} \left(\sum_{m=1}^{n} A_{mm}\right)$$

$m \notin \{i, j\}$

$m \notin \{k, q\}$

$m \notin \{i, j\}$

$m \notin \{k, q\}$
\[ A_{ij} A_{kq} + A_{ij} A_{qk} + A_{ji} \left( \sum_{m=1}^{n} A_{mm} \right) + A_{ji} A_{kq} + A_{ji} A_{qk} \]

\[ = \sum_{m=1}^{n} A_{mm} + A_{kq} + A_{qk} + A_{ij} + O + O + A_{ji} + O + O \]

\[ m \neq \{k, q\} \]

\[ = \sum_{m=1}^{n} A_{mm} + A_{ij} + A_{ji} + A_{kq} + A_{qk} \]

\[ m \neq \{i, j, k, q\} \]

\[ : h((i, j)) \cdot h((k, q)) = h((i, j) \odot (k, q)) \]

Case 2. \[ h((i, j) \odot (k, j)) = h(i, k, j) = \sum_{m=1}^{n} A_{mm} + A_{ik} + A_{ji} + A_{kj} \]

But \[ h((i, j)) = \sum_{m=1}^{n} A_{mm} + A_{ij} + A_{ji} \]

\[ m \neq \{i, j\} \]

and \[ h((k, j)) = \sum_{m=1}^{n} A_{mm} + A_{kj} + A_{jk} \]

\[ m \neq \{k, j\} \]

\[ : h((i, j)) \cdot h((k, j)) = \left( \sum_{m=1}^{n} A_{mm} + A_{ij} + A_{ji} \right) \left( \sum_{m=1}^{n} A_{mm} + A_{kj} + A_{jk} \right) \]

\[ = \left( \sum_{m=1}^{n} A_{mm} \right) \left( \sum_{m=1}^{n} A_{mm} \right) + \left( \sum_{m=1}^{n} A_{mm} \right) A_{kj} + \left( \sum_{m=1}^{n} A_{mm} \right) A_{jk} + A_{ij} \left( \sum_{m=1}^{n} A_{mm} \right) \]

\[ + A_{ij} A_{kj} + A_{ij} A_{jk} + A_{ji} \left( \sum_{m=1}^{n} A_{mm} \right) + A_{ji} A_{kq} + A_{ji} A_{qk} \]

\[ = \sum_{m=1}^{n} A_{mm} + A_{kj} + O + O + O + A_{ik} + A_{ji} + O + O \]

\[ m \neq \{i, j, k\} \]

\[ = \sum_{m=1}^{n} A_{mm} + A_{ik} + A_{ji} + A_{kj} \]

\[ m \neq \{i, j, k\} \]

\[ : h((i, j) \odot (k, j)) = h((i, j)) \odot h((k, j)) \]

Example: \[ (2 \ 3) (3 \ 4) = (2 \ 4 \ 3) \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \]
Case 3. \( h((i\ j)\cdot(i\ j)) = h((1)) = I_n \) or \( \sum_{m=1}^{n} A_{mm} \).

But \( h((i\ j)) = \sum_{m\neq\{i,j\}} A_{mm} + A_{ij} + A_{ji} \).

\[ \therefore \quad h((i\ j)) \cdot h((i\ j)) = \left( \sum_{m\neq\{i,j\}} A_{mm} + A_{ij} + A_{ji} \right) \cdot \left( \sum_{m\neq\{i,j\}} A_{mm} + A_{ij} + A_{ji} \right) \]

\[ = \left( \sum_{m\neq\{i,j\}} A_{mm} \right) \cdot \left( \sum_{m\neq\{i,j\}} A_{mm} \right) + \left( \sum_{m\neq\{i,j\}} A_{mm} \right) A_{ij} + \left( \sum_{m\neq\{i,j\}} A_{mm} \right) A_{ji} + \left( \sum_{m\neq\{i,j\}} A_{mm} \right) A_{ij} A_{ji} + A_{ij} A_{ji} + A_{ji} A_{ij} \]

\[ = \sum_{m=1}^{n} A_{mm} + A_{ii} + A_{jj} = I_n \cdot \sum_{m=1}^{n} A_{mm} = I_n. \]

\[ \therefore \quad h((i\ j)\cdot(i\ j)) = h((i\ j)) \cdot h((i\ j)). \]

Therefore every transposition, and thus every permutation, can be expressed as a permutation matrix.

If a representation is a monomorphism, it is said to faithful. We assert that \( h \) above is faithful.

We shall show if \( p_1 \neq p_2 \), then \( h(p_1) \neq h(p_2) \).

Now, since every two permutations \( p_1 \) and \( p_2 \) can be written as a product of transpositions, then \( p_1 \neq p_2 \) if and only if:

1) one of them (say \( p_1 \)) involves a transposition \( (i\ j) \) which is not a factor of the other.
or 2) if all the transpositions of $p_1$ and $p_2$ are the same, there is at least one pair of nondisjoint transpositions $(i \ j)$ and $(j \ k)$ which appear in different orders in $p_1$ and $p_2$;

provided we write permutations as products of transpositions only in the way described in Lemma 1 on page 9.

Proof: Case 1. Assume $p_1 = t_1 t_2 \cdots (i \ j) t_m t_{m+1} \cdots t_n$ and let $p_2 = t_1 t_2 \cdots (k \ q) t_m t_{m+1} \cdots t_n$. Now since $t_1 t_2 \cdots t_m t_{m+1} \cdots t_n$ will behave exactly the same in $p_1$ and $p_2$ under a homomorphism $h$, we need only consider $h(i \ j)$ and $h(k \ q)$.

$$h(i \ j) = \sum_{m=1}^{n} A_{mm} + A_{ij} + A_{ji} \quad \text{and} \quad h(k \ q) = \sum_{m=1}^{n} A_{mm} + A_{qk} + A_{kj}.$$

Now, by definition of the equality of two $n \times n$ matrices, $A = A''$ if and only if $A_{rs} = A''_{rs}$ for every $(r,s)^{th}$ entry in $A$ and $A''$.

In $h(i \ j)$, $A_{ij} = 1$. In $h(k \ q)$, $A_{ij} = 0$.

$\therefore h(i \ j) \neq h(k \ q)$. $\therefore h(p_1) \neq h(p_2)$.

Case 2. Assume $p_1 = t_1 t_2 \cdots (i \ j)(k \ j) t_m t_{m+1} \cdots t_n$ and $p_2 = t_1 t_2 \cdots (j \ k)(i \ j) t_m t_{m+1} \cdots t_n$.

Since all the other transpositions except $(j \ k)$ and $(i \ j)$ are the same and in the same order, we need consider only $h((i \ j)(j \ k))$ and $h((j \ k)(i \ j))$.

Above we saw that $h((i \ j)(j \ k)) = \sum_{m=1}^{n} A_{mm} + A_{jk} + A_{kj} + A_{ij} + A_{ji} - A_{ik} - A_{ki}$.

Similarly we can show $h((j \ k)(i \ j)) = \sum_{m=1}^{n} A_{mm} + A_{ij} + A_{jk} + A_{ki}$.

Since $A_{ik} \neq A_{ki} \neq A_{ij} \neq A_{ji} \neq A_{jk} \neq A_{kj}$, $h((i \ j)(j \ k)) \neq h((j \ k)(i \ j))$.

$\therefore h(p_1) \neq h(p_2)$.
Therefore representation of permutations by means of matrices is a faithful representation.

Although the representation of groups with permutation matrices has been extensively studied and frequently employed to discover more about groups, this is by no means the only representation possible.

**Definition 25.** Let $G$ be a group and $N \triangleleft G$. The *factor group* $G/N$ is the set of (left) cosets with respect to $N$ multiplied according to the formula: $xN \cdot yN = xyN$. $G/N$ is often called the quotient group of $G$ with respect to $N$.

To show the above definition indeed gives us a group:

1) the identity element is $eN$, since $xN \cdot eN = xeN = xN$.

2) the inverses exist: $xN \cdot x^{-1}N = xx^{-1}N = eN$.

3) $\circ$ is associative: $(xN \cdot yN) \cdot zN = (xyN) \cdot zN = (xy)zN = x(yz)N = xN \circ (yzN) = xN \circ (yN \circ zN)$.

$\therefore G/N$ is a group.

Let us consider the Klein 4 group and the factor group of order two, $V_4/(a)$ where $(a) = \{0, a\}$.

\[ 
\begin{array}{cccc}
\oplus & 0 & a & b & c \\
0 & 0 & a & b & c \\
a & a & 0 & c & b \\
b & b & c & 0 & a \\
c & c & b & a & 0 \\
\end{array} 
\]

Let $h$ be a homomorphism from $V_4$ to $V_4/(a)$. Then

\[ h(g_1 + g_2) = (g_1 + g_2)(a) = g_1(a) + g_2(a) = h(g_1) + h(g_2). \]

Let $k$ be a homomorphism from $V_4/(a)$ to the group of order two. Then $k \cdot h$ would be a homomorphism (since it is the composition of two homomorphisms) from $V_4$ to the group of order two. This is called an induced representation.

First to show $k$ is a homomorphism, let $k((0,a)) = 1$ and $k((b,c)) = -1$. 
Quite obviously, since mere substitution gives one table from another, \( k \) is in fact an isomorphism. We note that \( k \cdot h \) is faithful if and only if \( N \) is the identity group. This representation may of course itself be represented by matrices.

IV. Linear Algebras

We shall now consider vector spaces and algebras and exhibit some representations of them.

Definition 26. A vector space is a system \((V, F, \cdot)\) where:

1) \( F \) is a field (of scalars);

2) \( V \) is a nonempty set of objects called vectors along with an operation \(+\) on \( V \) so that \((V, +)\) is an abelian group;

and 3) \( \cdot \) is a function from \( F \times V \) to \( V \) (called scalar multiplication) such that:

a) \( 1 \alpha = \alpha \) for every \( \alpha \) in \( V \);

b) \((c_1 c_2)\alpha = c_1(c_2\alpha)\);

c) \( c(\alpha + \beta) = c\alpha + c\beta \);

d) \((c_1 + c_2)\alpha = c_1\alpha + c_2\alpha \).

Vectors shall be denoted by Greek letters; scalars shall be denoted by letters of the Roman alphabet.

A well known example is the set of all ordered \( n \)-tuples of real numbers, known as \( n \)-dimensional Euclidean space \( \mathbb{R}^n \).
Definition 27. Let $F$ be a field. A linear algebra over the field $F$ is a vector space $\mathcal{A}$ over $F$ with an additional operation called multiplication of vectors which associates with each pair of vectors $\alpha$, $\beta$ in $\mathcal{A}$ a vector $\alpha \beta$ in $\mathcal{A}$ called the product of $\alpha$ and $\beta$ in such a way that:

1) $\alpha(\beta \rho) = (\alpha \beta)\rho$;
2) $\alpha(\beta + \rho) = \alpha\beta + \alpha\rho$ and $(\alpha + \beta)\rho = \alpha\rho + \beta\rho$;
3) for each scalar $c$ in $F$, $c(\alpha\beta) = (c\alpha)\beta = \alpha(c\beta)$.

Example: The set of $n \times n$ matrices over a field, with usual operations, is a linear algebra with identity. In particular, the field itself is an algebra with identity (over itself).

We shall now concern ourselves with representing these abstract "things" called vectors and algebras as matrices and showing this representation to be a homomorphism. In order to do this we need some basic definitions.

Definition 28. Let $V$ be a vector space over $F$. A subset $S$ of $V$ is said to be linearly dependent if there exist distinct vectors $\alpha_1$, $\alpha_2$, $\ldots$, $\alpha_n$ in $S$, and scalars $c_1$, $c_2$, $\ldots$, $c_n$ in $F$, not all of which are zero, such that $c_1\alpha_1 + c_2\alpha_2 + \ldots + c_n\alpha_n = 0$.

A set which is not linearly dependent is called linearly independent.

Definition 29. Let $V$ be a vector space. A basis for $V$ is a linearly independent set $\mathcal{B}$ of vectors in $V$ which spans $V$, i.e., every vector $\alpha \in V$ can be expressed as: $\alpha = a_1\beta_1 + a_2\beta_2 + \ldots + a_n\beta_n$ where $\beta_i \in \mathcal{B}$, $i = 1, 2, \ldots, n$.

Example 1. The standard basis for $\mathbb{R}^n$, consisting of $e_1$, $e_2$, $\ldots$, $e_n$ defined by: $e_1 = (1, 0, 0, \ldots, 0)$; $e_2 = (0, 1, 0, \ldots, 0)$; $\ldots$ $e_n = (0, 0, 0, \ldots, 1)$ is a well-known example.

Example 2. In the example of a matrix algebra, the basis elements would be of the form: $\beta_{ij} = n \times n$ matrix with 1 in the $(i,j)$th place and
0's elsewhere. Then \( I_n \) (the identity matrix) = \( \sum_{i=1}^{n} \beta_{ii} \), and any other \( n \times n \) matrix
\[
\begin{pmatrix}
\alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\
\alpha_{21} & \alpha_{22} & \cdots & \alpha_{2n} \\
\vdots & \vdots & \ddots & \vdots \\
\alpha_{n1} & \alpha_{n2} & \cdots & \alpha_{nn}
\end{pmatrix}
\]
\( = \sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_{ij} \beta_{ij} \).

Therefore this definition does give a generating set which is clearly independent.

**Definition 30.** The mapping \( A \) from vector space \( V(F) \) to a vector space \( W(F) \) is a vector space homomorphism from \( V(F) \) to \( W(F) \) if and only if:

\[
(a \alpha + b \beta)A = a(\alpha)A + b(\beta)A,
\]
for any \( a \) and \( b \) in \( F \) and any \( \alpha \) and \( \beta \) in \( V \).

**Notation:** If we have a homomorphism \( A \) as defined above from \( V(F) \) to \( V(F) \), we shall denote this statement by \( A \in \text{Hom}_F(V,V) \), read "\( A \) is a vector space homomorphism from the vector space \( V \) over the field \( F \) to itself over \( F \)."

**Definition 31.** Let \( \mathcal{A}_1 \) and \( \mathcal{A}_2 \) be algebras over the field \( F \). An algebra homomorphism is a vector space homomorphism which is also a ring homomorphism, that is, it also preserves multiplication.

**Definition 32.** The dimension of a vector space \( V(F) \), denoted \( \dim(V) \), is the number of elements in a basis of \( V(F) \). \( V(F) \) is finite-dimensional if a basis contains only a finite number of vectors.

**Definition 33.** The dimension of an algebra \( \mathcal{A} \) (as an algebra) equals its dimension as a vector space.

**Theorem 4.** If \( \dim(V) = n \), (i.e., there are \( n \) elements in a basis \( \mathcal{B}_1 \) of a finite vector space \( V(F) \)), then every basis of \( V(F) \) has \( n \) elements.

**Proof:** Case 1. \( \mathcal{B}_2 \) equals a set of vectors with more than \( n \) vectors.
We shall prove that \( \mathcal{B}_2 \) is linearly dependent.

If \( \dim(\mathcal{B}_2) = x, \ x = n + 1 \), then each \( \beta_i^* \in \mathcal{B}_2, \ i \in \{1, 2, \ldots, x\} \) can be expressed in terms of \( \beta_i \in \mathcal{B}_1, \ i \in \{1, 2, \ldots, n\} \).

\[
\beta_1^* = a_1\beta_1 + a_2\beta_2 + \ldots + a_n\beta_n \quad \text{which implies} \\
\beta_1 = a_1^{-1}\beta_1^* - a_1^{-1}a_2\beta_2 - \ldots - a_1^{-1}a_n\beta_n; \\
\beta_2^* = b_1\beta_1^* + b_2\beta_2 + \ldots + b_n\beta_n \quad \text{which implies} \\
\beta_2 = b_1^{-1}\beta_2^* - b_1^{-1}b_2\beta_2^* - \ldots - b_1^{-1}b_n\beta_n; \\
\vdots \\
\vdots \\
\beta_n^* = n_1\beta_1^* + n_2\beta_2^* + \ldots + n_n\beta_n \quad \text{which implies} \\
\beta_n = n_1^{-1}\beta_n^* - n_1^{-1}n_2\beta_n^* - \ldots - n_1^{-1}n_n\beta_n^* - 1.
\]

Then \( \beta_x^* \) (where \( x = n + 1 \)) can also be expressed in terms of \( \beta_i \)'s, i.e.,

\[
\beta_x^* = x_1\beta_1 + x_2\beta_2 + \ldots + x_n\beta_n. 
\]

But from the above implications,

\[
\beta_x^* = y_1\beta_1^* + y_2\beta_2^* + \ldots + y_n\beta_n^*. 
\]

Therefore \( \beta_x^* \) can be expressed in terms of the vectors in \( \mathcal{B}_2 \), so \( \mathcal{B}_2 \) is linearly dependent and thus not a basis. Therefore \( \dim(V) \neq n \).

Case 2. \( \mathcal{B}_3 \) has \( m \) vectors, \( m = n - 1 \). Assume it is a basis. Then \( \beta_i \in \mathcal{B}_1 \) can be expressed in terms of \( \beta_i'' \), where \( \beta_i'' \in \mathcal{B}_3 \). Since we have \( n \) equations in \( n - 1 \) variables, by elementary algebra (simultaneous equations) we get \( \sum a_1^i \beta_i = 0 \). But since \( \mathcal{B}_1 \) is a basis, the vectors are linearly independent and this is a contradiction. Therefore \( \mathcal{B}_3 \) is not a basis. Thus \( \dim(V) \neq n \). Therefore the dimension of a vector space is unique.

**Definition 34.** Let \( \mathcal{A} \) be a finite dimensional linear associative algebra over a field \( F \). Let \( V \) be a finite dimensional vector space over \( F \).

A representation of \( \mathcal{A} \) is an algebra homomorphism from \( \mathcal{A} \) to \( \text{Hom}_F(V, V) \).
**Theorem 5.** Let $\mathcal{A}$ be an $n$ dimensional algebra over the field $F$. Then $\mathcal{A}$ has a faithful representation in $\text{Hom}_F(V,V)$; i.e., there is an algebra monomorphism from $\mathcal{A}$ to $\mathcal{M}_k(F)$ where $k$ is to be specified.

**Proof:** Case 1. $\mathcal{A}$ has an identity. In this case map $\mathcal{A}$ faithfully into $\mathcal{M}_n(F)$. Let $\mathcal{B} = \{\tilde{\beta}_1, \tilde{\beta}_2, \ldots, \tilde{\beta}_n\}$ be a basis for $\mathcal{A}$ with multiplication of the basis defined by:

$$\tilde{\beta}_i \cdot \tilde{\beta}_j = \sum_{k=1}^{n} \alpha_{ijk} \tilde{\beta}_k.$$

Define $\varphi : \mathcal{B} \rightarrow \mathcal{M}_n(F)$ by mapping, and $\varphi(\tilde{\beta}_i) = \mathcal{M}_{rs}$ where $\mathcal{M}_{rs}$ is the matrix of structural constants $(\alpha_{rs})$, i.e., the $n \times n$ matrix whose $(r,s)^{th}$ entry is the structural constants $\alpha_{rs}$.

$$\mathcal{M}_{rs} = \sum_{s=1}^{n} \alpha_{rs} \beta_{rs},$$

the linear extension of $\varphi$ to all of $\mathcal{A}$ is an algebra monomorphism. This makes the extension of $\varphi$ a vector space homomorphism.

We must now prove $\varphi$ is an algebra homomorphism. To verify this assertion, it will be sufficient to prove that:

$$(\tilde{\beta}_i \cdot \tilde{\beta}_j) \varphi = (\tilde{\beta}_i) \varphi \cdot (\tilde{\beta}_j) \varphi \quad \text{(matrix multiplication)}.$$

By definition,

\begin{align*}
(\tilde{\beta}_i \cdot \tilde{\beta}_j) \varphi &= \left( \sum_{k=1}^{n} \alpha_{ijk} \tilde{\beta}_k \right) \varphi = \sum_{k=1}^{n} \alpha_{ijk} \varphi(\tilde{\beta}_k) \\
&= \sum_{k=1}^{n} \sum_{r=1}^{n} \sum_{s=1}^{n} \alpha_{ijk} \alpha_{rks} \beta_{rs},
\end{align*}

(1)

On the other hand:

\begin{align*}
(\tilde{\beta}_i) \varphi \cdot (\tilde{\beta}_j) \varphi &= \left( \sum_{k=1}^{n} \sum_{r=1}^{n} \alpha_{rik} \beta_{rk} \right) \left( \sum_{m=1}^{n} \sum_{s=1}^{n} \alpha_{mjs} \beta_{rs} \right) \\
&= \sum_{r=1}^{n} \sum_{s=1}^{n} \sum_{k=1}^{n} \sum_{l=1}^{n} \alpha_{rik} \alpha_{mjs} \beta_{rs},
\end{align*}

(2)

We now need to conclude the equality of (1) and (2) above. But $\sum_{k=1}^{n} \alpha_{ijk} \alpha_{rks}$

$$= \sum_{k=1}^{n} \alpha_{rik} \alpha_{kjs} \quad \text{(this relation will be shown to follow from the associativity of the multiplication of basis elements of $\mathcal{A}$); that is if:}$$
\[ \tilde{\beta}_i \cdot [\tilde{\beta}_j, \tilde{\beta}_k] = [\tilde{\beta}_i \tilde{\beta}_j] \cdot \tilde{\beta}_k \]

\[ \sum_{q=1}^{n} \alpha_{jkq} \tilde{\beta}_q = \sum_{q=1}^{n} \alpha_{ijq} \tilde{\beta}_q \cdot \tilde{\beta}_k \]

\[ \sum_{p=1}^{n} \alpha_{ijk} a_ipq \tilde{\beta}_p = \sum_{p=1}^{n} \alpha_{ijp} a_kpq \tilde{\beta}_p. \]

Therefore, \( \sum_{q=1}^{n} \alpha_{ijk} a_ipq = \sum_{q=1}^{n} \alpha_{ijp} a_kpq \). Using this it is evident that

\[ \sum_{k=1}^{n} \alpha_{ijk} \alpha_{rks} = \sum_{k=1}^{n} \alpha_{rik} \alpha_{kjs}. \]

Therefore, \( \phi \) is an algebra homomorphism.

Finally \( \phi \) is one-to-one: we shall show the kernel of \( \phi \) is the zero element of \( \mathbb{R} \).

Let \( A \in \mathbb{R} \) be in the kernel of \( \phi \). Then \( A = \sum_{i=1}^{n} a_i \tilde{\beta}_i \).

Now \( A = AI; \) therefore, \( A \phi = (AI) \phi \).

\[ \sum_{s=1}^{n} \sum_{r=1}^{n} a_i \alpha_{ris} \delta_{rs} = \sum_{s=1}^{n} \sum_{r=1}^{n} 0 \delta_{rs}. \]

Therefore, for all \( r \) and \( s \), \( \sum_{i=1}^{n} a_i \alpha_{ris} = 0 \). Since \( \phi \) has an identity \( I \), there exist combinations of the subscripts \( r \) and \( s \) so that for all \( i \), \( \alpha_{ris} \neq 0 \). Therefore \( \phi \) is an algebra monomorphism.

Case 2. \( \mathbb{R} \) has no unity element. Imbed \( \mathbb{R} \) into a ring \( \mathbb{R}^* \) with unity and use the representation from Case 1.

Definition 35. Let \( R_1 \) and \( R_2 \) be rings. If \( R_2 \) has a subring \( R_1^* \) so that \( R_1^* \cong R_1 \), then \( R_1 \) is said to be imbedded in \( R_2 \).

There is a well known theorem that every ring can be imbedded into a ring with identity. \(^1\)

Example: A faithful representation of the complex numbers as $2 \times 2$ real matrices. The complex numbers are of dimension 2 over the real numbers (we may think of complex numbers as ordered pairs $(a, b)$ where $a$ and $b$ are real numbers; and $(a, b) + (c, d) = (a + c, b + d)$ and $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$.)

There is a natural basis for complex numbers over $\mathbb{R}^1$:

$\mathfrak{B} = \{1 = (1,0) = b_1, \ i = (0,1) = b_2 \}$ with multiplication table:

<table>
<thead>
<tr>
<th></th>
<th>$(1,0)$</th>
<th>$(0,1)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(1,0)$</td>
<td>$(1,0)$</td>
<td>$(0,1)$</td>
</tr>
<tr>
<td>$a_{11}$</td>
<td>$a_{12}$</td>
<td>$a_{12}$</td>
</tr>
<tr>
<td>$(0,1)$</td>
<td>$(0,1)$</td>
<td>$(-1,0)$</td>
</tr>
<tr>
<td>$a_{21}$</td>
<td>$a_{22}$</td>
<td>$a_{22}$</td>
</tr>
</tbody>
</table>

Then, $1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $i = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

Now we consider the complex cube roots of 1.

$a = \omega = \frac{-1 + \sqrt{-3}}{2}$ and $b = \omega^2 = \frac{-1 - \sqrt{-3}}{2}$ (that is, $a$ is represented by the matrix)

\[
\begin{pmatrix}
-1/2 & \sqrt{3}/2 \\
-\sqrt{3}/2 & -1/2
\end{pmatrix}
\]

and by matrix multiplication,

\[
a^2 = \begin{pmatrix}
-1/2 & \sqrt{3}/2 \\
-\sqrt{3}/2 & -1/2
\end{pmatrix} \begin{pmatrix}
-1/2 & \sqrt{3}/2 \\
-\sqrt{3}/2 & -1/2
\end{pmatrix} = \begin{pmatrix}
1/4 - 3/4 & -3/2 \\
3/2 & -3/4 + 1/4
\end{pmatrix} = b.
\]

Similarly $b^2 = a$, and of course $a^3 = l = b^3$. 

This gives us the table below which is clearly a finite cyclic group of order 3.

<table>
<thead>
<tr>
<th></th>
<th>e</th>
<th>a</th>
<th>b</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td>e</td>
<td>a</td>
<td>b</td>
</tr>
<tr>
<td>a</td>
<td>a</td>
<td>b</td>
<td>e</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>e</td>
<td>a</td>
</tr>
</tbody>
</table>

V. Conclusion

To conclude this paper, I shall emphasize a point made in the introduction, namely that all of this abstract theory is not merely a mathematical game or fantasy. In the field of quantum mechanics, the permutation group helps explain the structure of the periodic table, energy and momentum laws of quantum physics, and wave theory. The symmetric permutation group is a vital tool in the perturbation theory for the construction of molecules, spin, and valence. There also is a group theoretic classification of atomic spectra. Although one of the oldest fields of mathematics, group theory has far reaching applications in modern day science.
Bibliography


