A lightning tour of algebraic structures

Warren D. Smith
wds@research.NJ.NEC.COM

date = October 28, 1998

Abstract — **We state the definitions of the following important algebraic structures: Groupoid, loop, Moufang loop, semigroup, group, Lie group, quasi-group, ring, division ring, ideal, field, vector space, Lie algebra, Jordan algebra, Clifford algebra, Clifford group, Spinors. For each we give a few of the most important examples and theorems (without proofs), and then stop.**

Keywords —

1 Groups and their ilk

A *groupoid* is a set S together with a binary operation $\circ$ mapping $S \times S$ into S.

A *semigroup* is a groupoid such that $\circ$ is *associative*, i.e. $a \circ (b \circ c) = (a \circ b) \circ c$.

Example of a semigroup: composition of functions.

Easy semigroup **theorem** #1: if there exists a left identity 1_ℓ such that $\forall x \in S$ $1_\ell \circ x = x$ and there exists a right identity 1_r such that $\forall x \in S$ $x \circ 1_r = x$. then $1_\ell = 1_r$. In this case we just call it "the identity element 1."

Easy semigroup **theorem** #2: if, in a semigroup with an identity element 1, there exists a left inverse x_ℓ^{-1} of some element x, and a right inverse x_r^{-1} of some element x (i.e. $x_\ell^{-1}x = 1 = xx_r^{-1}$) then $x_\ell^{-1} = x_r^{-1}$. In this case we just call it "the inverse x^{-1} of x."

A *group* is a semigroup with an identity element 1 and such that every group element x has an inverse x^{-1}.

Three examples of groups:

1. S_n, the $n!$ permutations of n things [18], with composition as the operation. An important subgroup of S_n is A_n, the $n!/2$ even permutations (i.e. those expressible as an even number of swaps) of n things.

2. $U(n)$: The $n \times n$ unitary matrices with matrix multiplication as the operation [31].

3. $\mathrm{GL}_n(F)$: All $n \times n$ invertible matrices whose elements lie in any particular finite field F, with matrix multiplication as the operation.

Lagrange's **theorem**: If G is a group with $|G|$ elements, and H is a subgroup of G, then $|G|$ is divisible by $|H|$.

Sylow's partial converse: If p^k is a prime power dividing $|G|$, then G has a subgroup of cardinality p^k. All the cardinality-p^k subgroups of G are identical as abstract groups.

A *commutative group* is a group with a *commutative* $\circ$ operation, i.e. $a \circ b = b \circ a$.

Three examples of commutative groups:

1. The 7-tuples of integers $\mathbf{Z}^7$, with elementwise addition as the operation.

2. $\mathbf{Z}_n$, the integers mod n, with addition as the operation.

3. $\mathbf{Z}_p \backslash 0$, the nonzero integers mod some prime p, with multiplication as the operation.

A *Lie group* is a group G such that G is a paracompact, real analytic manifold and the mapping from $G \times G \to G$ defined by $(x, y) \to x \circ y^{-1}$ is real analytic (actually, 2-time differentiability will suffice [25]).

Two examples [31] of Lie groups:

1. The group $O_n^+(\mathbf{R})$ of $n \times n$ real rotation matrices.

2. The Lorentz transformations $O(3, 1)$ arising in special relativity.

A subgroup H of a group G is *normal* (as usual, the word "normal" was a terrible choice) if for any $h \in H$ and $g \in G$, $g \circ h \circ g^{-1} \in H$. Example: the group C_n of the n rotations of a regular n-gon in the plane, is a normal subgroup of the group D_{2n} of the $2n$ rotations and flips of the n-gon.

The group classification **theorem**: One of the triumphs of modern mathematics was the complete classification of all finite simple groups (a group is *simple* if it has no nontrivial normal subgroup). They are:

1. $(Z_p, +)$, (i.e. the cyclic groups of prime order);

2. A_n for each $n \geq 5$ (i.e. the $n!/2$ even permutations of n things);

3. groups of "Chevalley type" arising in various ways from the continuous Lie groups [9] by changing their real or complex number coordinates to instead be elements of the *finite fields* (discussed in §5);

4. and the 26 *sporadic groups* [8].

An n-dimensional *representation* of a group is a way to embed it inside the complex $n \times n$ unitary matrices.

Examples:

1. The group A_5 of the $5!/2 = 60$ permutations of n things, may be represented trivially by 60 5×5 permutation matrices.

2. But it is also possible to represent A_5 using 3×3 real rotation matrices: specifically, the 60 rotations constituting the orientation preserving symmetries of a regular icosahedron.

Permutation group algorithms are discussed in [13] [21] [4] [6].

There are remarkably powerful methods available which can find all representations of a group [12]. Also, other methods [11] [28] allow deduction of the "character table" of the group, which tells you a great deal about its representations (e.g. their dimensions, what traces all the matrices have) without actually finding them all.

2 Weaker things resembling groups

A *quasi-group* is like a group, but no associativity is required, and no identity element is required either – instead we make the weaker demand of "unique solvability:" $ax = b$ and $xa = b$ each have unique solutions x.

A *Loop* is a quasi-group with an identity element 1. (This is automatically two-sided and unique, and unique two-sided inverses automatically exist.)

A *Moufang Loop* is a loop satisfying $[(xy)z]x = x[y(zx)]$, $y[x(yz)] = [(yx)y]z$, $(yx)(zy) = [y(xz)]y$. This is not as strong a demand as associativity. These were introduced by Ruth Moufang, one of the earliest female math professors.

Moufang's **theorem**: any three elements a, b, c in a Moufang loop which are associative by themselves, generate a group.

Posets, or "partially ordered sets," are sets equipped with a boolean-valued partial order relation $a \prec b$. This relation has to be acyclic, i.e. there do not exist $a_1, a_2, \ldots, a_n$ so that $a_1 \prec a_2 \prec \cdots \prec a_n \prec a_1$, and it has to be transitive, i.e. if $a \prec b$ and $b \prec c$, then $a \prec c$.

Example: a set of groups with $\prec$ being the "is subgroup of" relation.

3 Algebras

Are sets equipped with *two* binary operations, usually denoted "+" and "×," where × is distributive over + and + is commutative.

Unusual example: the real numbers with min instead of addition and + instead of multiplication, form an algebra.

Rings and fields are important kinds of algebras. "Algebra" is mainly useful as a catch-all term which one uses to take care of all the stuff that doesn't fit in the usual subcategories such as rings and fields! We will often write ab instead of $a \times b$ below.

4 Rings and their ilk

A *ring* is a set R together with two binary operations $+$ and $\times$ where $(R, +)$ forms a commutative group and $(R, \times)$ forms a groupoid, and where $\times$ is *distributive* over $+$, i.e. $a \times (b + c) = a \times b + a \times c$, $(b + c) \times a = b \times a + c \times a$.

Many older authors also require $\times$ to be associative, i.e. demand that $(R, \times)$ is a semigroup, and would reserve the special name "non-associative rings" for the (rarely occurring) case when this demand is violated. I believe, however, that the present definition is a better one.

Easy ring **theorem**: A ring R must include a zero element "0" such that $0 \times r = r \times 0 = 0$, $0 + r = r + 0 = r$, $\forall r \in R$.

Two examples of associative rings:

1. The $n \times n$ integer matrices $\mathbf{Z}^{n \times n}$;
2. The $n \times n$ integer matrices $\mathbf{Z}_m^{n \times n}$ with arithmetic modulo some positive integer m.

A *commutative ring* is a ring in which $\times$ is commutative. Two examples of commutative, associative rings:

1. The integers $\mathbf{Z}$;
2. Multivariate polynomials with coefficients in a *field* (defined in §5).

A *division ring* is a ring in which there is a multiplicative identity element "1," and every nonzero ring element has a multiplicative inverse (i.e. the nonzero ring elements form a multiplicative loop). Such an inverse will necessarily be unique.

Easy **theorem** about division rings: A division ring has no *zero divisors*, and equations $ax = b$, $ya = b$ are uniquely soluble given any two nonzero ring elements a, b.

Example of a (noncommutative) division ring: The *quaternions*: $a + bi + cj + dk$ where $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$, $i^2 = j^2 = k^2 = ijk = -1$, and a, b, c, d are real.

Example of a (noncommutative, non-associative) division ring: The *octonions*: $a_0 i_0 + a_1 i_i + \ldots a_6 i_6 + a_\infty$ where $a_0, a_1, \ldots a_6, a_\infty$ are real and the multiplication laws among the i_j are deducible from the requirement that $(i_{m \bmod 7}, i_{m+1 \bmod 7}, i_{m+3 \bmod 7})$ generate a quaternion subring in a manner isomorphic to the way (i, j, k) generate the quaternions. Octonion multiplication, although non-associative since, e.g., $(i_0 i_1) i_2 = -i_0 (i_1 i_2)$, nevertheless obeys the partial associativity laws (called the *alternative* property) that $a(ab) = (aa)b$, $(ab)b = a(bb)$.

Theorem. The complex numbers $\mathbf{C}$, the quaternions $\mathbf{H}$, and the octonions $\mathbf{O}$ all share the remarkable property that they have a multiplicative norm. That is, letting the (real valued) norm $N(a)$ denote the sum of the squares of the real coefficients of an octonion (or complex, or quaternion) a, then $N(a)N(b) = N(ab)$.

Theorem: There are exactly 4 ways to define a alternative multiplication of n-dimensional real vectors (assuming the usual elementwise addition) to get a division ring. Also, there are exactly 4 possible "sum of squares" identities of the form $N(a)N(b) = N(ab)$ (where $N(a)$ is a quadratic function of the coefficients in a, and the coefficients in ab are assumed to be bilinear functions of the coefficients of a and b). The 4 rings are $\mathbf{R}$, $\mathbf{C}$, $\mathbf{H}$ and $\mathbf{O}$ and the 4 identities are their norm-multiplicativity statements.

The theorem above was due to G.Frobenius in 1878 (alternative division rings part) and A.Hurwitz in 1898 (identities part). It has a fairly elementary and short (5 pages) proof. J.F.Adams [1] in 1960 showed, by extremely deep methods, that for any method of multiplying real n-vectors (assuming the usual elementwise addition) to get a division ring, we must have $n \in \{1, 2, 4, 8\}$. Note that Adams did not require any assumption about norms or about alternativity laws; indeed, he did not even need to assume the existence of a multiplicative identity or multiplicative inverses – merely the unique solvability of equations $ax = b$ for a and $ya = b$ for y sufficed. However, Adams's assumptions do not force the rings to be **R**, **C**, **H** and **O**; other rings of dimensions 1,2,4,8 are possible, e.g. [2].

An *ideal* B in a ring R is a subset of R such that $(B, +)$ is a subgroup of $(R, +)$, and $b \in B,\ r \in R \Leftrightarrow rb \in B,\ br \in B$.

Examples of ideals:

1. The integers divisible by any fixed prime p, inside the integers;
2. Inside the ring of polynomials with integer coefficients of two variables x, y, consider those which are multiples of $x^2 + 7y + 3$.

Hilbert's basis **theorem**: In the ring of multivariate polynomials with coefficients in some fixed field, each ideal is generated by a *finite* set of polynomials, called its "basis."

5 Fields

A *field* is a division ring where $\times$ is commutative and associative. In other words both $+$ and $\times$ are both commutative and associative, and hence a field is an additive commutative group and at the same time the nonzero elements of the field form a multiplicative commutative group.

Six examples of fields:

1. The rational numbers **Q**;
2. The real numbers constructible with ruler and compass;
3. The reals **R**;
4. Conway has defined a remarkable field he calls "games" which includes the reals as a subfield [7];
5. The complex numbers **C**;
6. The integers modulo any fixed prime p, denoted $\mathbf{Z}_p$.

Galois's **theorem**: E.Galois (1811-1832) completely classified all finite fields: If a field has finite cardinality, then that cardinality must be a prime power p^n. For each prime p and positive integer n there is a unique finite field of cardinality p^n, called the "Galois field" GF(p^n).

Unique factorization **theorem**: Euclid's algorithm works to find the GCD of any two univariate polynomials with coefficients in some fixed field. Any such polynomial has a unique factorization (up to scalar multiples).

6 Vector spaces

A *vector space* V over a field F is a set equipped with a commutative group operation "+" mapping $V \times V \to V$ (the additive identity is "$\vec{0}$") and binary associative (but not necessarily commutative) scalar multiplication operations mapping $F \times V \to V$ (note, we only have a *left* multiplication by scalars) and $F \times F \to F$ (in this case $\times$ is just the field multiplication), and distributive over $+$: $a(\vec{u} + \vec{v}) = a\vec{u} + a\vec{v}$, and $(a + b)\vec{u} = a\vec{u} + b\vec{u}$ for $\vec{u}, \vec{v} \in V$, $a, b \in F$. By "associative" here, we mean that $a(b\vec{v}) = (ab)\vec{v}$ for $\vec{v} \in V,\ a, b \in F$, in addition to the usual associativity of multiplication already required because F is a field. The scalar multiplication has to respect the identity in F, i.e. $1\vec{v} = \vec{v}$.

A *finite* set of vectors $\vec{u}, \vec{v}, \ldots, \vec{w}$ is *linearly dependent* if there exist scalars $a, b, \ldots, c$ so that $a\vec{u} + b\vec{v} + \cdots + c\vec{w} = \vec{0}$.

A finite or infinite set of vectors is *linearly independent* if no finite subset of it is linearly dependent.

The *dimension* of a vector space is the maximum cardinality of any linearly independent set of vectors in it.

A set S (finite or infinite) of vectors *spans* a vector space V over a field F if every vector $\vec{v} \in V$ is expressible as a *finite* sum $\vec{v} = a\vec{u} + b\vec{v} + \cdots + c\vec{w}$ for some $a, b, \ldots, c \in F$ and $\vec{u}, \vec{v}, \ldots \vec{w} \in S$.

Notice the careful tiptoeing around infinity in some of the above definitions.

Theorem: The only finite dimensional vector spaces over the reals and complex numbers respectively, are the obvious ones $\mathbf{R}^n$ and $\mathbf{C}^n$ (n-tuples with elementwise addition and elementwise multiplication).

Basis **theorem**: Each vector space has a *basis*, i.e. a set of linearly independent vectors spanning the space.

The basis theorem is unusual in that it depends for its validity on the "axiom of choice," a comparatively little used axiom of mathematics (the 'C' in the ZFC axioms). Note that this theorem is *not* obvious. For example, consider the vector space (which happens also to be a Hilbert space) of infinite-tuples of reals: $(x_0, x_1, \ldots)$ such that $\lim_{n\to\infty} x_0^2 + x_1^2 + \cdots + x_n^2$ is finite. The obvious countably infinite set $(1, 0, 0, \ldots)$, $(0, 1, 0, 0, \ldots)$, etc. actually is not a basis. It is linearly independent, but it does not span because the definition of "span" requires being able to represent any vector as a weighted sum of a *finite* number of elements in our basis.

7 Jordan algebras

A *Jordan algebra*[1] is a vector space with a commutative group operation $+$ as usual, but also a commutative "Jordan product" operation $A \bullet B$ obeying $(x^2 \bullet y) \bullet x = x^2 \bullet (y \bullet x)$.

Example: Real symmetric and complex Hermitian $n \times n$ matrices form Jordan algebras under the symmetric Jordan product $A \bullet B = (AB + BA)c$ (for any constant scalar c; one usually uses $c = 1/2$) [24].

[1] Jordan algebras, Clifford algebras, and Lie algebras are actually (generally non-associative) rings, but since the old definition of a "ring" required multiplication to be assocative, the word "algebra" unfortunately has stuck.

The algebra of $n\times n$ Hermitian matrices whose elements are the (non-associative and non-commutative!) octonions turns out to be a Jordan algebra exactly when $n\le 3$.

These were introduced by physicist P.Jordan, who (1) noticed that the usual operators representing quantum mechanical observables, were Hermitian, and (2) saw that if AB and B are Hermitian, then so are ABA, A^n, $AB+BA$, $iAB-iBA$, and $A\pm B$, but *not* AB, and (3) then noticed that these could be boiled down to one axiom.

Later, Jordan, E.Wigner and J.von Neumann [19] classified all finite dimensional formally real Jordan algebras. Their result is:

Theorem. The finite dimensional irreducible formally real Jordan algebras are:

1. The real numbers $\mathbf{R}$.
2. The commutative Jordan algebras $\mathcal{G}_n$ $(n\ge 3)$ with basis $1, s_1, s_2, \ldots s_{n-1}$ where $1\bullet s_j=s_j$, $1\bullet 1=1$, $s_a\bullet s_b=0$ if $a\ne b$, and $s_a\bullet s_a=1$. (Note: $\mathcal{G}_1=\mathbf{R}$ and $\mathcal{G}_2$ is reducible.)
3. The Hermitian $n\times n$ matrices with $A\bullet B=(AB+BA)/2$ and either real, complex, or quaternionic elements for each $n\ge 3$, or octonion elements if $n=3$. (The cases with $n\in\{1,2\}$ are also allowed, but are subsumed by already defined algebras.)

8 Lie algebras

A *Lie algebra* is a vector space equipped with a binary operation ("Lie product") denoted $[x,y]$ mapping $L\times L\to L$ such that

$$[x,y]=-[y,x] \quad (\mathrm{anti-commutative}) \tag{1}$$

and

$$[x,[y,z]]+[y,[z,x]+[z,[x,y]]=0 \qquad (\text{Jacobi identity}). \tag{2}$$

Example: $n\times n$ complex matrices with the "commutator" $[A,B]=AB-BA$, (or any constant scalar multiple of this) as the Lie product.

The antisymmetric (or antiHermitian, i.e. i times a Hermitian) $n\times n$ matrices are also Lie algebras, which happen to lie inside the above Lie algebra.

The matrix exponentials e^{iH} where H is a Hermitian matrix are precisely the unitary matrices, which as we saw previously, form a "Lie group." This is an example of the notion (which we won't make formal here) that the "Lie groups are the exponentials of Lie algebras." On the other hand, consider the fact that the solution of a differential equation $\mathrm{d}\vec{x}/\mathrm{d}t=iH\vec{x}$ is $\vec{x}(t)=e^{iHt}\vec{x}(0)$.

Thus perturbing $\vec{x}$ continuously by infinitesimal Hermitian transformations of itself will result in a unitary transformation as the net effect. This is an example of the notion that "The Lie algebras describe the infinitesimal generators of Lie groups."

A Lie algebra is *simple* if it has no nontrivial ideal, and *semisimple* if it has no commutative ideals.

A famous **theorem** of E.Cartan (1869-1951) gave the complete classification of all semisimple Lie algebras over the complex numbers [30] [16].

9 Clifford algebras

Complex number multiplication can be used to perform 2D rotations. Quaternions attracted much attention because they can represent both 3D and 4D rotations [10] [3]. Specifically,

$$x\to qxq^{-1} \tag{3}$$

will rotate a 3-vector x, if the 3 imaginary components of a quaternion x with zero real part are regarded as a real 3-vector, and q is a quaternion; this correspondence shows that the quaternions q of unit "norm" (sum of squares of their 4 real coefficients) are in a 2-1 correspondence with the 3×3 real rotation matrices.

Specifically let $x=0+x_1i+x_2j+x_3k$ and $q=\cos\theta+(q_1i+q_2j+q_3k)\sin\theta$. Then $qxq^{-1}=0+y_1i+y_2j+y_3k$ where $\vec{y}$ is what you get if you rotate $\vec{x}$ an angle 2θ about the axis $\vec{q}$.

Similarly $x\to axb$, where a and b are unit-norm quaternions, performs arbitrary 4D rotations on a 4-vector x and gives a 2-1 correspondence between 2-tuples of unit-norm quaternions, and 4×4 real rotation matrices.

The 3D "vector cross product" and vector "dot product" naturally arise from quaternion multiplication: if $a=a_0+a_1i+a_2j+a_3k=a_0+\vec{a}\cdot(i,j,k)$ then $ab=c$ where $c_0=a_0b_0-\vec{a}\cdot\vec{b}$ and $\vec{c}=\vec{a}\times\vec{b}+a_0\vec{b}+b_0\vec{a}$. The corresponding formula for expressing the product of two rotations as a rotation (all rotations expressed quaternionically, i.e. in the "natural" way using an axis vector and a rotation angle θ) was published by O.Rodrigues in 1840, somewhat before W.R.Hamilton "invented" the quaternions in 1843.

Hence things like Maxwell's equations of electromagnetism and the Lorentz transformations from special relativity may be written rather slickly as quaternionic equations [20].

All this led to much hope that the quaternions would somehow revolutionize physics, and also to the question of whether this was special to 3D and 4D, or could this be generalized to work for higher dimensional rotations? Just what is going on?

Eventually Cartan showed that indeed one can generalize to all higher dimensions by use of "Clifford algebras" [26] [23] to get "spinors" (§10).

9.1 The real Clifford algebras

Let p and q be nonnegative integers. The *real Clifford algebras* $\mathrm{Cl}_{p,q}(\mathbf{R})$ are defined as follows. Define $p+q$ special symbols $e_1, e_2, \ldots e_{p+q}$ which obey the following rules of multiplication:

$$e_j^2=\begin{cases}-1 & \text{if } 1\le j\le p\\ 1 & \text{if } p+1\le j\le p+q\end{cases} \quad ; \quad e_je_k=-e_ke_j \text{ if } j\ne k. \tag{4}$$

Then $\mathrm{Cl}_{p,q}(\mathbf{R})$ is the algebra you get by putting these and the real numbers together and closing under addition and multiplication. $\mathrm{Cl}_{p,q}(\mathbf{R})$ is 2^{p+q} dimensional, with basis 1, e_1, e_2,..., e_{p+q}, e_1e_2, ..., $e_{p+q-1}e_{p+q}$, ..., $\prod_{j=1}^{p+q} e_j$, i.e., all possible monomials you can form out of a product of a subset of the e_j, there being 2^{p+q} such subsets.

Many interesting algebras are just special cases of the $\mathrm{Cl}_{p,q}(\mathbf{R})$. For example, with $p=0$ and $0 \le q \le 7$ we have: $\mathrm{Cl}_{0,0}(\mathbf{R}) = \mathbf{R}$; $\mathrm{Cl}_{0,1}(\mathbf{R}) = \mathbf{C}$ by taking $e_1 = i$; $\mathrm{Cl}_{0,2}(\mathbf{R})$ is the quaternions $\mathbf{H}$, as one may realize by taking $e_1 = i$, $e_2 = j$, $e_1e_2 = k$. $\mathrm{Cl}_{0,3}(\mathbf{R}) = \mathbf{H} \oplus \mathbf{H}$, that is, 2-tuples of quaternions with elementwise multiplication and addition; $\mathrm{Cl}_{0,4}(\mathbf{R}) = \mathrm{Cl}_{4,0}(\mathbf{R}) = \mathbf{H}^{2\times 2}$, that is, 2×2 quaternionic matrices; $\mathrm{Cl}_{0,5}(\mathbf{R}) = \mathbf{C}^{4\times 4}$, that is, 4×4 complex matrices; $\mathrm{Cl}_{0,6}(\mathbf{R}) = \mathbf{R}^{8\times 8}$; $\mathrm{Cl}_{0,7}(\mathbf{R}) = \mathbf{R}^{8\times 8} \oplus \mathbf{R}^{8\times 8}$.

Elie Cartan managed to understand this completely. It turns out that an 8×8 table of the $\mathrm{Cl}_{p,q}(\mathbf{R})$ for $0 \le p, q \le 7$ suffices, because of Cartan's period-8 **theorem**:

$\mathrm{Cl}_{p+8,q}(\mathbf{R}) = \mathrm{Cl}_{p,8+q}(\mathbf{R}) = \mathrm{Cl}_{p,q}(\mathbf{R})^{16\times 16}$, i.e. 16×16 matrices of elements from $\mathrm{Cl}_{p,q}(\mathbf{R})$.

Actually, we need only consider $0 \le p \le 3$ and $0 \le q \le p+1$ because of the additional **theorems** that $\mathrm{Cl}_{p+1,q}(\mathbf{R}) = \mathrm{Cl}_{q+1,p}(\mathbf{R})$ and $\mathrm{Cl}_{p,q}(\mathbf{R}) = \mathrm{Cl}_{p+4,q-4}(\mathbf{R})$.

The requisite cases $\mathrm{Cl}_{p,q}(\mathbf{R})$ for $0 \le p \le 3$ and $0 \le q \le 8$ are as follows.

$\mathbf{R}$	$\mathbf{R}\oplus\mathbf{R}$	$\mathbf{R}^{2\times 2}$	$\mathbf{C}^{2\times 2}$
$\mathbf{C}$	$\mathbf{R}^{2\times 2}$	$\mathbf{R}^{2\times 2}\oplus\mathbf{R}^{2\times 2}$	$\mathbf{R}^{4\times 4}$
$\mathbf{H}$	$\mathbf{C}^{2\times 2}$	$\mathbf{R}^{4\times 4}$	$\mathbf{R}^{4\times 4}\oplus\mathbf{R}^{4\times 4}$
$\mathbf{H}\oplus\mathbf{H}$	$\mathbf{H}^{2\times 2}$	$\mathbf{C}^{4\times 4}$	$\mathbf{R}^{8\times 8}$
$\mathbf{H}^{2\times 2}$	$\mathbf{H}^{2\times 2}\oplus\mathbf{H}^{2\times 2}$	$\mathbf{H}^{4\times 4}$	$\mathbf{C}^{8\times 8}$
$\mathbf{C}^{4\times 4}$	$\mathbf{H}^{4\times 4}$	$\mathbf{H}^{4\times 4}\oplus\mathbf{H}^{4\times 4}$	$\mathbf{H}^{8\times 8}$
$\mathbf{R}^{8\times 8}$	$\mathbf{C}^{8\times 8}$	$\mathbf{H}^{8\times 8}$	$\mathbf{H}^{8\times 8}\oplus\mathbf{H}^{8\times 8}$
$\mathbf{R}^{8\times 8}\oplus\mathbf{R}^{8\times 8}$	$\mathbf{R}^{16\times 16}$	$\mathbf{C}^{16\times 16}$	$\mathbf{H}^{16\times 16}$

In particular $\mathrm{Cl}_{p,p}(\mathbf{R}) = \mathbf{R}^{2^p\times 2^p}$.

9.2 Complex Clifford algebras

Instead of combining the special symbols e_j with real coefficients, one could instead use complex coefficients, getting the complex Clifford algebras. In this case it is pointless to have two indices p and q denoting the number of square roots of $+1$ and of -1 respectively among the e_j's, because you can just multiply a root of $+1$ by i to get a root of -1.

So define $\mathrm{Cl}_n(\mathbf{C})$ to be the algebra of all linear combinations, with complex coefficients, of n special anticommuting symbols $e_1, e_2, \ldots e_n$ (each of which is a square root of 1) and their products. This is a complex 2^n-dimensional space.

Obviously $\mathrm{Cl}_0(\mathbf{C}) = \mathbf{C}$ and $\mathrm{Cl}_1(\mathbf{C}) = \mathbf{C}\oplus\mathbf{C}$.

The three 2×2 Hermitian anticommuting *Pauli matrices*

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad (5)$$

are square roots of the 2×2 identity matrix I_2. Using any two of these as e_1 and e_2 then allows us to see that $\mathrm{Cl}_2(\mathbf{C}) = \mathbf{C}^{2\times 2} = \mathrm{Cl}_{2,1}(\mathbf{R})$.

Similarly $\mathrm{Cl}_4(\mathbf{C}) = \mathbf{C}^{4\times 4} = \mathrm{Cl}_{3,2}(\mathbf{R})$ arises because the 4×4 Hermitian *Dirac gamma matrices* [14]

$$\gamma_j = \begin{pmatrix} 0 & -i\sigma_j \\ i\sigma_j & 0 \end{pmatrix}, \quad \gamma_4 = \begin{pmatrix} -I_2 & 0 \\ 0 & I_2 \end{pmatrix} \qquad (6)$$

provide a suitable set of four anticommuting square roots of I_4.

These are special cases of the complex period **theorem** that $\mathrm{Cl}_{2n}(\mathbf{C}) = \mathbf{C}^{2^n\times 2^n} = \mathrm{Cl}_{n,n+1}(\mathbf{R})$ and $\mathrm{Cl}_{2n+1}(\mathbf{C}) = \mathrm{Cl}_{2n}(\mathbf{C}) \oplus \mathrm{Cl}_{2n}(\mathbf{C})$ for all $n \ge 0$.

10 Clifford groups and spinors

The real Clifford algebras $\mathrm{Cl}_{p,q}(\mathbf{R})$ we have just defined have dimension 2^{p+q} over the reals. Within this algebra is a subalgebra, denoted $\mathrm{Cl}^+_{p,q}(\mathbf{R})$, of dimension 2^{p+q-1}, generated only by the monomials which are products of an *even* number of e_j's.

Theorem: $\mathrm{Cl}^+_{p+1,q}(\mathbf{R}) = \mathrm{Cl}^+_{p,q+1}(\mathbf{R}) = \mathrm{Cl}_{p,q}(\mathbf{R})$.

Now, restrict attention to the invertible elements of either $\mathrm{Cl}_{p,q}(\mathbf{R})$ or $\mathrm{Cl}^+_{p,q}(\mathbf{R})$. These generate a multiplicative group $G_{p,q}$ (or $G^+_{p,q}$). These groups are the *Clifford groups* (resp. special Clifford groups).

Now, let s be an element of the special Clifford group $G^+_{p,q}$, and consider the action $x \to sxs^{-1}$ on x. (This type of map is called *conjugation*.) Restrict attention to those x which lie inside the $(p+q)$-dimensional subspace of linear combinations of $e_1, e_2, \ldots e_{p+q}$ only, i.e. $x = x_1e_1 + x_2e_2 + \cdots x_{p+q}e_{p+q}$. Also restrict attention to those s such that this action preserves this subspace. In that case, we have got a group action on $\mathbf{R}^{p+q}$ which preserves $x_1^2 + x_2^2 + \cdots x_p^2 - x_{p+1}^2 - \cdots - x_{p+q}^2$, i.e. consists of generalized rotation matrices (if $q=0$ or $p=0$, we get the usual kind of rotation matrices).

Theorem. The group action we have just described generates the entire group $O^+_{p,q}(\mathbf{R})$ of $(p+q)$-dimensional generalized rotation matrices.

These are called *spinors*. The spinors give a surprising way to get the effect of $n\times n$ rotation matrices: by conjugation in the even Clifford subalgebra $\mathrm{Cl}^+_{n,0}(\mathbf{R})$ of dimension 2^{n-1} generated by n special square roots of unity (or of -1) $e_1, e_2, \ldots, e_n$. The special case $\mathrm{Cl}^+_{3,0}(\mathbf{R}) = \mathbf{H}$, arising from $e_2e_1 = i$, $e_3e_2 = j$, $e_1e_3 = k$, finally explains the original observation (EQ **??**) that conjugation by unit norm quaternions yields the 3D rotations.

One can do the same thing to the complex Clifford algebras (**Theorem**: $\mathrm{Cl}^+_{n+1}(\mathbf{C}) = \mathrm{Cl}_n(\mathbf{C})$) to get complex spinors to represent unitary transformations.

References

[1] J.F.Adams: On the nonexistence of elements of Hopf invariant one, Annals of Math. 72 (1960) 20-104.

[2] S.C.Althoen & L.D.Kugler: When is $\mathbf{R}^2$ a division algebra? Amer. Math. Monthly 90,9 (1983) 625-635.

[3] S.L.Altmann: Rotations, quaternions, and double groups, Oxford University Press, 1986.

[4] Laszlo Babai, Gene Cooperman, Larry Finkelstein, Eugene Luks, and Akos Seress: Fast Monte Carlo algorithms for permutation groups, Journal of Computer and System Sciences, 50,2 (1995) 296-308.

[5] R.Brauer, H.Weyl: Spinors in n dimensions, Amer.J.Math. 57,2 (1935) 425-449.

[6] Gregory Butler: Fundamental algorithms for permutation groups, Springer-Verlag 1991.

[7] J.H.Conway: On numbers and games, Academic Press, 1976.

[8] Conway, Curtis, Norton, Parker, Wilson: ATLAS of finite groups, Oxford, Clarendon press, 1985. Updated in London Math. Society lecture notes #249.

[9] R.W.Carter: Finite groups of Lie type, Wiley 1986.

[10] H.S.M.Coxeter: Quaternions and Rotations, Amer. Math. Monthly 53 (1946) 136-146.

[11] John D. Dixon: High speed computation of group characters, Numer. Math. 10 (1967) 446-450.

[12] John D. Dixon: Constructing irreducible representations of finite groups, Math.Comput. 24 (1970) 707-712.

[13] Merrick Furst, John Hopcroft, Eugene Luks: Polynomial-Time Algorithms for Permutation Groups, Sympos. on Foundations of Computer Sci. 21 (Oct 1980) 36-41.

[14] R.H.Good Jr.: Properties of the Dirac matrices, Rev. Mod. Phys. 27 (1955) 187-211.

[15] L.C.Grove & C.J.Benson: Finite reflection groups, (2nd ed.) Springer 1985.

[16] J.E.Humphreys: Introduction to Lie algebras and representation theory, Springer 1972.

[17] A.Hurwitz: Ueber die Composition der quadratischen Formen von beliebig vielen Variabeln, Nachr. Gesell. Wiss. Göttingen, Math.-Phys. Klasse 1898) 309-316.

[18] G.D. James, A.Kerber: The representation theory of the symmetric group, Addison-Wesley 1981 ("Encyclopedia of mathematics and its applications" #16).

[19] P.Jordan, E.Wigner, J.von Neumann: On an algebraic generalization of the quantum mechanical formalism, Ann. of Math. (2) 35 (1934) 29-64. (Also a supplementary paper by A.Albert appears in the same issue pages 65-73.)

[20] J. Lambek: If Hamilton had prevailed: quaternions in physics, Math. Intelligencer 17,4 (1995) 7-15.

[21] J.S.Leon: On an algorithm for finding a base and a strong generating set for a group given by permutations, Math.Comput. 35 (1980) 941-974.

[22] R.Lidl & H.Niederreiter: Finite fields (2nd ed.) Cambridge U. Press 1997.

[23] Pertti Lounesto: Clifford Algebras and Spinors, London Math. Society Lecture Notes #239.

[24] Kevin McCrimmon: Jordan Algebras and Their Applications, Bull. Am. Math. Soc. 84 (1978) 612-627.

[25] L.S.Pontrjagin: Topological groups (2nd ed.) Gordon & Breach 1966.

[26] Ian Porteous: Clifford Algebras and the Classical Groups, Cambridge University Press 1995.

[27] J.J.Rotman: An introduction to the theory of groups, (4th ed.) Springer-Verlag 1995.

[28] G.J.A.Schneider: Dixon's character table algorithm revisited, J.Symbolic Comput. 9 (1980) 601-606.

[29] J.P.Serre: Linear representations of finite groups, Springer 1977.

[30] V.S.Varadarajan: Lie groups, Lie algebras, and their representations, Springer 1984.

[31] H.Weyl: The classical groups; their invariants and representations, Princeton University press 1946 (2nd ed.)