Advances in Linear Algebra & Matrix Theory, 2021, 11, 117-134
https://www.scirp.org/journal/alamt
ISSN Online: 2165-3348
ISSN Print: 2165-333X

Representations of Lie Groups

Amor Hasić

Department of Mathematics, Faculty of Natural Sciences and Mathematics, University of Montenegro, Podgorica, Montenegro
Email: amorhasic@gmail.com

How to cite this paper: Hasić, A. (2021) Representations of Lie Groups. *Advances in Linear Algebra & Matrix Theory*, **11**, 117-134.
https://doi.org/10.4236/alamt.2021.114009

Received: September 12, 2021
Accepted: November 13, 2021
Published: November 16, 2021

Copyright © 2021 by author(s) and Scientific Research Publishing Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/
Open Access

Abstract

In this paper, the most important liner groups are classified. Those that we often have the opportunity to meet when studying linear groups as well as their application in left groups. In addition to the introductory part, we have general linear groups, special linear groups, octagonal groups, symplicit groups, cyclic groups, dihedral groups: generators and relations. The paper is summarized with brief deficits, examples and evidence as well as several problems. When you ask why this paper, I will just say that it is one of the ways I contribute to the community and try to be a part of this little world of science.

Keywords

Algebras, Groups, Lie Groups, Lie Algebra

1. Introduction

Algebra is the mathematical discipline that arose from the problem of solving equations [1]. If one starts with the integers Z, one knows that every equation $a+x=b$, where a and b are integers, has a unique solution. However, the equation $ax=b$ does not necessarily have a solution in Z, or it might have infinitely many solutions (take $a=b=0$). So let us enlarge Z to the rational numbers Q, consisting of all fraction's c/d, where $d \neq 0$. Then both equations have a unique solution in Q, provided that $a \neq 0$ for the equation $ax=b$. So, Q is a field. If, for example, one takes the solutions of an equation such as $x^2-5=0$ and forms the set of all numbers of the form $a+b\sqrt{5}$, where a and b are rational, we get a larger field, denoted by $Q(\sqrt{5})$, called *an algebraic number field*. In the study of fields obtained by adjoining the roots of polynomial equations, a new notion arose, namely, the symmetries of the field that permute the roots of the equation. Evariste Galois (1811-1832) coined the term *group* for these symmetries, and now this group is called the Galois group of the field. While still a tee-

nager, Galois showed that the roots of an equation are expressible by radicals if and only if the group of the equation has a property now called solvability. This stunning result solved the 350-year-old question whether the roots of every polynomial equation are expressible by radicals.

[1]Linear Groups is the Accent on Infinite Dimensionality explores some of the main results and ideas in the study of infinite-dimensional linear groups. The theory of finite-dimensional linear groups is one of the best developed algebraic theories. The array of articles devoted to this topic is enormous, and there are many monographs concerned with matrix groups, ranging from old, classical texts to ones published more recently. However, in the case when the dimension is infinite (and such cases arise quite often), the reality is quite different.

The situation with the study of infinite-dimensional linear groups is like the situation that has developed in the theory of groups, in the transition from the study of finite groups to the study of infinite groups which appeared about one hundred years ago. It is well known that this transition was extremely efficient and led to the development of a rich and central branch of algebra: Infinite group theory.

Group theory arose from the study of polynomial equations [2]. The solvability of an equation is determined by a group of permutations of its roots; before Abel [1824] and Galois [1830] mastered this relationship, it led Lagrange [1770] and Cauchy [1812] to investigate permutations and prove forerunners of the theorems that bear their names. The term "group" was coined by Galois. Interest in groups of transformations, and in what we now call the classical groups, grew after 1850; thus, Klein's *Erlanger Programmed* [1872] emphasized their role in geometry. Modern group theory began when the axiomatic method was applied to these results; Burnside's *Theory of Groups of Finite Order* [1897] marks the beginning of a new discipline, abstract algebra, in that structures are defined by axioms, and the nature of their elements is irrelevant.

Definition 1.1. A *group* is a set G, together with a map of $G \times G$ into G with the following properties:

- Closure: For all $x, y \in G$, We have
$$x \cdot y \in G$$
- Associativity: For all $x, y, z \in G$.
$$(xy)z = x(yz)$$
- There exists an element e in G such that for all $x \in G$,
$$x \cdot e = e \cdot x = x$$

The element e is unique, and is called the identity element of the group, or simply the identity.

- and such that for all $x \in G$, there exists $x' \in G$ with
$$x \cdot x' = x' \cdot x = e$$

[1]https://www.routledge.com/Linear-Groups-The-Accent-on-Infinite-Dimensionality/Dixon-Kurdachenko-Subbotin/p/book/9781138542808.

is called an inverse of *x*.

Definition 1.2. A group G is said to be *commutative* or *abelian* if all $x, y \in G$, we have $x \cdot y = y \cdot x$. A group that is not abelian is said to benonabelian.

Proposition 1.3. (Uniqueness of the Identity). Let G be a group, and let $e, f \in G$ be such that for all $x \in G$.

$$e \cdot x = x \cdot e = x$$

$$f \cdot x = x \cdot f = x$$

Then $e = f$.

Proof. Since *e* is an identity, we have

$$e \cdot f = f$$

On the other hand, since *f* is an identity, we have

$$e \cdot f = e$$

Thus $e = e \cdot f = f$.

Proposition 1.4 (Uniqueness of Inverses). Let G be a group, *e* the (unique) identity of *G*, and $x, y, z \in G$. Suppose that

$$x \cdot y = y \cdot x = e$$

$$x \cdot z = z \cdot x = e$$

Then $y = z$.

Proof: We know that $x \cdot y = x \cdot z = e$. Multiplying on the left by *h* gives $y \cdot (x \cdot y) = y \cdot (x \cdot z)$.

By as sociativity, this gives

$$(y \cdot x) \cdot y = (y \cdot x) \cdot z$$

and so

$$e \cdot y = e \cdot z$$

$$y = z.$$

Proposition 1.5. [1] *For all* $x, y \in G$, *we have* $(xy)^{-1} = y^{-1}x^{-1}$.

Proof: Let $w = y^{-1}x^{-1}$. Then it suffices to show that $w(xy) = 1$. But

$$w(xy) = (wx)y = \left(\left(y^{-1}x^{-1}\right)x\right)y = \left(y^{-1}\left(x^{-1}x\right)\right)y = \left(y^{-1}1\right)y = y^{-1}y = 1.$$

If $x^1, x^2, \cdots, x^n$ are arbitrary elements of a group *G*, then the expression $x^1x^2\cdots x^n$ will stand for $x^1\left(x^2\cdots x^n\right)$, where $x^2\cdots x^n = x^2\left(x^3\cdots x^n\right)$ and soon. This gives an inductive definition of the product of an arbitrary finite number of elements of *M*oreover, by as sociativity, pairs $(\cdots)$ of parentheses can be inserted or removed in the expression $x^1x^2\cdots x^n$ without making any change in the group element being represented, provided the new expression makes sense. (For example, you can't have an empty pair of parentheses, and the number of left parentheses has to be the same as the number of right parentheses).

$$\left(y^{-1}x^{-1}\right)(xy) = y^{-1}\left(x^{-1}x\right)y^{-1} = y1y^{-1} = 1.$$

Definition 1.6. A *subgroup* of a group G is a subset H of G with the following

properties:

1) The identity is an element of *H*.

2) If $h \in H$, then $h^{-1} \in H$.

3) If $h_1, h_2 \in H$, then $h_1 \cdot h_2 \in H$.

Proposition 1.7. A subset *H* of a group *G* is a subgroup if and only if *H* is a group under the group operations of *G*. That is, *H* is closed under the group operation and contains the identity of *G*, and the inverse of an element of *H* is its inverse in *G*.

Definition 1.8. Let *G* and *H* be groups. A *homomorphism* from *G* to *H* is a map $\varphi : G \to H$ such that, for all x, y in *G*, $\varphi(x \cdot y) = \varphi(x)\varphi(y)$.

Proposition 1.9. Let *G* and *H* be groups and $\varphi : G \to H$ be a homomorphism, Then for all x, y in *G*,

$$\varphi\left(xy^{-1}\right) = \varphi(x)\varphi(y)^{-1} \quad \text{and} \quad \varphi\left(yx^{-1}\right) = \varphi(y)\varphi(x)^{-1}$$

Proof: We have

$$\varphi\left(xy^{-1}\right)\varphi(y) = \varphi\left(\left(xy^{-1}\right)y\right) = \varphi\left(xy^{0}\right) = \varphi(x)$$

Since φ is a homomorphism.

Definition 1.10. A homomorphism from *G* to *H* which is a bijection is an *isomorphism.* In that case, we say that *G* and *H* are isomorphic, and write $G \cong H$.

Definition 1.11. A bijective homomorphism φ from a group to itself is an *automorphism.*

Example 1.12. Let R^* denote the nonzero real numbers. Multiplication by $a \in R^*$ defines a bijection $\mu_a : R \to R$ given by $\mu_a(r) = ar$. The distributive law for *R* says that

$$\mu_a(r+s) = a(r+s) = ar + as = \mu_a(r) + \mu_a(s)$$

for all $r, s \in R$. Thus $\mu_a : R \to R$ is a homomorphism for the additive group structure on *R*. Since $a \neq 0$, *a* is in fact an isomorphism. Furthermore, the associative and commutative laws for *R* imply that $a(rs) = (ar)s = (ra)s = r(as)$. Hence,

$$\mu_a(rs) = r\mu_a(s).$$

2. The Classical Groups

In this study the structure of a classical group *G* and its Lie algebra [3]. We choose a matrix realization of *G* such that the diagonal subgroup $H \subset G$ is a maximal torus; by elementary linear algebra every conjugacy class of semi simple elements intersects *H*. Using the unipotent elements in *G*, we show that the groups *GL*(*n*,*R*), *SL*(*n*,*R*), *SO*(*n*,*R*), and *U*(*n*,*C*) are connected (as Lie groups and as algebraic groups). This group and its Lie algebra play a basic role in the structure of the other classical groups and Lie algebras. We decompose the Lie algebra of a classical group under the adjoint action of a maximal torus and find the invariant subspaces (called root spaces) and the corresponding characters

(called roots). The commutation relations of the root spaces are encoded by the set of roots; we use this information to prove that the classical (trace-zero) Lie algebras are simple (or semi simple). In the final section of the chapter, we develop some general Lie algebra methods (solvable Lie algebras, killing form) and show that every semi simple Lie algebra has a root-space decomposition with the same properties as those of the classical Lie algebras.

Definition 1.13. The classical groups are the groups of invertible linear transformations of finite-dimensional vector spaces over the real, complex, and quaternion fields, together with the subgroups that preserve a volume form or a bilinear form.

Proposition 1.14. The determinant function $\det : M_n \to k$: has the following properties.

i) For $A, B \in M_n(k)$, $\det(AB) = \det A \cdot \det B$.

ii) $\det I_n = 1$.

iii) $A \in M_n(k)$ is invertible if and only if $\det A \neq O$.

3. General Linear Groups *GL*(*n*,*R*)

$$GL(n,R) = \left\{ A = \left[a_{ij} \right]_{n\times n} \middle| \det A \neq 0, (|A| \neq 0) \right\}$$

- **Closure property**

Let $A, B \in GL(n,R)$ then $|A| \neq 0, |B| \neq 0$

$$|A \cdot B| = |A| \cdot |B|$$

$$|A| \neq 0, |B| \neq 0$$

$$|A| \cdot |B| \neq 0 \quad i.e.$$

$$|A \cdot B| \neq 0 A \cdot B \in GL(n,R)$$

$$|A| = \det A, |B| = \det B$$

$$\det(AB) = \det A \cdot \det B$$

$$\Rightarrow \det(AB) \neq 0 \quad i.e.$$

$$\Rightarrow \det A \neq 0, \det B \neq 0$$

$$\Rightarrow A \cdot B \in GL(n,R)$$

- **Associative property**

$$A \cdot (B \cdot C) = (A \cdot B) \cdot C, \forall A, B, C \in GL(n,R)$$

- **Existence of identity**

$$I_{n\times n} = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}_{n\times n}$$. Such that

$$|I| = 1 \neq 0$$

$$A \cdot I_{n\times n} = A = I_{n\times n} \cdot A$$

- **Existence of inverse**

Let $A \in GL(n,R)$, $|A| \neq 0$.

$$A^{-1} = \frac{1}{|A|}(adjA)$$

$$|A^{-1}| = \left|\frac{1}{|A|}(adjA)\right|$$

$$\Rightarrow \frac{(adjA)}{(A)^n} = \frac{|A|^{n-1}}{|A|^n} = \frac{1}{|A|} \neq 0$$

$$A \cdot A^{-1} = A \cdot \frac{1}{|A|}(adjA) = \frac{A \cdot (adjA)}{|A|}$$

$$\Rightarrow \frac{|A| \cdot I}{|A|} = I$$

- **Commutativity**

$(GL(n,R),\cdot)$ group is not Abellio group because $AB \neq BA$.

Let F denote either the field of real numbers R or the field of complex numbers C, and let V be a finite-dimensional vector space over F [3]. The set of invertible linear transformations from V to V will be denoted by $GL(V)$. This set has a group structure under composition of transformations, with identity element the identity transformation $I(x) = x$ for all $x \in V$. The group $GL(V)$ is the first of the classical groups. To study it in more detail, we recall some standard terminology related to linear transformations and their matrices. Let V and W be finite-dimensional vector spaces over F. Let $\{v_1,\cdots,v_n\}$ and $\{w_1,\cdots,w_m\}$ be bases for V and W, respectively. If $T: V \to W$ is a linear map then

$$Tv_j = \sum_{i=1}^{m} a_{ij} w_i \quad \text{for } j = 1,\cdots,n$$

with $a_{ij} \in F$. The numbers a_{ij} are called the matrix coefficients or entries of T with respect to the two bases, and the $m \times n$ array

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

Let $S: W \to U$ be another linear transformation, with U an l-dimensional vector space with basis $\{u_1,\cdots,u_n\}$, and let B be the matrix of S with respect to the bases $\{w_1,\cdots,w_m\}$ and $\{u_1,\cdots,u_n\}$, Then the matrix of $S \circ T$ with respect to the bases $\{v_1,\cdots,v_n\}$ and $\{u_1,\cdots,u_n\}$, is given by BA, with the product being the usual product of matrices.

We denote the space of all $n \times n$ matrices over F by $M_n(F)$, and we denote the $n \times n$ identity matrix by I (or in if the size of the matrix needs to be indicated); it has entries $\delta_{ij} = 1$ if $i = j$ and 0 otherwise. Let V be an n-dimensional vector space over F with basis $\{v_1,\cdots,v_n\}$. If $T: V \to V$ is a linear map we write

$\mu(T)$ for the matrix of T with respect to this basis. If $T,S \in GL(V)$ then the preceding observations imply that $\mu(S \circ T) = \mu(S)\mu(T)$. Furthermore, if $T \in GL(V)$ then $\mu(T \circ T^{-1}) = \mu(T^{-1} \circ T) = \mu(Id) = I$. The matrix $A \in M_n(F)$ is said to be invertible if there is a matrix $B \in M_n(F)$ such that $AB = BA = I$. We note that a linear map $T: V \to V$ is in $GL(V)$ if and only if its matrix $\mu(T)$ is invertible. We also recall that a matrix $A \in M_n(F)$ is invertible if and only if its determinant is nonzero.

We will use the notation $GL(n,F)$ for the set of *n_n* invertible matrices with coefficients in *F*. Under matrix multiplication $GL(n,F)$ is a group with the identity matrix as identity element. We note that if V is an *n*-dimensional vector space over F with basis $\{v_1,\cdots,v_n\}$, then the map $\mu: GL(V) \to GL(n,F)$ corresponding to this basis is a group isomorphism. The group $GL(n,F)$ is called the general linear group of rank *n*.

If $\{w_1,\cdots,w_m\}$ is another basis of *V*, then there is a matrix $g \in GL(n,F)$ such that

$$w_{ij} = \sum_{i=1}^{n} g_{ij} v_i \quad \text{and} \quad v_j = \sum_{i=1}^{n} h_{ij} w_i \quad \text{for } j = 1,\cdots,n$$

with $[h_{ij}]$ the inverse matrix to $[g_{ij}]$. Suppose that T is a linear transformation from V to V, that $A = [a_{ij}]$ is the matrix of T with respect to a basis $\{v_1,\cdots,v_n\}$, and that $B = [b_{ij}]$ is the matrix of T with respect to another basis $\{w_1,\cdots,w_m\}$. Then

$$Tw_j = T\left(\sum_i g_{ij} v_i\right) = \sum_i g_{ij} T v_i = \sum_i g_{ij}\left(\sum_k a_{ki} v_k\right) = \sum_l \left(\sum_k \sum_i h_{lk} a_{ki} g_{ij}\right) w_l$$

for $j = 1,\cdots,n$. Thus $B = g^{-1}Ag$ is similar to the matrix *A*.

4. Special Linear Group *SL*(*n*,*R*)

$$SL(n,R) = \left\{ A = [a_{ij}]_{n\times n} \in GL(n,R) \middle| \det A = 1, (|A| = 1) \right\}$$

- Closure property

Let $A,B \in SL(n,R)$ then $|A| = 1, |B| = 1$

$$|A \cdot B| = |A| \cdot |B|$$

$$|A| = 1, |B| = 1$$

$$|A| \cdot |B| = 1 \cdot 1 = 1 \quad i.e.$$

$$|A \cdot B| = 1$$

$$A \cdot B \in SL(n,R)$$

$$|A| = \det A, |B| = \det B$$

$$\det(AB) = \det A \cdot \det B$$

$$\Rightarrow \det(AB) = 1 \cdot 1 = 1 \quad i.e.$$

$$\Rightarrow \det A = 1, \det B = 1$$

$$\Rightarrow A \cdot B \in SL(n,R)$$

- Associative property

$$A \cdot (B \cdot C) = (A \cdot B) \cdot C, \forall A,B,C \in SL(n,R)$$

- Existence of identity

$$I_{n\times n} = [a_{ij}]_{n\times n} = \begin{cases} 1, i = j \\ 0, i \neq j \end{cases}$$

Such that

$$|I| = 1$$

$$A \cdot I_{n\times n} = A = I_{n\times n} \cdot A$$

- Existence of inverse

Let $A \in SL(n,R)$,

$$|A| = 1.$$

$$A^{-1} \text{ exist}$$

$$|A^{-1}| = |A|^{-1} = \frac{1}{|A|^1} = \frac{1}{1} = 1$$

$$A^{-1} \in SL(n,R)$$

- **Commutativity**

$(SL(n,R),\cdot)$ is a group but not Abellio group because $AB \neq BA$.

The special linear group $SL(n,R)$ is the set of all elements A of $M_n(R)$ such that $\det(A) = 1$ [3]. Since $\det(AB) = \det(A)\det(B)$ and $\det(I) = 1$, we see that the special linear group is a subgroup of $GL(n,R)$.

We note that if V is an n-dimensional vector space over F with basis $\{v_1, \cdots, v_n\}$. and if $\mu : GL(V) \to GL(n,R)$ is the map previously defined, then the group

$$\mu^{-1}(SL(n,R)) = \{T \in GL(V) : \det(\mu(T)) = 1\}$$

is independent of the choice of basis, by the change of basic formula. We denote this group by $SL(V)$.

5. Orthogonal and Special Orthogonal Group

$$O(n,R) = \left\{ A = [a_{ij}]_{n\times n} \in GL(n,R) \middle| AA^{\mathrm{T}} = I_n \right\}$$

Definition 4.1. The matrix obtained by replacing the same numbered rows and columns of a matrix A is called the transposition of A and is denoted by A^{T}. Accordingly, $A = [a_{ij}]$, $m \times n$-matrix, $A^{\mathrm{T}} = [a_{ji}]$, $n \times m$-matrix.

$$A = (a_{ij}) \to A^{\mathrm{T}} = (a_{ji})$$

Definition 4.2.

1) A square matrix with $A^{\mathrm{T}} = A$ is called a symmetric matrix. If $A = [a_{ij}]$

is a symmetric matrix then $a_{ij} = a_{ji}$ for each i, j.

2) A square matrix with $A^{\mathrm{T}} = -A$ is called an inverse symmetric matrix. If $A = \left[a_{ij}\right]$ is an inverse symmetric matrix then $a_{ij} = -a_{ji}$ for each i, j. Thus, in an inverse symmetric matrix, the prime diagonal elements are always zero.

Theorem 4.3. A, B are two matrices of the same order and r is a scalar.

1) $(A+B)^{\mathrm{T}} = A^{\mathrm{T}} + B^{\mathrm{T}}$

2) $(rA)^{\mathrm{T}} = rA^{\mathrm{T}}$

3) $\left(A^{\mathrm{T}}\right)^{\mathrm{T}} = A$

4) $(AB)^{\mathrm{T}} = B^{\mathrm{T}} A^{\mathrm{T}}$

Theorem 4.4. A square matrix A is orthogonal if and only if its column vectors form an orthonormal set.

Proof: Let A be an $n \times n$ orthogonal matrix and let $a_1 a_2 \cdots a_n$ be the column vectors of A. Then

$$A^{\mathrm{T}} A = \left(a_{ij}\right)^{\mathrm{T}} a_{ij} = \left(a_i^{\mathrm{T}} a_j\right) = \left(a_i a_j\right)$$

Therefore,

$$A^{\mathrm{T}} A = I_n$$

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \text{ and } A^{\mathrm{T}} = \begin{bmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & \cdots & a_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{mn} \end{bmatrix}$$

$$A^{\mathrm{T}} A = \begin{bmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & \cdots & a_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

$$= \begin{bmatrix} a_{11}a_{11} + a_{21}a_{21} + \cdots + a_{m1}a_{m1} & a_{11}a_{12} + a_{21}a_{22} + \cdots + a_{m1}a_{m2} & \cdots & a_{11}a_{1n} + a_{21}a_{2n} + \cdots + a_{m1}a_{mn} \\ a_{12}a_{11} + a_{22}a_{21} + \cdots + a_{m2}a_{m1} & a_{12}a_{12} + a_{22}a_{22} + \cdots + a_{m2}a_{m2} & \cdots & a_{12}a_{1n} + a_{22}a_{2n} + \cdots + a_{m2}a_{mn} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n}a_{11} + a_{2n}a_{21} + \cdots + a_{mn}a_{m1} & a_{1n}a_{12} + a_{2n}a_{22} + \cdots + a_{mn}a_{m2} & \cdots & a_{1n}a_{1n} + a_{2n}a_{2n} + \cdots + a_{mn}a_{mn} \end{bmatrix}$$

if and only if

$$a_i a_j = \begin{cases} 1, i = j \\ 0, i \neq j \end{cases}$$

$$A^{\mathrm{T}} A = \begin{bmatrix} 1+0+\cdots+0 & 0+0+\cdots+0 & \cdots & 0+0+\cdots+0 \\ 0+0+\cdots+0 & 0+1+\cdots+0 & \cdots & 0+0+\cdots+0 \\ \vdots & \vdots & \ddots & \vdots \\ 0+0+\cdots+0 & 0+0+\cdots+0 & \cdots & 0+0+\cdots+1 \end{bmatrix}$$

$$A^{\mathrm{T}} A = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix} = I_n$$

A simple example 3.5. The matrix

$$A=\begin{bmatrix} 3/\sqrt{11} & -1/\sqrt{6} & -1/\sqrt{66} \\ 1/\sqrt{11} & 2/\sqrt{6} & -4/\sqrt{66} \\ 1/\sqrt{11} & 1/\sqrt{6} & 7/\sqrt{66} \end{bmatrix}_{3\times 3}$$ is orthogonal matrix. Note that

$$A^{\mathrm{T}}A=I_n$$

$$\begin{bmatrix} 3/\sqrt{11} & 1/\sqrt{11} & 1/\sqrt{11} \\ -1/\sqrt{6} & 2/\sqrt{6} & 1/\sqrt{6} \\ -1/\sqrt{66} & -4/\sqrt{66} & 7/\sqrt{66} \end{bmatrix}\begin{bmatrix} 3/\sqrt{11} & -1/\sqrt{6} & -1/\sqrt{66} \\ 1/\sqrt{11} & 2/\sqrt{6} & -4/\sqrt{66} \\ 1/\sqrt{11} & 1/\sqrt{6} & 7/\sqrt{66} \end{bmatrix}$$

$$=\begin{bmatrix} (9+1+1)/11 & (-3+2+1)/\sqrt{66} & (-3-4+7)/\sqrt{726} \\ (-3+2+1)/\sqrt{66} & (1+4+1)/6 & (1-8+7)/\sqrt{396} \\ (-3-4+7)/\sqrt{726} & (1-8+7)/\sqrt{396} & (1+16+49)/66 \end{bmatrix}$$

$$=\begin{bmatrix} 11/11 & 0/\sqrt{66} & 0/\sqrt{726} \\ 0/\sqrt{66} & 6/6 & 0/\sqrt{396} \\ 0/\sqrt{726} & 0/\sqrt{396} & 66/66 \end{bmatrix}=\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}=I_{3\times 3}$$

Consider the determinant function restricted to $O(n)$, $\det: O(n)\to R^*$. For $A\in O(n)$,

$$(\det A)^2=\det A^{\mathrm{T}}\det A=\det\left(A^{\mathrm{T}}A\right)=\det I_n=1,$$

which implies that $\det A=\pm 1$. Thus, we have

$$O(n)=O(n)^+\cup O(n)^-,$$

where

$$O(n)^+=\{A\in O(n):\det A=I\},O(n)^-=\{A\in O(n):\det A=-I\}.$$

6. Special Orthogonal Group

$$SO(n,R)=\left\{A=\left[a_{ij}\right]_{n\times n}\in GL(n,R)\middle| AA^{\mathrm{T}}=I_n,\det A=1\right\}$$

The $SO(n)$ is a subgroup of the orthogonal group $O(n)$ and also known as the special orthogonal group or the set of rotations group.

The orthogonal and special orthogonal groups, $O(n)$ and $SO(n)$ [4]. An $n\times n$ real matrix A is said to be orthogonal if the column vectors that make up A are orthonormal, that is, if

$$\sum_{i=1}^{N}A_{ij}A_{ik}=\delta_{jk}$$

Equivalently, A is orthogonal if it preserves the inner product, namely, if $\langle x,y\rangle=\langle Ax,Ay\rangle$ for all vectors x,y in R^n. (Angled brackets denote the usual inner product on R^n, $\langle x,y\rangle=\sum_i x_i y_i$) Still another equivalent definition is that A is orthogonal if $A^{tr}A=I$, *i.e.*, if $A^{tr}=A^{-1}$. (A^{tr} is the transpose of A, $\left(A^{tr}\right)_{ij}=A_{ji}$.).

Since $\det A^{tr}=\det A$, we see that if A is orthogonal, then

$\det\left(A^{trA}\right)=\left(\det A\right)^2=\det I=1$. Hence $\det A=\pm 1$, for all orthogonal matrices *A*.

This formula tells us, in particular, that every orthogonal matrix must be invertible. But if *A* is an orthogonal matrix, then

$$\left\langle A^{-1}x, A^{-1}y\right\rangle=\left\langle A\left(A^{-1}x\right), A\left(A^{-1}x\right)\right\rangle=\langle x, y\rangle$$

Thus, the inverse of an orthogonal matrix is orthogonal. Furthermore, the product of two orthogonal matrices is orthogonal, since if *A* and *B* both preserve inner products, then so does *AB*. Thus, the set of orthogonal matrices forms a group

The set of all $n\times n$ real orthogonal matrices is the orthogonal group *O*(*n*), and is a subgroup of $GL(n,C)$. The limit of a sequence of orthogonal matrices is orthogonal, because the relation $A^{trA}=I$ is preserved under limits. Thus *O*(*n*) is a matrix Lie group.

The set of $n\times n$ orthogonal matrices with determinant one is the special orthogonal group *SO*(*n*). Clearly this is a subgroup of *O*(*n*), and hence of $GL(n,C)$.

Moreover, both orthogonality and the property of having determinant one is preserved under limits, and so *SO*(*n*) is a matrix Lie group. Since elements of *O*(*n*) already have determinant ±1, *SO*(*n*) is "half" of *O*(*n*).

7. Unitary Groups

$$U(n,C)=\left\{A=\left[a_{ij}\right]_{n\times n}\in GL(n,C)\,\middle|\,A\overline{A^{\mathrm{T}}}=I\right\}$$

For $A=\left[a_{ij}\right]\in M_n(C)$,

$$A^*=\left(\overline{A}\right)^{\mathrm{T}}=\overline{A^{\mathrm{T}}},$$

is the Hermitian conjugate of *A*, *i.e.*, $\left(A^*\right)_{ij}=a_{ji}$.

Definition 3.5. [5] In a matrix *A* whose elements are complex numbers, the matrix obtained by replacing each element with its conjugate is called the conjugate of *A* matrix and is denoted by $\overline{A}$.

Simple Example 5.1:

$$A=\begin{bmatrix}6 & 4+3i & 5i\\ 3 & i & 1-i\\ 3-2i & -i & 1+i\end{bmatrix}\text{ conjugate of the matrix}$$

$$\overline{A}=\begin{bmatrix}6 & 4-3i & -5i\\ 3 & -i & 1+i\\ 3+2i & i & 1-i\end{bmatrix}$$

Theorem 5.2. Let *A*, *B* be two matrices and *k* any scalar.

1) $\overline{\overline{A}}=A$
2) $\overline{(kA)}=\overline{k}\,\overline{A}$
3) $\overline{(A+B)}=\overline{A}+\overline{B}$
4) $\overline{(AB)}=\overline{A}+\overline{B}$

Example 5.3: Let

$$A=\begin{bmatrix}1 & -i & 1-i\\ i & -3 & 2+i\\ 1+i & 5-i & 3\end{bmatrix} \text{ and } B=\begin{bmatrix}1-i & i & 0\\ 3 & 2-2i & -i\end{bmatrix}$$

Note that,

$$A^{*}=\left(\overline{A}\right)^{\mathrm{T}}$$

$$A^{*}=\left(\overline{\begin{bmatrix}1 & -i & 1-i\\ i & -3 & 2+i\\ 1+i & 5-i & 3\end{bmatrix}}\right)^{\mathrm{T}}=\left(\begin{bmatrix}1 & i & 1+i\\ -i & -3 & 2-i\\ 1-i & 5+i & 3\end{bmatrix}\right)^{\mathrm{T}}=\begin{bmatrix}1 & -i & 1-i\\ i & -3 & 5+i\\ 1+i & 2-i & 3\end{bmatrix}$$

$$B^{*}=\left(\overline{\begin{bmatrix}1-i & i & 0\\ 3 & 2-2i & -i\end{bmatrix}}\right)^{\mathrm{T}}=\left(\begin{bmatrix}1+i & -i & 0\\ 3 & 2+2i & i\end{bmatrix}\right)^{\mathrm{T}}=\begin{bmatrix}1+i & 3\\ -i & 2+2i\\ 0 & i\end{bmatrix}$$

Definition 5.4. A square matrix with $\left(\overline{A}\right)'=A$ is called *Hermitian matrix*. If the square matrix $A=a_{ij}$ is the Hermitian matrix, then $a_{ij}=\overline{a_{ji}}$. The diagonal elements of a Hermitian matrix are real numbers.

Simple Example 5.5:

$$A=\begin{bmatrix}1 & i & 1+i\\ -i & -4 & 2-i\\ 1-i & 2+i & 3\end{bmatrix} \text{ matrix is a Hermitian matrix.}$$

Definition 5.6: [5] A square matrix with $\left(\overline{A}\right)'=-A$ is called the *inverse Hermitian matrix*. If the square matrix $A=a_{ij}$ is the inverse Hermitian matrix, then $a_{ij}=-\overline{a_{ji}}$. The diagonal elements of an inverse Hermitian matrix are 0 or their imaginary numbers.

Simple Example 5.7: Let

$$A=\begin{bmatrix}i & 1-i & 5\\ -1-i & 2i & -i\\ -2 & i & 0\end{bmatrix} \text{ matrix is the inverse Hermitian matrix.}$$

Example 5.8: Let $A=\begin{bmatrix}\frac{1}{2}(1+i) & \frac{1}{2}(1+i)\\ \frac{1}{2}(1-i) & \frac{1}{2}(-1+i)\end{bmatrix}$

$$AA^{*}=\begin{bmatrix}\frac{1}{2}(1+i) & \frac{1}{2}(1+i)\\ \frac{1}{2}(1-i) & \frac{1}{2}(-1+i)\end{bmatrix}\left(\overline{\begin{bmatrix}\frac{1}{2}(1+i) & \frac{1}{2}(1+i)\\ \frac{1}{2}(1-i) & \frac{1}{2}(-1+i)\end{bmatrix}}\right)^{\mathrm{T}}$$

$$=\begin{bmatrix}\frac{1}{2}(1+i) & \frac{1}{2}(1+i)\\ \frac{1}{2}(1-i) & \frac{1}{2}(-1+i)\end{bmatrix}\left(\begin{bmatrix}\frac{1}{2}(1-i) & \frac{1}{2}(1-i)\\ \frac{1}{2}(1+i) & \frac{1}{2}(-1-i)\end{bmatrix}\right)^{\mathrm{T}}$$

$$=\begin{bmatrix}\frac{1}{2}(1+i) & \frac{1}{2}(1+i)\\ \frac{1}{2}(1-i) & \frac{1}{2}(-1+i)\end{bmatrix}\begin{bmatrix}\frac{1}{2}(1-i) & \frac{1}{2}(1+i)\\ \frac{1}{2}(1-i) & \frac{1}{2}(-1-i)\end{bmatrix}=\begin{bmatrix}\frac{1}{2}+\frac{1}{2} & \frac{1}{2}-\frac{1}{2}\\ \frac{1}{2}-\frac{1}{2} & \frac{1}{2}+\frac{1}{2}\end{bmatrix}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$$

Theorem 5.9: Let $A=\begin{bmatrix}\frac{1}{2}(a_{11}+ib_{11}) & \frac{1}{2}(a_{12}+ib_{12}) & \cdots & \frac{1}{2}(a_{1n}+ib_{1n})\\ \frac{1}{2}(a_{21}+ib_{21}) & \frac{1}{2}(a_{22}+ib_{22}) & \cdots & \frac{1}{2}(a_{2n}+ib_{2n})\\ \vdots & \vdots & \ddots & \vdots\\ \frac{1}{2}(a_{m1}+ib_{m1}) & \frac{1}{2}(a_{m2}+ib_{2m}) & \cdots & \frac{1}{2}(a_{mn}+ib_{mn})\end{bmatrix}$

$$A\overline{A^{\mathrm{T}}}=I$$

$$A\overline{A^{\mathrm{T}}}=\begin{bmatrix}\frac{1}{2}(a_{11}+ib_{11}) & \frac{1}{2}(a_{12}+ib_{12}) & \cdots & \frac{1}{2}(a_{1n}+ib_{1n})\\ \frac{1}{2}(a_{21}+ib_{21}) & \frac{1}{2}(a_{22}+ib_{22}) & \cdots & \frac{1}{2}(a_{2n}+ib_{2n})\\ \vdots & \vdots & \ddots & \vdots\\ \frac{1}{2}(a_{m1}+ib_{m1}) & \frac{1}{2}(a_{m2}+ib_{2m}) & \cdots & \frac{1}{2}(a_{mn}+ib_{mn})\end{bmatrix}\overline{\begin{bmatrix}\frac{1}{2}(a_{11}+ib_{11}) & \frac{1}{2}(a_{12}+ib_{12}) & \cdots & \frac{1}{2}(a_{1n}+ib_{1n})\\ \frac{1}{2}(a_{21}+ib_{21}) & \frac{1}{2}(a_{22}+ib_{22}) & \cdots & \frac{1}{2}(a_{2n}+ib_{2n})\\ \vdots & \vdots & \ddots & \vdots\\ \frac{1}{2}(a_{m1}+ib_{m1}) & \frac{1}{2}(a_{m2}+ib_{2m}) & \cdots & \frac{1}{2}(a_{mn}+ib_{mn})\end{bmatrix}}^{\mathrm{T}}$$

$$=\begin{bmatrix}\frac{1}{2}(a_{11}+ib_{11}) & \frac{1}{2}(a_{12}+ib_{12}) & \cdots & \frac{1}{2}(a_{1n}+ib_{1n})\\ \frac{1}{2}(a_{21}+ib_{21}) & \frac{1}{2}(a_{22}+ib_{22}) & \cdots & \frac{1}{2}(a_{2n}+ib_{2n})\\ \vdots & \vdots & \ddots & \vdots\\ \frac{1}{2}(a_{m1}+ib_{m1}) & \frac{1}{2}(a_{m2}+ib_{2m}) & \cdots & \frac{1}{2}(a_{mn}+ib_{mn})\end{bmatrix}\begin{bmatrix}\frac{1}{2}(a_{11}-ib_{11}) & \frac{1}{2}(a_{12}-ib_{12}) & \cdots & \frac{1}{2}(a_{1n}-ib_{1n})\\ \frac{1}{2}(a_{21}-ib_{21}) & \frac{1}{2}(a_{22}-ib_{22}) & \cdots & \frac{1}{2}(a_{2n}-ib_{2n})\\ \vdots & \vdots & \ddots & \vdots\\ \frac{1}{2}(a_{m1}-ib_{m1}) & \frac{1}{2}(a_{m2}-ib_{2m}) & \cdots & \frac{1}{2}(a_{mn}-ib_{mn})\end{bmatrix}^{\mathrm{T}}$$

$$=\begin{bmatrix}\frac{1}{2}(a_{11}+ib_{11}) & \frac{1}{2}(a_{12}+ib_{12}) & \cdots & \frac{1}{2}(a_{1n}+ib_{1n})\\ \frac{1}{2}(a_{21}+ib_{21}) & \frac{1}{2}(a_{22}+ib_{22}) & \cdots & \frac{1}{2}(a_{2n}+ib_{2n})\\ \vdots & \vdots & \ddots & \vdots\\ \frac{1}{2}(a_{m1}+ib_{m1}) & \frac{1}{2}(a_{m2}+ib_{2m}) & \cdots & \frac{1}{2}(a_{mn}+ib_{mn})\end{bmatrix}\begin{bmatrix}\frac{1}{2}(a_{11}-ib_{11}) & \frac{1}{2}(a_{21}-ib_{21}) & \cdots & \frac{1}{2}(a_{m1}-ib_{m1})\\ \frac{1}{2}(a_{12}-ib_{12}) & \frac{1}{2}(a_{22}-ib_{22}) & \cdots & \frac{1}{2}(a_{m2}-ib_{2m})\\ \vdots & \vdots & \ddots & \vdots\\ \frac{1}{2}(a_{1n}-ib_{1n}) & \frac{1}{2}(a_{2n}-ib_{2n}) & \cdots & \frac{1}{2}(a_{mn}-ib_{mn})\end{bmatrix}$$

if and only if

$$a_i a_j=\begin{cases}1, i=j\\ 0, i\neq j\end{cases}$$

$$\begin{bmatrix}\frac{1}{2}(1+i\cdot 1) & \frac{1}{2}(0+i\cdot 0) & \cdots & \frac{1}{2}(0+i\cdot 0)\\ \frac{1}{2}(0+i\cdot 0) & \frac{1}{2}(1+i\cdot 1) & \cdots & \frac{1}{2}(0+i\cdot 0)\\ \vdots & \vdots & \ddots & \vdots\\ \frac{1}{2}(0+i\cdot 0) & \frac{1}{2}(0+i\cdot 0) & \cdots & \frac{1}{2}(1+i\cdot 1)\end{bmatrix}\begin{bmatrix}\frac{1}{2}(1-i\cdot 1) & \frac{1}{2}(0-i\cdot 0) & \cdots & \frac{1}{2}(0-i\cdot 0)\\ \frac{1}{2}(0-i\cdot 0) & \frac{1}{2}(1-i\cdot 1) & \cdots & \frac{1}{2}(0-i\cdot 0)\\ \vdots & \vdots & \ddots & \vdots\\ \frac{1}{2}(0-i\cdot 0) & \frac{1}{2}(0-i\cdot 0) & \cdots & \frac{1}{2}(1-i\cdot 1)\end{bmatrix}$$

$$\begin{bmatrix} \frac{1}{2}(1+i) & 0 & \cdots & 0 \\ 0 & \frac{1}{2}(1+i) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \frac{1}{2}(1+i) \end{bmatrix} \begin{bmatrix} \frac{1}{2}(1-i) & 0 & \cdots & 0 \\ 0 & \frac{1}{2}(1-i) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \frac{1}{2}(1-i) \end{bmatrix}$$

$$\begin{bmatrix} \frac{1}{2}(2) & 0 & \cdots & 0 \\ 0 & \frac{1}{2}(2) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \frac{1}{2}(2) \end{bmatrix} = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}$$

An $n \times n$ complex matrix A is said to be unitary if the column vectors of A are orthonormal [4], that is, if

$$\sum_{i=1}^{n} \overline{A_{ij}} A_{ik} = \delta_{jk}$$

Equivalently, A is unitary if it preserves the inner product, namely, if $\langle x, y \rangle = \langle A_x, A_y \rangle$ for all vectors x, y in C^n. (Angled brackets here denote the inner product on C^n, $\langle x, y \rangle = \sum_i \overline{x_i} y_i$. We will adopt the convention of putting the complex conjugate on the left.) Still another equivalent definition is that A is unitary if $A^* A = I$, *i.e.*, if $A^* = A^{-1}$. (A^* is the adjoint of A, $(A^*)_{ij} = A_{ji}$).

Since $\det A^* = \overline{\det A}$, we see that if A is unitary, then $\det(A^* A) = |\det A|^2 = \det I = 1$. Hence $|\det A| = 1$, for all unitary matrices A. This in particular shows that every unitary matrix is invertible. The same argument as for the orthogonal group shows that the set of unitary matrices forms a group.

This in particular shows that every unitary matrix is invertible. The same argument as for the orthogonal group shows that the set of unitary matrices forms a group. The set of all $n \times n$ unitary matrices is the unitary group $U(n)$, and is a subgroup of $GL(n, C)$. The limit of unitary matrices is unitary, so $U(n)$ is a matrix Lie group. The set of unitary matrices with determinant one is the special unitary group $SU(n)$. It is easy to check that $SU(n)$ is a matrix Lie group. Note that a unitary matrix can have determinant $e^{i\theta}$ for any θ, and so $SU(n)$ is a smaller subset of $U(n)$ than $SO(n)$ is of $O(n)$. (Specifically, $SO(n)$ has the same dimension as $O(n)$, whereas $SU(n)$ has dimension one less than that of $U(n)$).

8. Symplectic Groups

$n \times n$ real *skew symmetric* matrix A [6], *i.e.*, one for which $S^{\mathrm{T}} = -A$. For such a matrix,

$$\det A^{\mathrm{T}} = \det(-A) = (-1)^n \det A$$

giving

$$\det A = (-1)^n \det A$$

The most interesting case occurs if $\det A \neq 0$ when n must be even and we then write $n = 2m$. The standard example of this is built up using the 2 × 2 block

$$J = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

If $m \geq 1$ we have the non-degenerate skew symmetric matrix

$$J_{2m} = \begin{bmatrix} J & O_2 & \cdots & O_2 \\ O_2 & J & \cdots & O_2 \\ \vdots & \vdots & \ddots & \vdots \\ O_2 & O_2 & \cdots & J \end{bmatrix}$$

The matrix group

$$SP_{2m}(R) = \left\{ A \in GL_{2m}(R) : A^{\mathrm{T}} J_{2m} A = J_{2m} \right\} \leq GL(R)$$

Is called the $2m \times 2m$ (*real*) *symplectic group*.

We will now look at the coordinate-free version of these groups. A bilinear form B is called skew symmetric if $B(v,w) = -B(w,v)$. If B is skew-symmetric and non-degenerate, then $m = \dim V$ must be even, since the matrix of B relative to any basis for V is skew-symmetric and has nonzero determinant.

9. Cyclic Groups

The next class of groups we will consider consists of the cyclic groups. Before defining these groups, we need to explain how exponents work. If G is a group and $x \in G$, then if m is a positive integer, $x^m = x \cdots x$ (m factors). We define x^{-m} to be $\left(x^{-1}\right)^m$. Also, $x^0 = 1$. Then the usual laws of exponentiation hold for all integers m, n:

1) $x^m x^n = x^{m+n}$
2) $\left(x^m\right)^n = x^{mn}$

Definition 7.1. A group G is said to be cyclic if there exists an element $x \in G$ such that for every $y \in G$, there is an integer m such that $y = x^m$. Such an element x is said to generate G.

10. Dihedral Groups: Generators and Relations

In the next example, we give an illustration of a group G that is described by giving a set of its generators and the relations the generators satisfy. The group we will study is called the dihedral group. We will see in due course that the dihedral groups are the symmetry groups of the regular polygons in the plane. As we will see in this example, defining a group by giving generators and relations does not necessarily reveal much information about the group.

Example 8.1. [2] Let us now verify that $D(2)$ is a group. Since the multiplication of words is associative, it follows from the requirement that $a^2 = b^2 = 1$ and $ab = ba$ that every word can be collapsed to one of $1, a, b, ab, ba$. But $ab = ba$, so $D(2) = \{1, a, b, ab\}$. To see that $D(2)$ is closed under multiplication, we observe that

$$a(ab) = a^2b = b, b(ab) = (ba)b = ab^2 = a,$$
$$(ab)a = (ba)a = ba^2 = b \text{ and } (ab)(ab) = (ba)(ab) = ba^2b = b^2 = 1.$$

Therefore, $D(2)$ is closed under multiplication, so it follows from our other remarks that $D(2)$ a group. Note that the order of $D(2)$ is 4.

Example 8.2. [2] (Dihedral Groups) The dihedral groups are groups that are defined by specifying two generators a and b and also specifying the relations that the generators satisfy. When we define a group by generators and relations, we consider all words in the generators, in this case a and b: these are all the strings or products $x_1x_2\cdots x_n$, where each x_i is either a or b, and n is an arbitrary positive integer. For example, *abbaabbaabbaabba* is a word with $n = 16$. Two words are multiplied together by placing them side by side.

Thus,

$$(x_1x_2\cdots x_n)(y_1y_2\cdots y_p) = x_1x_2\cdots x_ny_1y_2\cdots y_p.$$

This produces an associative binary operation on the set of words. The next step is to impose some relations that a and b satisfy. Suppose $m > 1$. The dihedral group $D(m)$ is defined to be the set of all words in a and b with the above multiplication that we assume is subject to the following relations:

$$a^m = b^2 = 1, ab = ba^{m-1}.$$

It is understood that the cyclic groups $\langle a\rangle$ and $\langle b\rangle$ have orders m and two respectively. By, $a^{-1} = a^{m-1}$ and $b = b^{-1}$. For example, if $m = 3$, then $a^3 = b^2 = 1$, so

$$aaababababbb = (aaa)(bab)(ab)(bb) = (a^2)(ab) = a^3b = b.$$

The reader can show that $D(3) = \{1, a, a^2, b, ab, ba\}$. For example, $a^2b = a(ab) = a(ba^2) = (ab)a^2 = ba^4 = ba$. Hence, $D(3)$ has order 6. We will givea more convincing argument in due course.

11. Quaternionic Groups

We recall some basic properties of the quaternions [3]. Consider the four-dimensional real vector space H consisting of the 2 × 2 complex matrices

$$w = \begin{bmatrix} x & \overline{-y} \\ y & \overline{x} \end{bmatrix}$$

with $x, y \in C$.

One checks directly that H is closed under multiplication in $M_2(C)$. If $w \in H$ then $w^* \in H$ and

$$w^*w = ww^* = \left(|x|^2 + |y|\right)^2 I$$

(where w denotes the conjugate-transpose matrix). Hence every nonzero element of H is invertible. Thus H is a division algebra (or skew field) over R. This division algebra is a realization of the quaternions. The more usual way of introducing the quaternions is to consider the vector space H over R with basis $f = \{1, i, j, k\}$. Define a multiplication so that 1 is the identity and

$$i^2 = j^2 = k^2 = -1;$$

$$ij = -ji = k, ki = -ik = j, jk = -kj = i;$$

then extend the multiplication to H by linearity relative to real scalars. To obtain an isomorphism between this version of H and the 2_2 complex matrix version, take

$$1 = I, i = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, j = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, k = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$$

where i is a fixed choice of $\sqrt{-1}$. The conjugation $w \to w^*$ satisfies $(uv)^* = v^* u^*$. In terms of real components, $(a + bi + cj + dk)^* = a - bi - cj - dk$ for $a, b, c, d \in R$. It is useful to write quaternions in complex form as $x + jy$ with $x, y \in C$; however, note that the conjugation is then given as

$$(x + jy)^* = x + yj = x - jy$$

On the $4n$-dimensional real vector space H^n we define multiplication by $a \in H$ on the right:

$$(u_1, \cdots, u_n) \cdot a = (u_1 a, \cdots, u_n a)$$

We note that $u \cdot 1 = u$ and $u \cdot (ab) = (u \cdot a) \cdot b$. We can therefore think of H^n as a vector space over H. Viewing elements of H^n as $n \times 1$ column vectors, we define Au for $u \in H^n$ and $A \in M_n(H)$ by matrix multiplication. Then $A(u \cdot a) = (Au) \cdot a$ for $a \in H$; hence A defines a quaternionic linear map. Here matrix multiplication is defined as usual, but one must be careful about the order of multiplication of the entries.

We can make H^n into a $2n$-dimensional vector space over C in many ways; for example, we can embed C into H as any of the subfields

$$R1 + Ri, R1 + Rj, R1 + Rk$$

Using the first of these embeddings, we write $z = x + jy \in H^n$ with $x, y \in C^n$, and likewise $C = A + jB \in M_n(H)$ with $A, B \in M_n(C)$. The maps

$$z \to \begin{bmatrix} x \\ y \end{bmatrix} \text{ and } C \to \begin{bmatrix} A & \overline{-B} \\ B & \overline{A} \end{bmatrix}$$

identify H^n with C^{2n} and $M_n(H)$ with the real subalgebra of $M_{2n}(C)$ consisting of matrices T such that

$$JT = \overline{T}J$$

where

$$J = \begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix}$$

The Future Perspective of This Paper

The future of this paper is to help some to better understand the introductory part of linear groups, while others, like me, to be an incentive in further work and engaging in science.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Carrell, J.B. (2017) Groups, Matrices, and Vector Spaces. Department of Mathematics University of British Columbia Vancouver, BC Canada. http://www.uop.edu.pk/ocontents/Groups,%20Matrices,%20and%20Vector%20Spaces%20A%20Group%20Theoretic%20Approach%20to%20Linear%20Algebra.pdf

[2] Grillet, P.A. (2007) Abstract Algebra. Department of Mathematics Tulane University USA. http://dobrochan.ru/src/pdf/1204/Grillet_P._A._-_Abstract_Algebra_(2007)(684).pdf

[3] Goodman, R. and Wallach, N.R. (2009) Symmetry, Representations, and Invariants. Department of Mathematics, Rutgers University of California, San Diego Piscataway. https://www.maths.ed.ac.uk/~v1ranick/papers/goodwallx.pdf

[4] Hall. B.C. (2000) An Elementary Introduction to Groups and Representations. University of Notre Dame, Department of Mathematics, Notre Dame. https://arxiv.org/abs/math-ph/0005032

[5] Agargun, A.G. and Uzdag, H. (2007) Linear Algebra and Calculus Problems. Yildiz Teknik University, Turkey. https://www.cimri.com/kaynak-kitaplari/en-ucuz-lineer-cebir-ve-cozumlu-problemleri-a-goksel-agargunhulya-ozdag-9781111138769-fiyatlari,528793

[6] Baker, A. (1953) Matrix Groups an Introduction to Lie Group Theory (Library of Congress Cataloging-in-Publication Data Baker, Andrew, 1953), Department of Mathematics, University of Glasgow, Glasgow, USA. http://inis.jinr.ru/sl/vol1/UH/_Ready/Mathematics/Algebra/Baker%20A.%20Matrix%20groups,%20an%20introduction%20to%20Lie%20groups%20(Springer,%202002)(L)(173s).pdf