# Notes On Various Algebraic Structures With A View Toward Applications In Particle Physics

Jack F. McMillan[1]

[1]*Hawaii Pacific University, College of Natural and Computational Sciences*

These notes provide a quick overview of various algebraic structures arising in modern physics. For brevity's sake no attempt at thoroughness is made as each topic merits voluminous books and indeed many fine texts exist. Students are strongly encourages to avail themselves of those resources. Rather these notes represent a rudimentary introduction to the vast subject of universal algebra. I will cover several structures including groups, rings, modules, and algebras and will introduce number systems involving split- and dual- algebras. Applications to high-energy physics will be briefly discussed. As always, these notes are intended for students and do not reflect original research. I will correct errors as I find them, so the notes at any time $t < \infty$ should be considered incomplete.

## I. OVERVIEW

Here as he walked by
on the 16th of October 1843
Sir William Rowan Hamilton
in a flash of genius discovered
the fundamental formula for
quaternion multiplication
$i^2 = j^2 = k^2 = ijk = -1$
and cut it on a stone of this bridge.

*Plaque on Brougham Bridge, Dublin*

Real numbers (denoted as a set by $\mathbb{R}$) have been known since circa 500 B.C. when Greek mathematicians realized that in addition to the rationals ( numbers which may be expressed as quotients of integers) there also exists numbers such as $\pi$, $\sqrt{2}$, etc. which aren't realizable as integer quotients. It was not until the 16th century that a new number system, the complex numbers (denoted by $\mathbb{C}$), was devised by Italian mathematicians Cardano and Tartaglia to describe roots of polynomial equations. In the 19th century Hamilton discovered quaternions $\mathbb{H}$ and Cayley formulated the octonions $\mathbb{O}$. Additionally there are other less-known algebras such as 'split' and 'dual' versions of complex, quaternionic and octonionic numbers, as well as other extensions such as sedenions.

*Dimensionality.* The dimensionality of a space is defined as the cardinality (i.e., size) of a basis set containing the minimum number of linearly-independent elements spanning the entire space. For the various spaces mentioned above, one finds:

- Reals: $\dim(\mathbb{R}) = 1 = 2^0$ with basis set $B = \{1\}$,
- Complex numbers: $\dim(\mathbb{C}) = 2 = 2^1$ with basis set $B = \{1, i\}$,
- Quaternions: $\dim(\mathbb{H}) = 4 = 2^2$ with basis set $B = \{1, i, j, k\}$,
- Octonions: $\dim(\mathbb{O}) = 8 = 2^3$ with basis set $B = \{1, i, j, k, l, il, jl, kl\}$,
- Sedenions: $\dim(\mathbb{S}) = 16 = 2^4$ with basis set $B = \{1, i, j, k, l, il, jl, kl, m, im, jm, km, lm, ilm, jlm, klm\}$.

As one observes, dimensionality doubles as additional base elements are added to produce new number systems. This process is known as Cayley-Dickinson construction. It is understood that elements of $\mathbb{C}$, $\mathbb{H}$, $\mathbb{O}$, and $\mathbb{S}$ are taken over the reals. Algebraic properties change as well as one goes to higher-dimensional spaces. For example, multiplication is commutative and associative for both real and complex numbers. However quaternion multiplication is not commutative (though associativity remains). Octonion multiplication is neither commutative nor associative. With sedenions another property, divisibility, is lost as well: sedenions possess *zero divisors* whence one can find non-zero $a$, $b \in \mathbb{S}$ such that $a\,b = 0$.

**Some Terminology From Universal Algebra.**

In any field of endeavor it is always essential to be well-versed in the pertinent fundamental underlying concepts in order to eventually gain mastery of the subject. However, having a broad perspective is important as well. Specialization occurs at the professional level but the student should strive to be a Renaissance person. The prolific mathematician Paul Halmos once quipped one can learn a lot of mathematics simply by reading the first chapters of many textbooks. I agree and encourage students to follow suit. In this section we cover some of those relevant elementary ideas. Students familiar with abstract algebra might be inclined to skip this portion but shouldn't as we shall present a hopefully broader view of the subject and, besides, a little review never hurts.

*Universal Algebra.* The perspective of universal algebra is that of a broad overview of abstract algebra. Its targets are algebraic structures. So we must first define that term. Recall our mathematical education began with learning about numbers. Once we had those numbers we needed to do something with them, so we were then taught various processes such as addition, subtraction, multiplication, and division. Each such process, known formally as an *operation*, is simply a means by which we take numbers and combine them in some manner to form other numbers. The numbers (or other objects of interest) are considered to be elements of a *set*, a well-defined collection of objects which itself may be considered as a singular object. An operation basically maps a set to itself. Given a set $S$, an textitn-ary operation is a map $S^n \to S$, where $S^n$ represents $n$ copies of $S$. In other words, an n-ary operation takes $n$ objects in the set and converts them to a single object within the set. For example, a *nullary operation* maps the null set $\emptyset$ to a particular element in $S$ usually 0 (the additive identity) or 1 (the multiplicative identity element). A *unary* operation is a map $S \to S$. A typical unary operation is taking the inverse $x^{-1}$ of an element $x \in S$, that is to say $x \mapsto x^{-1}$. *Binary* operations take two elements $x, y \in S$ to form a third element $z$. Operations such as addition or multiplication are therefore binary. Now we are in a position to define the subject of these notes.

**Definition:** An *algebraic structure* consists of a set $S$ known as the underlying or *carrier set* along with a collection of finitary operations and a finite number of identities known as *axioms* which govern the usage of operations.

The definition provided above represents the broadest explanation of algebraic structures. More concretely, examples of algebraic structures include groups, rings, lattices, vector spaces, modules, and algebras. Let us begin with perhaps the most fundamental object of interest here - the group.

*Groups.* Let $G$ be a non-empty set with a composition rule called *group multiplication* (denoted by $\circ$) which permits us to combine group elements to produce other elements. Thus a *group* $(G, \circ)$ satisfies the following axioms:

- **Closure:** Given elements two elements $g_1, g_2 \in G$, $g_1 \circ g_2 \in G$,
- **Identity:** There exists a unique element $e \in G$ called the identity element which satisfies $e \circ g = g \circ e = g$ $\forall\, g \in G$. Thus the identity commutes with all group elements.
- **Inversion:** For each group element $g$, there is a unique element $g^{-1}$ called the *inverse* of $g$ which satisfies $g \circ g^{-1} = g^{-1} \circ g = e$,
- **Associativity:** Given three group elements $g_1$, $g_2$, and $g_3$, $(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$.

These axioms define all essential group properties. The term "group multiplication" is of course generic; the actual operation may be multiplication, addition, or some more abstract process depending on the underlying set such as composition of functions or matrix multiplication. Note commutativity isn't generally required (except for the identity element and multiplication of elements by their inverses) and thus isn't a necessary condition. If it so happens that group multiplication is always commutative then the group is labeled a commutative or *abelian* group. From the above discussions we note group multiplication is a binary operation, identity is nullary, and inversion is unary.

**Some Examples Of Groups:**

- The real numbers $\mathbb{R}$ under addition $(\mathbb{R}, +)$ is an abelian group,
- Real numbers with zero excluded, $\mathbb{R}\backslash\{0\}$ likewise forms an abelian group under multiplication,
- The set of all $n \times n$ non-singular real matrices forms a non-abelian group under matrix multiplication called the *general linear group* $GL(n) = \{M \in \mathbb{R}^{n\times n} \mid \det(M) \neq 0\}$,

- The set of all $n \times n$ unimodular real matrices under matrix multiplication forms the *special linear group* $SL(n) = \{M \in \mathbb{R}^{n\times n} \mid \det(M) = 1\}$,
- The set of all permutation of $n$ objects $S_n$ forms a group under composition. $S_n$ is non-abelian for $n \geq 3$,
- The set of all polynomials with real coefficients $\mathbb{R}[x]$ under addition constitutes an abelian group,
- The set of integers $\mathbb{Z}$ under addition.

There are of course many more examples but the above list hopefully illustrates the diversity of possible groups. As seen from the above cases, groups may be finite (such as the permutation groups) or infinite such as the reals (continuous, uncountably infinite) or the integers (countably infinite).

**Some Important Results From Group Theory.**

A *subgroup* of $G$ consists of a subset of $G$ that satisfies all group axioms. For example the special linear group $SL(n)$ is a subgroup of $GL(n)$. All groups have at least two subgroups, the *trivial subgroup* $\{e\}$ containing only the identity and $G$ itself (the*improper subgroup*).

**Lagrange's Theorem.** Let $G$ be a finite group of order (cardinality) $n$, that is $G$ has $n$ elements, or equivalently $|G| = n$. Then possible subgroups possess orders equal to the positive integer factors of $n$.

Notice I wrote possible subgroups - if $G$ possesses a non-trivial subgroup $H$, then $|H| \mid |G|$. However the converse of Lagrange's Theorem is not generally true; it is not the case that if $|G|$ is composite, then subgroups of each permissible factor order *must* exist. For example, $A_4$, the group consisting of even permutations of four objects, has 12 elements yet $A_4$ has no order 6 subgroup (despite 6 being a factor of 12). So one should proceed with caution.

**Example:** Let $\mathbb{Z}_6$ be the group $\{0, 1, 2, 3, 4, 5\}$ under addition modulo 6. The factors of 6 are 1, 2, 3, and 6, whence from Lagrange's Theorem the subgroups are:

- Order 1: the subgroup is $\{0\}$,
- Order 2: the subgroup is $\{0, 3\}$,
- Order 3: the subgroup equals $\{0, 2, 4\}$,
- Order 6: the subgroup is $\mathbb{Z}_6$ itself.

Let us pursue some concepts using this example. Set $\langle a\rangle = \{x \mid x = a^n \mod 6,\ n \in \mathbb{Z}\}$. Since group multiplication equals modulo 6 addition in this example, $a^n = \underbrace{a + a \ldots + a}_{\text{n times}} \mod 6$. Thus $\langle 0\rangle = \{0\}$, $\langle 1\rangle = \langle 5\rangle = \mathbb{Z}_6$, $\langle 2\rangle = \langle 4\rangle = \{0, 2, 4\}$, and $\langle 3\rangle = \{0, 3\}$. Thus $\langle a\rangle$ yields all subgroups of $\mathbb{Z}_6$ as $a$ runs from 0 to 5. Also notice $\langle 1\rangle$ and $\langle 5\rangle$ forms the entire group. So either 1 or 5 may be employed to generate the entire group. Thus 1 and 5 are called *generators* of $\mathbb{Z}_6$. Let us now give a formal definition of a generator:

**Definition:** A *generator* $x$ of a group $G$ is an element which reproduces the entire group via group multiplication, that is $\langle x\rangle = G$, where $\langle x\rangle = \{\, x^n \mid n \in \mathbb{Z}\}$. A group $G$ which can be reproduced from a single element is called a *cyclic group*. If a group $G$ has multiple generators $x_1, x_2, \ldots x_m$, then the generating set as written as $\langle x_1,\ x_2,\ \ldots x_m\rangle$.

For cyclic groups, generators have the form $\langle x,\ x^{-1}\rangle$. In the above case, the additive inverse of 1 is indeed 5. For the infinite cyclic group $(\mathbb{Z},\ +)$ the generating set is $\langle 1,\ -1\rangle$. For the cyclic group $(\mathbb{Z}_5,\ +)$, 1 and 4 are inverses as are 2 and 3. The generating set is then $\langle 1,\ 2,\ 3,\ 4\rangle$. Indeed, for a cyclic group of any order $n$, $n-1$ is always a generator.

If a group has only one generator it can have at most two elements. Let $x$ be the sole generator of some group. The group must have an identity element $e$. Likewise $x$ must have an inverse, but being the sole generator its inverse is $x$ itself. This means $x^2 = e$. Whence the group is $\{e,\ x\}$.

**The Euler Totient Function.**

Using the above example of $(\mathbb{Z}_6, +)$, define a function h(a) = gcd($a$, 6) for $a$ = 1,2,3,4,5. Then only h(1) and h(5) = 1 as 1 and 5 are the only non-zero numbers relatively prime to 6. Thus if $x$ is a generator, it is the case h($x$) = 1. The *Euler totient function* $\phi(n)$ is defined as the number of integers $k$ relatively prime to $n$ in the range $1 \leq k \leq n$. So in our example $\phi(6) = 2$. As another example, what is $\phi(10)$? Only 1, 3, 7, and 9 are relatively prime to 10, so $\phi(10) = 4$. Note that $(\mathbb{Z}_{10}, +)$ has as its generating set $\langle 1, 3, 7, 9\rangle$. As an exercise, prove $\mathbb{Z}_{10} = \langle 1\rangle = \langle 3\rangle = \langle 7\rangle = \langle 9\rangle$ (remember to use mod 10 addition!). For $n$ prime, it is readily seen $\phi(n) = n - 1$. As another exercise, write down the generating set of $(\mathbb{Z}_7, +)$. The Euler totient function also has the interesting property that if $m$ and $n$ are relatively prime, then $\phi(m\,n) = \phi(m)\,\phi(n)$. Whence the function is *almost*, but not quite, a homomorphism over $\mathbb{Z}^+$. For example, $\phi(18) = \phi(2)\,\phi(9) = 6$ (do you see why?), but $\phi(3)\,\phi(6) = 4$. Why do the results differ despite the fact 9 x 2 = 3 x 6 ? Two and nine are relatively prime; three and six aren't.

**Example:** $\mathrm{Q}_8$**.**

Define the *quaternion group* $(\mathrm{Q}_8, \times)$ to be the set $\{1, -1, i, -i, j, -j, k, -k\}$ under multiplication. This group is obviously non-abelian as quaternion multiplication is non-commutative. The order $|\mathrm{Q}_8| = 8$, so possible subgroups will be of orders 1, 2, 4, and 8. I list all subgroups below.

- Order 1: The sole singleton subgroup consists of the multiplicative identity $\{1\} = \langle 1\rangle$.
- Order 2: The subgroup is $\{1, -1\} = \langle -1\rangle$.
- Order 4: There are in fact 3 subgroups of order 4 -
- $\{1, -1, i, -i\} = \langle i\rangle$,
- $\{1, -1, j, -j\} = \langle j\rangle$, and
- $\{1, -1, k, -k\} = \langle k\rangle$.
- Order 8: $\mathrm{Q}_8$ itself, which can be expressed as $\langle i\rangle \cup \langle j\rangle \cup \langle k\rangle$.

$\mathrm{Q}_8$ possesses multiple generators with a generating set given by $\langle i, j\rangle$.

**Example:** $(n\mathbb{Z}, +)$

Given an integer $n > 0$, the underlying set $n\mathbb{Z} = \{\ldots - 2n, -n, 0, n, 2n, \ldots\}$. It is readily seen this set is closed under addition. The generating set is given by $\langle n, -n\rangle$. As a cyclic group it can be expressed as $\{n^z \mid \text{where } n^z \coloneqq z\,n,\ z \in \mathbb{Z}\}$.

**The Center Of A Group.**

The *center* of a group $G$ is defined as the set of elements that commute with all group elements. Thus formally the center $Z(G) \coloneqq \{\, x \in G \mid \forall\, g \in G,\ x\,g = g\,x \,\}$.

The "Z" here comes from the German word *Zentrum*, meaning center. It is easily demonstrated the center always constitutes a subgroup of $G$. First, the identity element $e \in Z(G)$ since $e\,g = g\,e = g$ for all $g \in G$ by definition. Next, let $g_1,\ g_2 \in Z(G)$ and let $x$ be some arbitrary element of $G$. Then $g_1\,g_2\,x = g_1\,x\,g_2 = x\,g_1\,g_2$ since $g_1,\ g_2$ commute with all $x$. Thirdly, consider $g^{-1}$ for some $g \in Z(G)$. For any $x \in G$, $g\,x = x\,g$. Left-multiplying by $g^{-1}$ yields $x = g^{-1}\,x\,g$. Now right-multiply by $g^{-1}$ to obtain $x\,g^{-1} = g^{-1}\,x\,g\,g^{-1} = g^{-1}\,x\,e = g^{-1}\,x$. This concludes the proof that $Z(G)$ is a subgroup of $G$. If it is the case that $G$ is abelian, then the center is the entire group i.e., $Z(G) = G$. Of course this is not generally the case; non-abelian groups satisfy $|Z(G)| < |G|$. If $Z(G) = \{e\}$, then $G$ is called a *simple group*. I will discuss this in more detail shortly.

**Conjugacy Classes.**

Two group elements $x$, $y$ are said to be *conjugate* if there exists a $g \in G$ such that $y = g\,x\,g^{-1}$. This relation establishes equivalence classes called *conjugacy classes*. For abelian groups each element forms a singleton conjugacy class while non-abelian groups have conjugacy classes containing multiple elements. Thus conjugacy classes measure how "abelian" a group is. For example, $\mathbb{Q}_8$ has conjugacy classes $\{1\}$, $\{-1\}$, $\{i, -i\}$, $\{j, -j\}$, and $\{k, -k\}$. Note the subgroup $\{1, -1\} \simeq \mathbb{Z}_2$ in fact is abelian with the expected conjugacy classes.

**Normal Subgroups.**

The center $Z(G)$ is not merely a subgroup of $G$, but rather is a special subgroup known as a *normal subgroup* of $G$. A normal subgroup $N$ of $G$ partitions $G$ into subsets called *cosets* such that *left-cosets* of the form $x\,N$ equal *right cosets* $N\,x$ where $x \in G$. Thus group elements are *invariant under conjugation* with normal subgroups: $N\,x\,N^{-1} = x$. A word of caution is in order here: $x\,N = N\,x$ does **not** mean $n_1\,x = x\,n_1$ for all $n_1 \in N$. It simply means $n_1\,x = x\,n_2$ for some $n_2 \in N$. Indeed, for non-aelian groups $n_1$ and $n_2$ will usually differ. We indicate $N$ is a normal subgroup of $G$ by $N \triangleleft G$. A *simple group* is now defined as one whose only normal subgroups are the trivial subgroup $\{e\}$ and $G$ itself. Any non-simple group may be split into two groups, the (non-trivial) normal subgroup $N$ and the *quotient group* $G/N$ formed by modding $G$ with $N$. So in this respect, normal subgroups act as the "prime numbers" of groups in that a group is either normal or may be expressed as the quotient group and the normal subgroup. In particular if $|G| = p^k$ where $p$ is prime and $k \in \mathbb{N}$, then any subgroup of order $p$ will be normal. Normal subgroups also play another special role - only normal subgroups can produce quotient groups. Consider the above examples. All subgroups of $(\mathbb{Z}_6, +)$are normal. $(Q)_8$ is especially interesting case: all subgroups are normal though the group itself in non-abelian. As an example of a simple group, consider $(\mathbb{Z}_5, +)$. Group elements are 0, 1, 2, 3, 4 with multiplication being modulo 5 addition. The only subgroups are $\{0\}$ and $\mathbb{Z}_5$ itself and they are both normal. In fact, $(\mathbb{Z}_p, +)$ is always simple when $p$ is prime. To illustrate cosets, let's review $G = (\mathbb{Z}_6, +)$. Choose $N = \{0, 3\}$. Since the group is abelian, left- and right- cosets are identical. We list them below.

- $N = \{0, 3\}$,
- $1 + N = 4 + N = \{1, 4\}$,
- $2 + N = 5 + N = \{2, 5\}$.

Note $\{1, 4\}$ and $\{2, 5\}$ aren't subgroups, they're just sets. The quotient group $G/N$ has $|6|/|2| = 3$ elements and is given by

$$G/N = \{\, \{0, 3\}, \{1, 4\}, \{2, 5\} \,\}.$$

$\{0, 3\}$ acts as the identity element with $\{0, 3\} + \{1, 4\} = \{1, 4\}$ and $\{0, 3\} + \{2, 5\} = \{2, 5\}$. Also $\{1, 4\} + \{2, 5\} = \{0, 3\}$.

**Example Of A Non-normal Subgroup.**

I shall now provide an example of a non-normal subgroup. Consider the dihedral group $D_3$ consisting of all symmetries of an equilateral triangle. $D_3$ is a non-abelian group of order 6 and is isomorphic to $S_3$, the group of permutations of 3 objects. For the student's convenience, I include a visual representation below. Think of the triangle as lying in the x-y plane, centered at the origin with the upper vertex on the y-axis. The identity $e$ represents the triangle in its initial configuration, $r$ represents a $120^o$ counter-clockwise rotation around the z-axis, and $s$ represents a $180^o$ rotation around the y-axis.

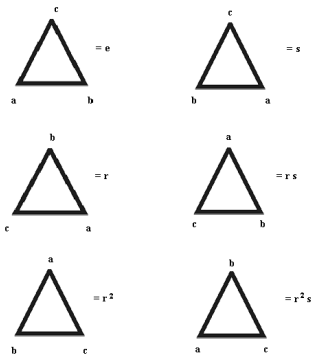


FIG. 1: The dihedral group $D_3$ illustrated.

We now identify all subgroups of $D_3$: $\{e\}$, $\left\{e,\, r,\, r^2\right\}$, $\{e,\, s\}$, and $D_3$ itself. Consider the subgroup $\langle s\rangle = \{e,\, s\}$. The left coset $r\,\langle s\rangle = \{r, r\,s\}$, while the right coset $\langle s\rangle\, r = \left\{r,\, s\,r = r^2\,s\right\}$. So left and right cosets differ in this case, whence $\langle s\rangle$ is not a normal subgroup. On the other hand, the order 3 subgroup $\left\{e,\, r,\, r^2\right\}$, the cyclic abelian group of rotations around the z-axis, is normal and forms the quotient group

$$G/N \;=\; \left\{\left\{e,\, r,\, r^2\right\},\, \left\{s,\, r\,s,\, r^2\,s\right\}\right\}.$$

**Commutators, Centralizers, and Normalizers.**

*Commutators.* Let $G$ be a group and $x,\, y \in G$. The *commutator* of $x$ and $y$ is defined as $(xy)(yx)^{-1} = xyx^{-1}y^{-1}$ and is typically denoted by $[x,\, y]$. This notation should be quite familiar to physics students as it's commonly employed in quantum mechanics. The set generated by all commutators in $G = \langle\, [x,\, y]\,\rangle$ is called the *commutator subgroup* also known as the *derived group* $G'$ of $G$. Another commonly used notation is $[G,\, G]$. The derived group is a normal subgroup of $G$, i.e., $G' \triangleleft G$. The last statement merits proof. First, we need to demonstrate $G'$ is a group and secondly we need to show it is normal in $G$. Let us show $G'$ satisfies all group axioms:

- (i) $e \;=\; e\,e\,e^{-1}\,e^{-1}$ whence $e \in G'$.
- (ii) If $g_1,\, g_2 \;\in\; G'$ then $g_1\,g_2 \;\in\; G'$ as $g_1\,g_2$ is a product of commutators.
- (iii) Given $g = xyx^{-1}y^{-1}$ the inverse $g^{-1}$ is easily seen to be $yxy^{-1}x^{-1}$.

**Caution:** the commutator subgroup is *not* merely the set of all commutators. Depending on the underlying group, the set of all commutators might not even be a subgroup. One cannot assume the product of two commutators is another commutator. For finite groups however this won't be an issue until $|G| \;=\; 96$.

The most important feature of the commutator subgroup however is that for any group $G$, the quotient group $G/G'$ is *always* abelian. This is sometimes called the abelianization of $G$.

**Centralizers And Normalizers.**

Let $S$ be an arbitrary non-empty subset of a group $G$. The *commutant* or *centralizer* $C(S)$ of $S$ is defined as the set of all $g \;\in\; G$ that commute with every element in $S$, that is to say

$$C(S) \;\coloneqq\; \{\, g \;\in\; G \,|\, \forall\, s \;\in\; S,\; g\,s \;=\; s\,g\,\}.$$

Whence we can think of centralizers as mini-versions of centers. Indeed if $S = G$, then obviously $C(G) \;=\; Z(G)$. The centralizer $C(S)$ is always a subgroup $G$ and if $G$ is abelian then for any $S \subseteq G$, $C(S) \;=\; G$. $C(S)$ thus will not in general contain $S$ and only does so when $S$ is abelian. However $C(\,C(S)\,)$ will always contain $S$ regardless.

The *normalizer* $N(S)$ of $S$ satisfies a slightly weaker condition than the centralizer. The normalizer consists of those elements in $G$ for which "left cosets" and "right cosets" formed by $S$ are equal. Thus it's similar in concept to a normal subgroup. Formally we define the normalizer:

$$N(S) \coloneqq \{\, g \in G \mid g\,S = S\,g \,\}.$$

To be specific, the normalizer is such that $g\,s = t\,g$ where $s,\, t \in S$. Like the centralizer, the normalizer is also a subgroup of $G$. Clearly it is also the case that the centralizer is contained within the normalizer, that is $C(S) \subseteq N(S)$. In fact the centralizer is a *normal subgroup* of the normalizer $C(S) \triangleleft N(S)$. If $H$ is a subgroup of $G$ then $N(H)$ will in fact be a normal subgroup of $G$. So for an arbitrary subset $S$, we can always establish a normal subgroup, namely $N(\,N(S)\,)$.

**Example: $Q_8$ Again.**

The results are trivially simple if $G$ is an abelian group, so let's use a non-abelian group instead. We again turn to the quaternion group $Q_8$. Let our arbitrary set $S = \{i,\, k,\, -k\}$. This is certainly not a subgroup of $Q_8$ so it will do quite nicely for our purposes. First, the centralizer is given by

$$C(S) = \{1,\, -1\},$$

which we note is a normal subgroup of $Q_8$. Now one finds the normalizer to be

$$N(S) = \{1,\, -1,\, i,\, -i\},$$

which is also a normal subgroup of $Q_8$. In fact the quotient group $Q_8/N(S)$ is given by

$$Q_8/N(S) = \{\, \{1,\, -1,\, i,\, -i\},\, \{j,\, -j,\, k,\, -k\} \,\}.$$

We also note $N(S)$ contains the centralizer as expected and that the centralizer is a normal subgroup of the normalizer as well. In fact we can write

$$N(S)/C(S) = \{\, \{1,\, -1\},\, \{i,\, -i\} \,\}.$$

Now let's look at commutators. It turns out all commutators (which recall have the form $x\,y\,x^{-1}\,y^{-1}$) formed in $Q_8$ are either 1 or -1. So the derived group $G' = \{1,\, -1\}$ and the quotient group

$$G/G' = \{\, \{1,\, -1\},\, \{i,\, -i\},\, \{j,\, -j\},\, \{k,\, -k\} \,\},$$

which is an abelian group isomorphic to the Klein Vierergruppe.

**Rings.**

Now that we have introduced groups the next algebraic structure to consider is the *ring*. Before giving a formal definition, let me state that, roughly speaking, a ring is a set whose elements may be added, subtracted, or multiplied but not necessarily divided. The archetypal example of a ring is the set of integers $\mathbb{Z}$ which closed under addition and multiplication (subtraction is merely adding a negative or *additive inverse*) but not division. For example take any two integers, say 2 and 3. Both $2 + 3$ and $2 \times 3$ are integers but $\frac{2}{3}$ and $\frac{3}{2}$ aren't. We say $\mathbb{Z}$ isn't 'closed' under division. Let us now proceed with the formal definition.

**Definition:** A **ring** $(R,\, +,\, \mathrm{x})$ consists of a non-empty set $R$ along with two operations addition $(+)$ and multiplication (x) that satisfies the following axioms:

- $(R,\, +)$ is an abelian group. Thus there is an additive identity element 0 such that $r + 0 = 0 + r = r$ for all $r \in R$ and for each element $r$ there exists an element $-r$ called the *additive inverse* of $r$ satisfying $r + (-r) = 0$.
- $(R \backslash \{0\}\,, \times)$ is a *monoid*, an associative algebraic structure similar to a group but possibly lacking multiplicative inverses. Some mathematicians do not require rings to possess a multiplicative identity (denoted by 1), in which case $(R \backslash \{0\}\,, x)$ is a semi-group. and is called a *rng* because identity (the "i") is missing. A monoid is a semi-group with identity.
- Multiplication is distributive over addition thus $a \cdot (b+c) = a \cdot b + a \cdot c$ (*left distributivity*) and $(b+c) \cdot a = b \cdot a + c \cdot a$ (*right distributivity*).

**Some Examples Of Rings.**

- The integers, the reals, the rationals, and the complex numbers with addition and multiplication form commutative rings.
- The quaternions with addition and multiplication form a non-commutative ring.
- Polynomials with real, rational, or complex coefficients i.e., $\mathbb{Z}[x]$, $\mathbb{R}[x]$, $\mathbb{Q}[x]$, $\mathbb{C}[x]$, form commutative rings. $\mathbb{Z}[x]$ is pronounced "Z adjoin x" where $x$ is called an independent variable or *indeterminate*.
- Integers modulo n, written as $\mathbb{Z}_n \simeq \mathbb{Z}/n\mathbb{Z}$ where $n$ is a positive integer, form a commutative ring.

Ring multiplication is not required to be commutative, but if it is then the ring is called a *commutative ring*. Addition is always commutative so it is understood the adjective 'commutative' refers to multiplication. If a ring element has a multiplicative inverse, that element is called a *unital*. Elements not possessing multiplicative inverses are called *proper elements*. Thus the set of integers $\mathbb{Z}$ has only two unitals, namely 1 and $-1$. A commutative ring where all non-zero elements are unitals is called a *field*. In other words, a field is a commutative ring where both $(R, +)$ and $(R\backslash\{0\}, \times)$ are abelian groups. If one takes the position that the multiplicative identity isn't required, then rings containing 1 are variously called unit rings, unital rings, unitary rings, rings with identity, or simply rings with 1. To avoid confusion, I prefer the term 'ring with identity'. Also, by 'unital ring' I shall mean a ring in which all nonzero elements are unitals; that makes far more sense to me than simply meaning the presence of 1. Unitals automatically imply the existence of 1, so my definition is more economical. So **properly restated**, a *field* is an *associative unital commutative ring*. This formulation guarantees the group properties mentioned above are satisfied while eschewing vague terminology.

**Ideals Of Rings.**

Let $R$ be a ring. An *ideal* $I$ is a sub-ring of $R$ that 'absorbs' all elements in $R$. Formally, ideals satisfy the following axioms:

- For a ring $R$, $(R, +)$ is always an abelian group. An ideal $I$ is an additive subgoup of $R$, i.e., $(I, +)$ is also an abelian group.
- $I$ is a *left ideal* of $R$ if for all $r \in R$ and all $s \in I$ $rs \in I$.
- $I$ is a *right ideal* of $R$ if for all $r \in R$ and all $s \in I$ $sr \in I$.
- $I$ is a *two-sided ideal* of $R$ if $I$ is both a left- and right- ideal of $R$.

**Example.** Let $\mathbb{R}[x]$ be the polynomial ring with real coefficients. An element of $\mathbb{R}[x]$ thus possesses the form

$$r(x) = \sum_{k=0}^{\infty} a_k\, x^k, \text{ where } a_k \in \mathbb{R}.$$

We seek polynomials, not transcendental functions, so we require all but a finite number of $a_k$ values be zero. Let us choose the ideal

$$I = \langle x^2 + 1\rangle \coloneqq \left\{ p(x) \in R \,|\, p(x) = q(x)\left(x^2 + 1\right),\, q(x) \in R\right\}.$$

Roughly speaking, ideals are to rings what normal subgroups are to groups. This implies the ring modded by the ideal is also a ring called a *factor ring*. Thus we find

$$\mathbb{R}[x]/\langle x^2 + 1\rangle = \left\{ax + b + \langle x^2 + 1\rangle \,|\, a,\, b \in \mathbb{R}\right\}.$$

So in the factor ring. $\langle x^2 + 1\rangle$ acts effectively as the additive identity, that is to say zero. Whence $x^2 + 1 = 0$, or $x^2 = -1$. This implies the factor ring $\mathbb{R}[x]/\langle x^2 + 1\rangle$ is in fact isomorphic to the complex numbers $\mathbb{C}$. The factor ring in this example therefore constitutes a map from the polynomials to the complex numbers.

*Principal Ideals.* Given a ring $R$, an ideal $I \subseteq R$ generated from a single element $a \in R$ is called a *principal ideal*. Of course if a ring is commutative left- and right- ideals are always identical. So we only distinguish cases for non-commutative rings, of which there are three types listed below.

- A *principal left-ideal* generated by an element $a \in R$ is defined as the set $I_a^L ::= \{ r\,a \mid r \in R\}$.
- A *principal right-ideal* generated by an element $a \in R$ is defined as the set $I_a^R ::= \{ a\,r \mid r \in R\}$.
- A *principal two-sided ideal* generated by an element $a \in R$ is defined as the set $I_a^{T-S} ::= \{ r\,a\,s \mid r, s \in R\}$.

As an example, the ideal $\langle x^2 + 1\rangle$ in $\mathbb{R}[x]$ is principal, as are $\langle x\rangle$ (all uni-variate polynomials of degree $\geq 1$), or $\langle x^2\rangle$ (all uni-variate polynomials of degree $\geq 2$). Let us now show an example of an ideal that is *not* principal. Define $\mathbb{R}[x,\, y]$ as the set of all polynomials in two variables. So, for example, a bi-variate polynomial of degree two possesses the general form

$$p(x,\, y) \,=\, a_0 \,+\, a_1\, x \,+\, a_2\, y \,+\, a_3\, x^2 \,+ a_4\, xy \,+ a_5\, y^2.$$

Now define the ideal

$$\langle x,\, y\rangle \,\coloneqq\, \{p(x,\, y)x \,+\, q(x,\, y)y \mid p(x,\, y),\, q(x,\, y) \,\in\, \mathbb{R}[x,\, y]\}\,.$$

Thus the ideal $\langle x,\, y\rangle$ consists of all bi-variate polynomials of degree $\geq 1$. We show that it cannot be principal. For a principal ideal, $I = \langle p\rangle$ where $p$ is some bi-variate polynomial. Thus we must have $x = g_1(x,\, y)p$ and $y = g_2(x,\, y)p$ for some $g_1,\, g_2$. The only polynomials dividing $x$ however have the form $a$ or $ax$ where $a$ is a non-zero real number. Likewise the only polynomials dividing $y$ have the form $a$ or $ay$. Therefore the only polynomials dividing *both* $x$ and $y$ are unitals of $\mathbb{R}$, i.e, constants. This would imply $p$ is a constant and the ideal $\langle p\rangle$ would thus include constant terms (polynomials of degree zero). This is a contradiction because we know $\langle x,\, y\rangle$ contains only polynomials of degree $\geq 1$. So we have verified $\langle x,\, y\rangle$ is non-principal by *reductio ad absurdium. Quod erat demonstrandum.*

**Example:** Let $I$ and $J$ be ideals over the same ring $R$. Show that $I + J$ and $I \cup J$ are ideals and that $I \cup J \subseteq I + J$,

**Solution:** Let $K = I + J = \{\, a + b \mid a \in I,\, b \in J\,\}$. Then an element of $rK = ra + rb$ . But $ra \in I$ and $rb \in J$, whence $rK = K$. Let $L = I \cup J = \{\, a \mid a \in I \cup J\,\}$. An element $ra$ is in $I$ or $J$ , so $ra \in I \cup J$. $I + J$ contains all elements in both $I$ and $J$ and thus contains $I \cup J$ (note: since zero is always in the ideals, we can write e. g., $I = I + 0\ J$, etc.). Thus we have $I \cup J \subseteq I + J$. To prove the converse is not true, a single counter-example suffices. Let the ring $R = \mathbb{Z}$ and let $I = 2\,\mathbb{Z}$ and $J = 3\,\mathbb{Z}$. Then $I \cup J = \{a \in R \mid a = 2m \text{ or } 3n \text{ where } m, n \in \mathbb{Z}\} = \{\ldots, -6,\, -4,\, -3,\, -2,\, 0,\, 2,\, 3,\, 4,\, 6,\, \ldots\}$. However $I + J = \{\, a \in R \mid a = 2m + 3n \text{ where } m, n \in \mathbb{Z}\,\}$. It is readily seen $I + J = \mathbb{Z}$.

*Zero Divisors.* Let $(R,\, +,\, \mathrm{x})$ be a ring. Now consider $(R\backslash\,\{0\}\,,\, \times)$. If some elements multiply to zero, then the ring is said to have zero divisors. The most common examples of rings with zero divisors are those where $R = \mathbb{Z}_n$ where $n$ is composite, that is to say, $n$ is a positive non-prime integer. To illustrate this concept, take $R = \mathbb{Z}_6 \,=\, \mathbb{Z}/6\mathbb{Z}$. The integers are now partitioned into 6 subsets where, in each set, elements differ by multiples of 6:

- $\overline{0} \,=\, \{\ldots, -18,\, -12,\, -6,\, 0,\, 6,\, 12,\, 18, \ldots\}$,
- $\overline{1} \,=\, \{\ldots, -17,\, -11,\, -5,\, 1\,7,\, 13,\, 19, \ldots\}$,
- $\overline{2} \,=\, \{\ldots, -16,\, -10,\, -4,\, 2,\, 8,\, 14,\, 20, \ldots\}$,
- $\overline{3} \,=\, \{\ldots, -15,\, -9,\, -3,\, 3,\, 9,\, 15,\, 21, \ldots\}$,
- $\overline{4} \,=\, \{\ldots, -14,\, -8,\, -2,\, 4,\, 10,\, 16,\, 22, \ldots\}$,
- $\overline{5} \,=\, \{\ldots, -13,\, -7,\, -1,\, 5,\, 11,\, 17,\, 23, \ldots\}$.

Such 'hyper-numbers' were first discovered by Gauss who found that addition respects the subset classification. So if an element of $\overline{3}$ is added to any element in $\overline{4}$ the result is an element in $\overline{1}$. In other words these hyper-numbers obey addition modulo 6 since $(3 \mod 6) + (4 \mod 6) = (7 \mod 6) = (1 \mod 6)$. So we only need representative elements from each set, thus we write $\mathbb{Z}_6 \,=\, \{0,\, 1,\, 2,\, 3,\, 4,\, 5\}$. Now let us write the multiplication table which of course will be multiplication mod 6 excluding zero. Even though zero was excluded from the table, some entries are

| x | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 | 5 |
| 2 | 2 | 4 | 0 | 2 | 4 |
| 3 | 3 | 0 | 3 | 0 | 3 |
| 4 | 4 | 2 | 0 | 4 | 2 |
| 5 | 5 | 4 | 3 | 2 | 1 |

TABLE I: Multiplication Table For $\mathbb{Z}_6$

nonetheless zero due to the fact that multiples of 6 occur in the multiplication. Hence $\mathbb{Z}_6$ contains zero divisors. Furthermore $(\mathbb{Z}_6 \backslash \{0\}, \times)$ fails to even be a group; from the table we note 3 has no inverse and of course the presence of zeroes implies the set isn't even closed.

**Integral Domains And Fields.**

Let $(R, +, \mathrm{x})$ be a ring. If it is the case $(R \backslash \{0\}, \times)$ contains no zero divisors then $R$ is called an *integral domain*. Looking at the table above, it can readily be seen that zeroes in the multiplication table of $\mathbb{Z}_n$ can be avoided by choosing $n$ to be prime. For example, let's look at the multiplication table of $\mathbb{Z}_5$.

| x | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 |
| 2 | 2 | 4 | 1 | 3 |
| 3 | 3 | 1 | 4 | 2 |
| 4 | 4 | 3 | 2 | 1 |

TABLE II: Multiplication Table For The Integral Domain $\mathbb{Z}_5$

$\mathbb{Z}_5$ has no zero divisors and is therefore an integral domain. A unital commutative ring that is also an integral domain is called a *field*. The rationals, reals and complex numbers are thus (infinite) fields. $\mathbb{Z}_p$ where $p$ is prime are finite fields. Quaternions $\mathbb{H}$ constitute an integral domain that is not a field as quaternion multiplication is non-commutative.

*Semirings.* A *semiring* is another algebraic structure similar to a ring but without the requirement that each element have an additive inverse. For example, the natural numbers $\mathbb{N} = \{1, 2, 3, \ldots\}$ is not a groups as it lacks an identity element and there are no additive inverses. In fact $(\mathbb{N}, +)$ is a semigroup and $(\mathbb{N}, \times)$ is a monoid. Thus $(\mathbb{N}, +, \mathrm{x})$ is a semiring. Some authors refer to this structure as a "rig" (the "n" for "negative" being removed).

When one considers octonions another issue arises, namely its multiplicative non-associativity. So even with zero excluded, $(\mathbb{O} \backslash \{0\}, \times)$ cannot form a group. So a new structure is required - the non-associative ring. Non-associative rings are similar to rings but their multiplication needn't be associative. In the case of octonions $(\mathbb{O} \backslash \{0\}, \times)$ constitutes a group-like structure called a *loop*. Loops without multiplicative identity are called *quasigroups*.

**Division Rings.**

A *division ring* also called a *division algebra* is an algebraically closed unital ring with no zero divisors thus ensuring division is always possible. Furthermore division rings are automatically integral domains. By Wedderburn's 'little theorem' finite division rings are commutatiove and thus are finite fields. According to Frobenius' Theorem there are only 3 finite-dimensional associative division rings over the reals: the reals themselves $\mathbb{R}$, the complex numbers $\mathbb{C}$, and the quaternions $\mathbb{H}$. Notice we did not include the rational numbers $\mathbb{Q}$ as its closure is $\mathbb{R}$ (whence the algebraically closed condition). These algebras all have characteristic zero, meaning $1 + 1 + 1$ ... never sums to zero (unlike finite fields). The octonions $\mathbb{O}$ form an non-associative division algebra.

**Vector Spaces And Modules.**

Vector spaces are ubiquitous in physics, but let us give a formal definition. As it turns out, the mathematical definition is broader than the vectors of physics (which are elements of $\mathbb{R}^n$ in the finite-dimensional case or elements of a Hilbert space in the more general infinite-dimensional case). Vector spaces obey the following axioms:

- A vector space requires two sets, a field $F$ (usually the real or complex numbers) called *scalars* and a set $V$ of objects over $F$ called *vectors* along with two operations - *scalar multiplication* and *vector addition*,
- For any $a \in F$ and $\vec{v} \in V$, $a\vec{v} \in V$. This is scalar multiplication of vectors.
- For any two vectors $\vec{v}$, $\vec{w} \in V$, $\vec{v} + \vec{w} \in V$. This is vector addition.
- Associativity of addition: for any three vectors $\vec{x}\,\vec{y}, \vec{z} \in V$, $(\vec{x} + \vec{y}) :+ \vec{z} = \vec{x} + (\vec{y} :+ \vec{z})$.
- Commutativity of addition: For any two vectors $\vec{v}$, $\vec{w} \in V$, $\vec{v} + \vec{w} := \vec{w} + \vec{v}$.
- Existence of a additive identity: There exists a additive identity element called the zero vector $\vec{0}$ satisfying $\vec{0} + \vec{v} = \vec{v} + \vec{0} = \vec{v}$.
- Existence of an inverse: For each $\vec{v}$ there exists a vector $-\vec{v}$ such that $\vec{v} + (-\vec{v}) = \vec{0}$.
- Distributivity of scalar multiplication over vector addition: $a(\vec{v} + \vec{w}) = a\vec{v} + a\vec{w}$.
- Distributivity of scalar multiplication over field addition: $(a + b)\vec{v} = a\vec{v} + b\vec{v}$.
- Compatibility of scalar multiplication: $a(b\vec{v}) = (ab)\vec{v} = ab\vec{v}$.

These axioms fulfill all requirements for $(F, V)$ to be a vector space. Examples of vector spaces include $\mathbb{R}^n$, n x n matrices M$n$, $F$, complex numbers, and real-valued function spaces to name but a few.

**New Vector Spaces From Old.**

Given a vector space $V$ we may form new spaces by 'multiplying' $V$ by itself in various ways. We may also combine different vector spaces as well. The dimensionality of the generated spaces will naturally depend critically upon the dimensionalities of the underlying spaces and the 'multiplication' methods employed. Various products are in fact found in the literature, so the following list of examples must be incomplete by necessity. With that caveat in mind let us now look at a few examples.

**Example: The Cartesian Product.**

This is perhaps the simplest case. Given sets $A$ and $B$, the Cartesian product $A \times B \coloneqq \{\, (a, b) \mid a \in A,\ b \in B \,\}$. Naturally we can extend this concept to an n-fold product: given sets $A_1, A_2, \ldots A_n$ the Cartesian product $A_1 \times A_2 \ldots \times A_n \coloneqq \{\, (a_1, a_2, \ldots a_n) \,|a_i \in A_i \,\}$. Common examples include $\mathbb{R}^{\mathrm{n}} \coloneqq \underbrace{\mathbb{R} \times \mathbb{R} \ldots \times \mathbb{R}}_{\text{n times}}$ and $\mathbb{C}^{\mathrm{n}}$, which consists of n copies of complex numbers. In the latter case, the *real* dimensionality is $2n$.

**Example: The Direct Sum.**

Direct sums are similar to Cartesian products and in some cases are equivalent. Let us first define direct sums. Given *abelian groups* $(A, \circ)$, $(B, \star)$, the direct sum $A \oplus B$ consists of pairs $(a, b)$ such that group multiplication is respected. By this I mean that given pairs $(a_1, b_1)$ and $(a_2, b_2)$, then $(a_1, b_1) \oplus (a_2, b_2) = (a_1 \circ a_2, b_1 \star b_2)$. So $A \oplus B$ also constitutes an abelian group. One sees for example $\mathbb{R} \oplus \mathbb{R}$ is just $\mathbb{R}^2$. Likewise by extension one can easily show $(A \oplus B) \oplus C \simeq A \oplus (B \oplus C)$. These are examples of *external* direct sums. One can also define so-called *internal* direct sums by dividing a group into subgroups and treating the subgroups as distinct subspaces. This procedure can always be performed as every group $G$ possesses two trivial subgroups, namely $\{0\}$ and $G$ itself. For example, consider $(\mathbb{Z}_{10}, +)$. Take $A = (0, 2, 4, 6, 8)$ and $B = (0, 5)$. Writing $a \oplus b$ as simply $a + b$ (since subgroups are abelian here) one reproduces the entire group. For a finite abelian group $G$ one employs Lagrange's theorem to determine the orders of possible subgroups. Clearly if $|G|$ is prime, only trivial subgroups exist.

Another direct sum commonly found in physics is the Dirac bi-spinor describing particles such as electrons within a relativistic setting. There are two so-called Weyl spinor spaces denoted by $\left(\frac{1}{2}, 0\right)$ for "left-handed"' spinors and $\left(0, \frac{1}{2}\right)$ for the right-handed counterparts. An arbitrary Dirac bi-spinor is then an element of the space $\left(\frac{1}{2}, 0\right) \oplus \left(0, \frac{1}{2}\right)$.

**Example: Exterior Products.**

One method of forming new spaces from old involves creating so-called exterior products. For example, consider "differential forms" in $\mathbb{R}^3$: there are three "1-forms", namely the infinitesimal length elements $dx$, $dy$, and $dz$. There are likewise three "area elements" $dx\,dy$, $dy\,dz$, and $dx\,dz$ which we write as "wedge products" (exterior products) $dx \wedge dy$, $dy \wedge dz$, and $dz \wedge dx$, and a single "volume element" $dx\,dy\,dz$ expressed as $dx \wedge dy \wedge dz$. Exterior products are *anti-commutative*: thus $dx \wedge dy = -dy \wedge dx$, and so forth. From this we also see $dx \wedge dx = 0$, etc. We say exterior products obey the *Grassmann algebra*. Physicists will recognize the Grassmann algebra as that which vector cross-products obey.

*Modules.* In the above vector space axioms, nowhere was it actually necessary to demand $F$ be a field. After all, fields have rather tight constraints. If we relax these conditions and let $F$ just be a ring, we have another structure - the module. Modules are thus generalizations of vector spaces. Of course all vectors are modules (a vector space may be defined as a module over a field) but not all modules are vectors. Many of the axioms for vector spaces apply to modules as well, so I won't repeat them here. Nonetheless the formal definition is provided below.

**Definition Of A Module.**

Let $R$ be a ring with identity $1_R$. A *left R-module M* is an abelian group under addition that satisfies the following:

- For all $r, s \in R$ and all $x, y \in M$, $r(x + y) = rx + ry$.
- $(r + s) = rx + sx$.
- $(rs)x = r(sx)$.
- $1_R x = x$.

A right $R$-module is defined in a similar manner with $x$, $y$ being right-multiplied by 'scalars' $r$ and $s$. Examples of modules include vector spaces over a field, rings (viewed as a module over itself), Cartesian products of rings ($R^n$), polynomial rings over fields $F[x]$ , left ideals of rings, right ideals of rings, m x n matrices with ring elements as entries ($M_{m\times n}(R)$), as well abelian groups. In fact, every abelian group forms a $\mathbb{Z}$-module.

A module is *finitely generated* is there exists a finite number of basis elements ($x_1$, $x_2$ $\ldots x_n$) in $M$ such that all module elements can be expressed as a linear combination of those bases with coefficients in $R$. If the module $M$ can be generated from a single element then it is said to be *cyclic*. Examples of cyclic modules include $n\,\mathbb{Z}$, cyclic groups, principal ideals of rings, etc. A *free module* is one that has a basis. For example, $R^n$ is a free module. Unlike finitely-generated modules, the basis of a free module needn't be finite. To distinguish free modules from finitely-generated ones, consider the module $M = \mathbb{Z}$ x $(\mathbb{Z}/7\,\mathbb{Z})$ x $8\,\mathbb{Z}$. This is a finitely-generated module that is definitely not free.

A *sub-module* is a subgroup of a module $M$. For example, $5\,\mathbb{Z}$ is a $\mathbb{Z}$-module. Sub-modules include $10\,\mathbb{Z}$, $15\,\mathbb{Z}$, $20\,\mathbb{Z}$, etc. As you can see $5\,\mathbb{Z}$ in fact has a countably-infinite number of sub-modules.

**Dimension = 1**. In one dimension we have the real numbers $\mathbb{R}$, which comprises the field over which all other number systems are defined.

**Dimension = 2**. In two dimensions we have a basis set $\{\,1,\,\mathbf{e}\,\}$ and any element may be expressed as $a + b\mathbf{e}$. As an aside, I note the most "natural" framework to discuss at least some of what follows is Clifford algebra, whence I will include a brief discussion on Clifford algebras in an appendix. We distinguish three possibilities:

$$a + b\mathbf{e} = \begin{cases} \text{complex numbers if } \mathbf{e}^2 = -1, \\ \text{split} - \text{complex numbers if } \mathbf{e}^2 = 1, \\ \text{dual complex numbers if } \mathbf{e}^2 = 0. \end{cases}$$

For complex numbers, $\mathbf{e}$ is typically denoted by physicists and mathematicians as $i$ and as $j$ by engineers. For split-complex numbers, also known as *Study numbers*, $\mathbf{e}$ is commonly denoted by the letter $j$ . Dual complex numbers

or simply *dual numbers* have a nilpotent imaginary element. Of the three, only the complex numbers form a division algebra as $(1+j)(1-j) = 0$ and dual numbers of the form $0 + a\mathbf{e}$ possess no inverse.

**Dimension = 4**. The four-dimensional basis set is given by $\{ 1, \mathbf{i}, \mathbf{j}, \mathbf{k} \}$. Hence an arbitrary element may be written as $q = a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}$, where $a_n \in \mathbb{R},\ n = 0, 1, 2, 3$. Again there are several possibilities:

$$a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k} = \begin{cases} \text{quaternions if } \mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1, \\ \text{split} - \text{quaternions (coquaternions) if } \mathbf{i}^2 = -1,\ \mathbf{j}^2 = \mathbf{k}^2 = 1, \\ \text{hyperbolic quaternions if } \mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = 1, \\ \text{complex quaternions (\textit{biquaternions}) if } a_n \text{ are complex numbers}, \\ \text{dual quaternions if } a_n \text{ are dual numbers}, \\ \text{bicomplex numbers or \textit{tessarines} if } \mathbf{j}^2 = 1,\ \mathbf{ij} = \mathbf{ji} = \mathbf{k}, \\ \text{split} - \text{biquaternions if } a_n \text{ are Study numbers}. \end{cases}$$

Admittedly that is a lot of information and one might well find it overwhelming. To simplify matters, multiplication tables are provided below.

| x | 1 | i | j | k |
|---|---|---|---|---|
| 1 | 1 | i | j | k |
| i | i | -1 | k | -j |
| j | j | -k | -1 | i |
| k | k | j | -i | -1 |

TABLE III: Multiplication Table For Quaternions

| x | 1 | i | j | k |
|---|---|---|---|---|
| 1 | 1 | i | j | k |
| i | i | -1 | k | -j |
| j | j | -k | 1 | -i |
| k | k | j | i | 1 |

TABLE IV: Multiplication Table For Split-Quaternions

| x | 1 | i | j | k |
|---|---|---|---|---|
| 1 | 1 | i | j | k |
| i | i | 1 | k | -j |
| j | j | -k | 1 | i |
| k | k | j | -i | 1 |

TABLE V: Multiplication Table For Hyperbolic Quaternions

Let us briefly pause to review some of the properties of the three above quaternion-based systems. First, all three systems preserve anti-commutativity, thus

$$ij = -ji,\ ik = -ki,\ jk = -kj$$

holds in all three systems. Regular quaternions and split-quaternions are likewise associative, whence $(ij)k = i(jk)$, etc. However hyperbolic quaternions are non-associative. For example, $(ii)j = j$ since $ii = i^2 = 1$. On the other hand $i(ij) = ik = -j$. Furthermore neither split- nor hyperbolic- quaternions constitute a division algebra. For example, $(1 + j)(1 - j) = (i + j)(i - j) = (i - j)^2 = 0$ in both the split and hyperbolic quaternions. Such non-divisibility is to be expected since some (all) non-unital (i.e., $\neq 1$) base elements in split (hyperbolic) quaternions behave as Study numbers.

Let us next consider the complex quaternions, also known as *biquaternions*. The multiplication rules governing quaternionic base elements $\{ 1, \mathbf{i}, \mathbf{j}, \mathbf{k} \}$ are the same as regular quaternions but coefficients are now permitted to be complex. This immediately causes us to distinguish the regular complex $i$ from the quaternionic $\mathbf{i}$, which is why I used boldface for quaternionic elements. Complex $i$ is treated exactly like a real number in that it commutes with any quaternionic element and the biquaterternions as a whole may be expressed $\mathbb{H} \oplus i\mathbb{H}$ or as the module tensor product $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{H}$ where the $\otimes_{\mathbb{R}}$ symbol means the product is taken over the reals. Biquaternions may be thought of as a four-dimensional algebra over $\mathbb{C}$ or an eight-dimensional algebra over $\mathbb{R}$. It is not a division algebra since $1+i\mathbf{i})(1-i\mathbf{i})$ $= 0$.

Dual quaternions may be expressed as $\mathbb{D} \otimes \mathbb{H}$, where of course $\mathbb{D}$ is the set of all dual numbers viz,

$$\mathbb{D} = \{\, a + b\,\epsilon \,|\, a, b \in \mathbb{R},\ \epsilon^2 = 0. \,\}$$

As before, one employs regular quaternion multiplication with $\epsilon$ commuting with all quaternionic elements. When multiplying, any term involving $\epsilon^2$ will be zero. Like biquaternions, dual quaternions form an eight-dimensional algebra over the reals, and of course dual quaternions aren't a division algebra due to the nilpotency of $\epsilon$.

Tessarines were invented by James Cockle in 1848 and form a four-dimensional associative algebra over the reals or equivalently a two-dimensional algebra over $\mathbb{C}$. Thus tessarines possess the structure $\mathbb{C} \oplus \mathbb{C}$. Unlike quaternions tessarines are commutative, obeying the rules

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

The tessarine multiplication table is presented below.

| x | 1 | i | j | k |
|---|---|---|---|---|
| 1 | 1 | i | j | k |
| i | i | -1 | k | -j |
| j | j | k | 1 | i |
| k | k | -j | i | -1 |

TABLE VI: Multiplication Table For Tessarines

Split-biquaternions obey the usual quaternion multiplication with coefficients being Study numbers. Naturally Study numbers commute with quaternionic terms giving us an eight-dimensional associative algebra over the reals, but not a division algebra as Study numbers do not form a division ring. We may express split-biquaternions as the set $\mathbb{H} \oplus j\,\mathbb{H}$ where $j^2 = 1$.

I would be remiss if I didn't include one more number system here, the Grassmann algebra. Grassmann algebras obey the usual quaternion multiplication but with $i^2 = j^2 = k^2 = 0$. Thus Grassmann algebra is truly anti-commutative and non-associative. As previously mentioned, physics students are in fact already familiar with Grassmann algebra in the form of vector cross-products. Grassmann algebras arise in physics not only as cross products , but also as the previously noted *differential forms* and *Weyl spinors*. Its multiplication table in the current context is lovingly presented below.

| x | 1 | i | j | k |
|---|---|---|---|---|
| 1 | 1 | i | j | k |
| i | i | 0 | k | -j |
| j | j | -k | 0 | i |
| k | k | j | -i | 0 |

TABLE VII: Multiplication Table For A Grassmann Algebra

The Grassmann structure of cross-products is immediately obvious: $\hat{i} \times \hat{i} = 0$, $\hat{i} \times \hat{j} = -\hat{j} \times \hat{i} = \hat{k}$, etc.