Course 2BA1: Hilary Term 2003
Section 4: Abstract Algebra

David R. Wilkins

Contents

4 Abstract Algebra

4.1 Binary Operations on Sets

Definition A *binary operation* $*$ on a set A is an operation which, when applied to any elements x and y of the set A, yields an element $x * y$ of A.

Example The arithmetic operations of addition, subtraction and multiplication are binary operations on the set $\mathbb{R}$ of real numbers which, when applied to real numbers x and y, yield the real numbers $x + y$, $x - y$ and xy respectively.

However division is not a binary operation on the set of real numbers, since the quotient x/y is not defined when $y = 0$. (Under a binary operation $*$ on a set must determine an element $x * y$ of the set for every pair of elements x and y of that set.)

4.2 Commutative Binary Operations

Definition A binary operation $*$ on a set A is said to be *commutative* if $x * y = y * x$ for all elements x and y of A.

Example The operations of addition and multiplication on the set $\mathbb{R}$ of real numbers are commutative, since $x + y = y + x$ and $x \times y = y \times x$ for all real numbers x and y. However the operation of subtraction is not commutative, since $x - y \neq y - x$ in general. (Indeed the identity $x - y = y - x$ holds only when $x = y$.)

4.3 Associative Binary Operations

Let $*$ be a binary operation on a set A. Given any three elements x, y and z of a set A, the binary operation, applied to the elements $x * y$ and z of A, yields an element $(x * y) * z$ of A, and, applied to the elements x and $y * z$ of A, yields an element $x * (y * z)$ of A.

Definition A binary operation $*$ on a set A is said to be *associative* if $(x * y) * z = x * (y * z)$ for all elements x, y and z of A.

Example The operations of addition and multiplication on the set $\mathbb{R}$ of real numbers are associative, since $(x + y) + z = x + (y + z)$ and $(x \times y) \times z = x \times (y \times z)$ for all real numbers x, y and z. However the operation of subtraction is not associative. For example $(1 - 2) - 3 = -4$, but $1 - (2 - 3) = 2$.

When a binary operation $*$ is associative it is not necessary to retain the parentheses in expressions such as $(x * y) * z$ or $x * (y * z)$. These two expressions may both be written without ambiguity as $x * y * z$.

4.4 Semigroups

Definition A *semigroup* consists of a set on which is defined an associative binary operation.

We may denote by $(A, *)$ a semigroup consisting of a set A together with an associative binary operation $*$ on A.

Definition A semigroup $(A, *)$ is said to be *commutative* (or *Abelian*) if the binary operation $*$ is commutative.

Example The set of natural numbers, with the operation of addition, is a commutative semigroup, as is the set of natural numbers with the operation of multiplication.

Let $(A, *)$ be a semigroup. Given any element a of A, we define

$$\begin{aligned} a^1 &= a, \\ a^2 &= a * a, \\ a^3 &= a * a^2 = a * (a * a), \\ a^4 &= a * a^3 = a * (a * (a * a)), \\ a^5 &= a * a^4 = a * (a * (a * (a * a))), \\ &\vdots \end{aligned}$$

In general we define a^n recursively for all natural numbers n so that $a^1 = a$ and $a^n = a * a^{n-1}$ whenever $n > 1$.

Remark In the case of the semigroup consisting of the set of natural numbers with the operation of multiplication, the value of 'a^n' given by the above rule is the nth power of a natural number a. However in the case of the semigroup consisting of the set of natural numbers with the operation of addition it is not the nth power of a, but is na.

Theorem 4.1 *Let $(A, *)$ be a semigroup, and let a be an element of A. Then $a^m * a^n = a^{m+n}$ for all natural numbers m and n.*

Proof We prove this theorem by induction on m.

Now it follows immediately from the definition of a^{n+1} that $a * a^n = a^{1+n}$ for all natural numbers n. Thus the theorem is true in the case when $m = 1$.

Suppose that the required result is true in the case when $m = s$ for some natural number s, so that $a^s * a^n = a^{s+n}$ for all natural numbers n. Then

$$a^{s+1} * a^n = (a * a^s) * a^n = a * (a^s * a^n) = a * a^{s+n} = a^{s+1+n}$$

for all natural numbers n. Thus if the required result is true when $m = s$ then it is also true when $m = s + 1$. We conclude using the Principle of Mathematical Induction that the identity $a^m * a^n = a^{m+n}$ holds for all natural numbers m and n, as required. ∎

Theorem 4.2 *Let $(A, *)$ be a semigroup, and let a be an element of A. Then $(a^m)^n = a^{mn}$ for all natural numbers m and n.*

Proof The result may be proved by induction on the natural number n. The identity $(a^m)^n = a^{mn}$ clearly holds whenever $n = 1$. Suppose that s is a natural number with the property that $(a^m)^s = a^{ms}$ for all natural numbers m. Then

$$(a^m)^{s+1} = (a^m)^s * a^m = a^{ms} * a^m = a^{ms+m} = a^{m(s+1)}.$$

Thus if the identity $(a^m)^n = a^{mn}$ holds when $n = s$ then it also holds when $n = s + 1$. We conclude from the Principle of Mathematical Induction that this identity holds for all natural numbers n.

Remark Note that the above proof made use of the fact that the binary operation on a semigroup is associative.

4.5 The General Associative Law

Let $(A, *)$ be a semigroup, and let x, y, z and w be elements of A. We can use the associative property of $*$ to show that the value of a product involving x, y, z, w is independent of the manner in which that product is bracketed, though it generally depends on the order in which x, y, z and w occur in that product (unless that binary operation is also commutative). For example,

$$\begin{aligned}(x * (y * z)) * w &= ((x * y) * z) * w \\ &= (x * y) * (z * w) \\ &= x * (y * (z * w)) \\ &= x * ((y * z) * w)\end{aligned}$$

All the above products may therefore be denoted without ambiguity by the expression $x * y * z * w$ from which the parentheses have been dropped.

The analogous property holds for products involving five or more elements of the semigroup.

In any semigroup, the value of a product of three or more elements of the semigroup depends in general on the order in which those elements occur in the product (unless the binary operation is commutative), but the value of the product is independent of the manner in which the product is bracketed. This general result is often referred to as the General Associative Law, and can be proved using induction on the number of elements that occur in the product.

4.6 Identity elements

Definition Let $(A, *)$ be a semigroup. An element e of A is said to be an *identity element* for the binary operation $*$ if $e*x = x*e = x$ for all elements x of A.

Example The number 1 is an identity element for the operation of multiplication on the set $\mathbb{N}$ of natural numbers.

Example The number 0 is an identity element for the operation of addition on the set $\mathbb{Z}$ of integers.

Theorem 4.3 *A binary operation on a set cannot have more than one identity element.*

Proof Let e and f be identity elements for a binary operation $*$ on a set A. Then $e = e*f = f$. Thus there cannot be more than one identity element. ∎

4.7 Monoids

Definition A *monoid* consists of a set on which is defined an associative binary operation with an identity element.

We see immediately from the above definition that a semigroup is a monoid if and only if it has an identity element.

Definition A monoid $(A, *)$ is said to be *commutative* (or *Abelian*) if the binary operation $*$ is commutative.

Example The set $\mathbb{N}$ of natural numbers with the operation of multiplication is a commutative monoid. Indeed the operation of multiplication is both commutative and associative, and the identity element is the natural number 1.

Example The set $\mathbb{N}$ of natural numbers with the operation of addition is not a monoid, since there is no identity element for the operation of addition that belongs to the set of natural numbers.

Let a be an element of a monoid $(A, *)$. We define $a^0 = e$, where e is the identity element.

Theorem 4.4 *Let $(A, *)$ be a monoid, and let a be an element of A. Then $a^m * a^n = a^{m+n}$ for all non-negative integers m and n.*

Proof Any monoid is a semigroup. It therefore follows from Theorem 4.1 that $a^m * a^n = a^{m+n}$ when $m > 0$ and $n > 0$. It also follows directly from the definition of the identity element that the result is also true if $m = 0$ or if $n = 0$. ∎

Theorem 4.5 *Let $(A, *)$ be a monoid, and let a be an element of A. Then $(a^m)^n = a^{mn}$ for all non-negative integers m and n.*

Proof It follows directly from Theorem 4.2 that $(a^m)^n = a^{mn}$ whenever m and n are both positive. But this identity holds also when m or n is zero, since both sides of the identity are then equal to the identity element of the monoid. ∎

4.8 Inverses

Definition Let $(A, *)$ be a monoid with identity element e, and let x be an element of A. An element y of A is said to be the *inverse* of x if $x * y = y * x = e$. An element x of A is said to be *invertible* if there exists an element of A which is an inverse of x.

Theorem 4.6 *An element of a monoid can have at most one inverse.*

Proof Let $(A, *)$ be a monoid with identity element e, and let x, y and z be elements of A. Suppose that $x * y = y * x = e$ and $x * z = z * x = e$. Then

$$y = y * e = y * (x * z) = (y * x) * z = e * z = z,$$

and thus $y = z$. Thus an element of a monoid cannot have more than one inverse. ∎

Remark The above proof shows in fact that if x is an element of a monoid $(A, *)$, and if y and z are elements of A satisfying $y * x = x * z = e$, where e is the identity element of the monoid, then $y = z$.

Let $(A, *)$ be a monoid, and let x be an invertible element of A. We shall denote the inverse of x by x^{-1}. (This inverse element x^{-1} is uniquely determined by x, by Theorem 4.6.)

Theorem 4.7 *Let $(A, *)$ be a monoid, and let x and y be invertible elements of A. Then $x * y$ is also invertible, and $(x * y)^{-1} = y^{-1} * x^{-1}$.*

Proof Let e denote the identity element of the monoid. Then $x * x^{-1} = x^{-1} * x = e$ and $y * y^{-1} = y^{-1} * y = e$, and therefore

$$\begin{aligned}(x * y) * (y^{-1} * x^{-1}) &= ((x * y) * y^{-1}) * x^{-1} = (x * (y * y^{-1})) * x^{-1} \\ &= (x * e) * x^{-1} = x * x^{-1} = e, \\ (y^{-1} * x^{-1}) * (x * y) &= y^{-1} * (x^{-1} * (x * y)) = y^{-1} * ((x^{-1} * x) * y) \\ &= y^{-1} * (e * y) = y^{-1} * y = e.\end{aligned}$$

and thus the element $y^{-1} * x^{-1}$ has the properties required of an inverse of the element $x * y$. We conclude that $x * y$ is indeed invertible, and $(x * y)^{-1} = y^{-1} * x^{-1}$. ∎

Theorem 4.8 *Let $(A, *)$ be a monoid, let a and b be elements of A, and let x be an invertible element of A. Then $a = b * x$ if and only if $b = a * x^{-1}$. Similarly $a = x * b$ if and only if $b = x^{-1} * a$.*

Proof Let e denote the identity element of the monoid. Suppose that $a = b * x$. Then

$$a * x^{-1} = (b * x) * x^{-1} = b * (x * x^{-1}) = b * e = b.$$

Conversely, if $b = a * x^{-1}$, then

$$b * x = (a * x^{-1}) * x = a * (x^{-1} * x) = a * e = a.$$

Similarly if $a = x * b$ then

$$x^{-1} * a = x^{-1} * (x * b) = (x^{-1} * x) * b = e * b = b,$$

and, conversely, if $b = x^{-1} * a$ then

$$x * b = x * (x^{-1} * a) = (x * x^{-1}) * a = e * a = a. \quad ∎$$

Let $(A, *)$ be a monoid, and let a be an invertible element of A. We extend the definition of a^n to negative integers n by defining a^n to be the inverse $(a^q)^{-1}$ of a^q whenever $q > 0$ and $n = -q$.

Theorem 4.9 *Let $(A, *)$ be a monoid, and let a be an invertible element of A. Then $a^m * a^n = a^{m+n}$ for all integers m and n.*

Proof The proof breaks down into a case-by-case analysis, depending on the signs of the integers m and n.

The appropriate definitions ensure that the identity $a^m * a^n = a^{m+n}$ holds if $m = 0$ or if $n = 0$.

The result has already been verified if both m and n are positive (see Theorem 4.1 and Theorem 4.4).

Suppose that m and n are both negative. Then $a^m = (a^{-m})^{-1}$, $a^n = (a^{-n})^{-1}$ and $a^{m+n} = (a^{-(m+n)})^{-1}$. Now $a^{-n} * a^{-m} = a^{-n-m} = a^{-(m+n)}$. It follows from Theorem 4.7 that

$$a^{m+n} = (a^{-(m+n)})^{-1} = (a^{-n} * a^{-m})^{-1} = (a^{-m})^{-1} * (a^{-n})^{-1} = a^m * a^n.$$

The only remaining cases to consider are those when m and n have different signs.

Let p and q be non-negative integers. Now $a^{p+q} = a^p * a^q = a^q * a^p$. It follows from Theorem 4.8 that

$$a^p = a^{p+q} * a^{-q} = a^{-q} * a^{p+q}, \quad a^q = a^{p+q} * a^{-p} = a^{-p} * a^{p+q},$$

and hence

$$a^{-p} = a^q * a^{-(p+q)} = a^{-(p+q)} * a^q, \quad a^{-q} = a^p * a^{-(p+q)} = a^{-(p+q)} * a^p.$$

Suppose that $m < 0$, $n > 0$ and $m + n \geq 0$. On setting $p = -m$ and $q = m + n$ we see that $a^{m+n} = a^q = a^{-p} * a^{p+q} = a^m * a^n$. Next suppose that $m < 0$, $n > 0$ and $m + n < 0$. On setting $p = -m - n$ and $q = n$ we see that $a^{m+n} = a^{-p} = a^{-(p+q)} * a^q = a^m * a^n$. Next suppose that $m > 0$, $n < 0$ and $m + n \geq 0$. On setting $p = m + n$ and $q = -n$ we see that $a^{m+n} = a^p = a^{p+q} * a^{-q} = a^m * a^n$. Finally suppose that $m > 0$, $n < 0$ and $m + n < 0$. On setting $p = m$ and $q = -m - n$ we see that $a^{m+n} = a^{-q} = a^p * a^{-(p+q)} = a^m * a^n$. The result has now been verified for all integers m and n, as required. ∎

Theorem 4.10 *Let $(A, *)$ be a monoid, and let a be an invertible element of A. Then $(a^m)^n = a^{mn}$ for all integers m and n.*

Proof Let m be an integer. First we prove by induction on n that $(a^m)^n = a^{mn}$ for all positive integers n. The result clearly holds when $n = 1$. Suppose $(a^m)^s = a^{ms}$ for some positive integer s. It then follows from Theorem 4.9 that

$$(a^m)^{s+1} = (a^m)^s * a^m = a^{ms} * a^m = a^{m(s+1)}.$$

It follows from the Principle of Mathematical Induction that $(a^m)^n = a^{mn}$ for all positive integers n. The result is also true when $n = 0$, since both sides of the identity are then equal to the identity element of the monoid.

Finally suppose that n is a negative integer. Then $n = -q$ for some positive integer q, and $(a^m)^q = a^{mq}$. On taking the inverses of both sides of this identity, we find that

$$(a^m)^n = ((a^m)^q)^{-1} = (a^{mq})^{-1} = a^{-mq} = a^{mn},$$

as required. We can now conclude that the identity $(a^m)^n = a^{mn}$ holds for all integers m and n. ∎

4.9 Groups

Definition A *group* consists of a set A together with a binary operation $*$ on A with the following properties:—

(i) $x * (y * z) = (x * y) * z$ for all elements x, y and z of A (i.e., the operation $*$ is associative);

(ii) there exists an element e of A with the property that $e * x = x * e = x$ for all elements x of A (i.e., there exists an identity element e for the binary operation $*$ on A);

(iii) given any element x of A, there exists an element y of A satisfying $x * y = y * x = e$ (i.e., every element of A is invertible).

We see immediately from this definition that a *group* can be characterized as a monoid in which every element is invertible.

Definition A group $(A, *)$ is said to be *commutative* (or *Abelian*) if the binary operation $*$ is commutative.

Example The set of integers with the operation of addition is a commutative group.

Example The set of real numbers with the operation of addition is a commutative group.

Example The set of non-zero real numbers with the operation of multiplication is a commutative group.

Example The set of integers with the operation of multiplication is not a group, since not every element is invertible. Indeed the only integers that are invertible are $+1$ and -1.

Example Let n be a natural number, and let

$$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}.$$

Any integer k may be expressed uniquely in the form $k = qn + r$ for some integers q and r with $0 \leq r < n$. (When k is positive, q and r are the quotient and remainder respectively, when k is divided by n in integer arithmetic.) Then r is the unique element of $\mathbb{Z}_n$ for which $k - r$ is divisible by n. In particular, given any elements x and y of $\mathbb{Z}_n$, there exist unique elements s and p of $\mathbb{Z}_n$ such that $x + y - s$ and $xy - p$ are divisible by n. We define $x \oplus_n y = s$ and $x \otimes_n y = p$. Then $\oplus_n$ and $\otimes_n$ are binary operations on the set $\mathbb{Z}_n$.

We show that the binary operation $\oplus_n$ is associative. Let x, y and z be integers belonging to $\mathbb{Z}_n$, and let $u = x \oplus_n y$ and $v = y \oplus_n z$. Then $x + y - u$ and $y + z - v$ are both divisible by n. Now

$$(u + z) - (x + v) = (y + z - v) - (x + y - u).$$

It follows that $(u + z) - (x + v)$ is divisible by n, and hence $u \oplus_n z = x \oplus_n v$. Thus $(x \oplus_n y) \oplus_n z = x \oplus_n (y \oplus_n z)$.

We also show that the binary operation $\otimes_n$ is associative. Let x, y and z be integers belonging to $\mathbb{Z}_n$, and let $p = x \otimes_n y$ and $q = y \otimes_n z$. Then $xy - p$ and $yz - q$ are both divisible by n. Now

$$pz - xq = x(yz - q) - (xy - p)z.$$

It follows that $pz - xq$ is divisible by n, and hence $p \otimes_n z = x \otimes_n q$. Thus $(x \otimes_n y) \otimes_n z = x \otimes_n (y \otimes_n z)$.

Now $0 \oplus_n x = x \oplus_n 0 = x$ and $1 \otimes_n x = x \otimes_n 1 = x$ for all $x \in \mathbb{Z}_n$. It follows that $(\mathbb{Z}_n, \oplus_n)$ is a monoid with identity element 0, and $(\mathbb{Z}_n, \otimes_n)$ is a monoid with identity element 1.

Every element x of the monoid $(\mathbb{Z}_n, \oplus_n)$ is invertible: the inverse of x is $n - x$ if $x \neq 0$, and is 0 if $x = 0$. Thus $(\mathbb{Z}_n, \oplus_n)$ is a group.

However $(\mathbb{Z}_n, \otimes_n)$ is not a group if $n > 1$. Indeed 0 is not an invertible element, since $0 \otimes_n x = 0$ for all elements x of $\mathbb{Z}_n$, and therefore there cannot exist any element x of $\mathbb{Z}_n$ for which $0 \otimes_n x = 1$.

It can be shown that an element x of $(\mathbb{Z}_n, \otimes_n)$ is invertible in this monoid if and only if the highest common factor of x and n is equal to 1. It follows from this that the non-zero elements of $\mathbb{Z}_n$ constitute a group under $\otimes_n$ if and only if the natural number n is a prime number.

Let us consider the particular case when $n = 9$. The 'multiplication table' for the monoid $(\mathbb{Z}_9, \otimes_9)$ is the following:—

$\otimes_9$	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	4	6	8	1	3	5	7
3	0	3	6	0	3	6	0	3	6
4	0	4	8	3	7	2	6	1	5
5	0	5	1	6	2	7	3	8	4
6	0	6	3	0	6	3	0	6	3
7	0	7	5	3	1	8	6	4	2
8	0	8	7	6	5	4	3	2	1

From this table we see that the invertible elements are 1, 2, 4, 5, 7 and 8. Indeed $1 \otimes_9 1 = 1$, $2 \otimes_9 5 = 1$, $4 \otimes_9 7 = 1$, $8 \otimes_9 8 = 1$.

4.10 Homomorphisms and Isomorphisms

Definition Let $(A, *)$ and $(B, *)$ be semigroups, monoids or groups. A function $f\colon A \to B$ from A to B is said to be a *homomorphism* if $f(x * y) = f(x) * f(y)$ for all elements x and y of A.

Example Let q be an integer, and let $f\colon \mathbb{Z} \to \mathbb{Z}$ be a the function from the set of integers to itself defined by $f(n) = qn$ for all integers n. Then f is a homomorphism from the group $(\mathbb{Z}, +)$ to itself, since

$$f(m + n) = q(m + n) = qm + qn = f(m) + f(n)$$

for all integers m and n.

Example Let $\mathbb{R}^*$ denote the set of non-zero real numbers, let a be a non-zero real number, and let $f\colon \mathbb{Z} \to \mathbb{R}^*$ be the function defined by $f(n) = a^n$ for all integers m and n. Then $f\colon \mathbb{Z} \to \mathbb{R}^*$ is a homomorphism from the group $(\mathbb{Z}, +)$ of integers under addition to the group $(\mathbb{R}^*, \times)$ of non-zero real numbers under multiplication, since

$$f(m + n) = a^{m+n} = a^m a^n = f(m)f(n)$$

for all integers m and n.

Example This last example can be generalized. Let a be an invertible element of a monoid $(A, *)$, and let $f\colon \mathbb{Z} \to A$ be the function from $\mathbb{Z}$ to A defined by $f(n) = a^n$. Then this function is a homomorphism from the group $(\mathbb{Z}, +)$ of integers under addition to the monoid $(A, *)$ since it follows from Theorem 4.9 that

$$f(m + n) = a^{m+n} = a^m * a^n = f(m) * f(n)$$

for all integers m and n.

We recall that a function $f: A \to B$ is said to be *injective* if distinct elements of A get mapped to distinct elements of B (i.e., if x and y are elements of A and if $x \neq y$ then $f(x) \neq f(y)$). Also a function $f: A \to B$ is said to be *surjective* if each element of B is the image $f(a)$ of at least one element a of A. A function $f: A \to B$ is said to be *bijective* if it is both injective and surjective. One can prove that a function $f: A \to B$ has a well-defined inverse $f^{-1}: B \to A$ if and only if it is bijective.

Definition Let $(A, *)$ and $(B, *)$ be semigroups, monoids or groups. A function $f: A \to B$ from A to B is said to be an *isomorphism* if it is both a homomorphism and a bijective function.

Theorem 4.11 *Let $(A, *)$ and $(B, *)$ be semigroups, monoids or groups. Then the inverse $f^{-1}: B \to A$ of any isomorphism $f: A \to B$ is itself an isomorphism.*

Proof The inverse $f^{-1}: B \to A$ of an isomorphism $f: A \to B$ is itself a bijective function whose inverse is the function $f: A \to B$. It remains to show that $f^{-1}: B \to A$ is a homomorphism. Let u and v be elements of B, and let $x = f^{-1}(u)$ and $y = f^{-1}(v)$. Then $u = f(x)$ and $v = f(y)$, and therefore

$$f(x * y) = f(x) * f(y) = u * v$$

and therefore

$$f^{-1}(u * v) = x * y = f^{-1}(u) * f^{-1}(v),$$

showing that the function $f^{-1}: B \to A$ is a homomorphism from $(B, *)$ to $(A, *)$, as required. ∎

Definition Let $(A, *)$ and $(B, *)$ be semigroups, monoids or groups. If there exists an isomorphism from $(A, *)$ to $(B, *)$ then $(A, *)$ and $(B, *)$ are said to be *isomorphic*.

4.11 Quaternions

A *quaternion* may be defined to be an expression of the form $w + xi + yj + zk$, where w, x, y and z are real numbers. There are operations of addition, subtraction and multiplication defined on the set $\mathbb{H}$ of quaternions. These are binary operations on that set.

Quaternions were introduced into mathematics in 1843 by William Rowan Hamilton (1805–1865).

The definitions of addition and subtraction are straightforward. The *sum* and *difference* of two quaternions $w + xi + yj + zk$ and $w' + x'i + y'j + z'k$ are given by the formulae

$$\begin{aligned}
&(w + xi + yj + zk) + (w' + x'i + y'j + z'k) \\
&\qquad = (w + w') + (x + x')i + (y + y')j + (z + z')k; \\
&(w + xi + yj + zk) - (w' + x'i + y'j + z'k) \\
&\qquad = (w - w') + (x - x')i + (y - y')j + (z - z')k.
\end{aligned}$$

If the quaternions $w + xi + yj + zk$ and $w' + x'i + y'j + z'k$ are denoted by q and q' respectively, then we may denote the sum and the difference of these quaternions by $q + q'$ and $q - q'$.

These operations of addition and subtraction of quaternions are binary operations on the set $\mathbb{H}$ of quaternions. It is easy to see that the operation of addition is commutative and associative, and that the *zero quaternion* $0 + 0i + 0j + 0k$ is an identity element for the operation of addition. In particular the quaternions constitute a monoid under the operation of addition.

The operation of subtraction of quaternions is neither commutative nor associative. This results directly from the fact that the operation of subtraction on the set of real numbers is neither commutative nor associative.

Let q be a quaternion. Then $q = w + xi + yj + zk$ for some real numbers w, x, y and z, and there is a corresponding quaternion $-q$, with $-q = (-w) + (-x)i + (-y)j + (-z)k$. Then $q + (-q) = (-q) + q = 0$, where 0 here denotes the zero quaternion $0 + 0i + 0j + 0k$. Thus, in the monoid $(\mathbb{H}, +)$ every quaternion is invertible. It follows that the quaternions constitute a group $(\mathbb{H}, +)$, the binary operation on this group being the operation of addition of quaternions.

The definition of quaternion multiplication is somewhat more complicated than the definitions of addition and subtraction. The *product* of two quaternions $w + xi + yj + zk$ and $w' + x'i + y'j + z'k$ is given by the formula

$$\begin{aligned}
&(w + xi + yj + zk) \times (w' + x'i + y'j + z'k) \\
&\qquad = (ww' - xx' - yy' - zz') + (wx' + xw' + yz' - zy')i \\
&\qquad\quad + (wy' + yw' + zx' - xz')j + (wz' + zw' + xy' - yx')k.
\end{aligned}$$

We shall often denote the product $q \times q'$ of quaternions q and q' by qq'.

Given any real number w, let us denote the quaternion $w + 0i + 0j + 0k$ by w itself. Let us also denote the quaternions $0 + 1i + 0j + 0k$, $0 + 0i + 1j + 0k$ and $0 + 0i + 0j + 1k$ by i, j and k respectively. It follows directly from the above formula defining multiplication of quaternions that

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

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

where $i^2 = i \times i$, $ij = i \times j$ etc. It follows directly from these identities that

$$ijk = -1,$$

where $ijk = i \times (j \times k) = (i \times j) \times k$.

Let q be a quaternion, given by the expression $w + xi + yj + zk$, where w, x, y and z are real numbers. One can easily verify that the quaternion q can be formed from the seven quaternions w, x, y, z, i, j and k according to the formula

$$q = w + (x \times i) + (y \times j) + (z \times k).$$

The operation of multiplication on the set $\mathbb{H}$ of quaternions is not commutative. Indeed $i \times j = k$, but $j \times i = -k$.

One can however verify by a straightforward but somewhat tedious calculation that this operation of multiplication of quaternions is associative. Moreover the quaternion $1 + 0i + 0j + 0k$ is an identity element for this operation of multiplication. It follows therefore that the quaternions form a monoid under multiplication.

A quaternion $w + xi + yj + zk$ is said to be *real* if $x = y = z = 0$. Such a quaternion may be identified with the real number w. In this way the set of real numbers may be regarded as a subset of the set of quaternions.

Although quaternion multiplication is not commutative, one can readily show that $a \times q = q \times a$ for all real numbers a and for all quaternions q. Indeed if $q = w + xi + yj + zk$, where w, x, y and z are real numbers, then the rules of quaternion multiplication ensure that

$$a \times q = q \times a = (aw) + (ax)i + (ay)j + (az)k.$$

Let q be a quaternion. Then $q = w + xi + yj + zk$ for some real numbers w, x, y and z. We define the *conjugate* $\overline{q}$ of q to be the quaternion $\overline{q} = w - xi - yj - zk$. The definition of quaternion multiplication may then be used to show that

$$q \times \overline{q} = \overline{q} \times q = w^2 + x^2 + y^2 + z^2.$$

We define the *modulus* $|q|$ of the quaternion q by the formula

$$|q| = \sqrt{w^2 + x^2 + y^2 + z^2}.$$

Then $q\overline{q} = \overline{q}q = |q|^2$ for all quaternions q. Moreover $|q| = 0$ if and only if $q = 0$.

If q and r are quaternions, and if $\overline{q}$ and $\overline{r}$ denote the conjugates of q and r respectively, then the conjugate $\overline{q \times r}$ of the product $q \times r$ is given by the formula $\overline{q \times r} = \overline{r} \times \overline{q}$.

If q is a non-zero quaternion, and if the quaternion q^{-1} is defined by the formula $q^{-1} = |q|^{-2}\overline{q}$, then $qq^{-1} = q^{-1}q = 1$. We conclude therefore that every non-zero quaternion is invertible in the monoid $(\mathbb{H}, \times)$.

It follows directly from this that the non-zero quaternions constitute a group with respect to the operation of multiplication.

4.12 Quaternions and Vectors

Let q be a quaternion. We can write

$$q = q_0 + q_1 i + q_2 j + q_3 k,$$

where q_0, q_1, q_2 and q_3 are real numbers. We can then write

$$q = q_0 + \vec{q}$$

where

$$\vec{q} = q_1 i + q_2 j + q_3 k.$$

Following Hamilton, we can refer to q_0 as the *scalar part* of the quaternion q, and we can refer to $\vec{q}$ as the *vector part* of the quaternion q. Moreover $\vec{q}$ may be identified with the vector (q_1, q_2, q_3) in three-dimensional space whose components (with respect to some fixed orthonormal basis) are q_1, q_2 and q_3. Thus a quaternion may be regarded as, in some sense, a formal sum of a scalar and a vector.

In particular, we can regard vectors as a special type of quaternion: a quaternion $q_0 + q_1 i + q_2 j + q_3 k$ represents a vector $\vec{q}$ in three-dimensional space if and only if $q_0 = 0$. Thus vectors are identified with those quaternions whose scalar part is zero.

Now let $\vec{q}$ and $\vec{r}$ be vectors, with Cartesian components (q_1, q_2, q_3) and (r_1, r_2, r_3) respectively. If we consider $\vec{q}$ and $\vec{r}$ to be quaternions (with zero scalar part), and multiply them together in accordance with the rules of quaternion multiplication, we find that

$$\vec{q}\,\vec{r} = -(\vec{q} \,.\, \vec{r}) + (\vec{q} \wedge \vec{r}),$$

where $\vec{q}.\vec{r}$ denotes the *scalar product* of the vectors $\vec{q}$ and $\vec{r}$, and $\vec{q} \wedge \vec{r}$ denotes the *vector product* of these vectors. Thus the scalar part of the quaternion $\vec{q}\,\vec{r}$ is $-\vec{q} \,.\, \vec{r}$, and the vector part is $\vec{q} \wedge \vec{r}$.

Note that $\vec{q}\vec{r}$ is itself a vector if and only if the vectors $\vec{q}$ and $\vec{r}$ are orthogonal.

More generally, let q and r be quaternions with scalar parts q_0 and r_0 and with vector parts $\vec{q}$ and $\vec{r}$, so that

$$q = q_0 + \vec{q}, \quad r = r_0 + \vec{r}.$$

Then

$$qr = q_0 r_0 - \vec{q} \,.\, \vec{r} + q_0 \vec{r} + r_0 \vec{q} + \vec{q} \wedge \vec{r},$$

and thus the scalar part of the quaternion qr is

$$q_0 r_0 - \vec{q} \,.\, \vec{r},$$

and the vector part of the quaternion qr is

$$q_0 \vec{r} + r_0 \vec{q} + \vec{q} \wedge \vec{r}.$$

Now let $\vec{u}$, $\vec{v}$ and $\vec{w}$ be an orthonormal triad of vectors in three dimensional space, with

$$|\vec{u}| = |\vec{v}| = |\vec{w}| = 1,$$

$$\begin{aligned} \vec{u} \wedge \vec{v} = -\vec{v} \wedge \vec{u} &= \vec{w}, \\ \vec{v} \wedge \vec{w} = -\vec{w} \wedge \vec{v} &= \vec{u}, \\ \vec{w} \wedge \vec{u} = -\vec{u} \wedge \vec{w} &= \vec{v}, \end{aligned}$$

If we multiply these with one another in accordance with the rules for quaternion multiplication, we find that

$$\vec{u}^2 = \vec{v}^2 = \vec{w}^2 = -1,$$

$$\begin{aligned} \vec{u}\,\vec{v} = -\vec{v}\,\vec{u} &= \vec{w}, \\ \vec{v}\,\vec{w} = -\vec{w}\,\vec{v} &= \vec{u}, \\ \vec{w}\,\vec{u} = -\vec{u}\,\vec{w} &= \vec{v}, \end{aligned}$$

(Note that the rules for multiplying $\vec{u}$, $\vec{v}$ and $\vec{w}$ with one another correspond to Hamilton's rules for multiplying the basic quaternions i, j and k with one another, whenever $\vec{u}$, $\vec{v}$ and $\vec{w}$ constitute a positively oriented basis of three-dimensional space.)

4.13 Quaternions and Rotations

Let us consider the effect of a rotation through an angle θ about an axis in three-dimensional space passing through the origin. Let l, m and n be the cosines of the angles between the axis of the rotation and the three coordinate axes. In Cartesian coordinates, the axis of rotation is then in the direction of the vector (l, m, n), where $l^2 + m^2 + n^2 = 1$. The angle θ and the direction cosines l, m, n of the axis of the rotation together determine a quaternion q, with

$$q = \cos\frac{\theta}{2} + \sin\frac{\theta}{2}(li + mj + nk).$$

Let $\overline{q}$ be the conjugate of q, given by the formula

$$\overline{q} = \cos\frac{\theta}{2} - \sin\frac{\theta}{2}(li + mj + nk).$$

Let (x, y, z) and (x', y', z') be the Cartesian coordinates of two points in three-dimensional space, and let r and r' be the quaternions r and r' be defined by

$$r = xi + jy + zk \text{ and } r' = x'i + y'j + z'k.$$

We shall show that if $r' = qr\overline{q}$ then a rotation about the axis (l, m, n) through an angle θ will send the point (x, y, z) to the point (x', y', z'). (The effect of a rotation through an angle θ in the opposite sense can be calculated by replacing θ by $-\theta$ in the definition of the quaternion q.)

In this way the algebra of quaternions may be used in areas of application such as computer-aided design and the programming of computer games, in order to calculate the results of rotations applied to points in three-dimensional space.

Let $\vec{u}$, $\vec{v}$, $\vec{w}$ be an orthonormal basis of three-dimensional space with $\vec{w} = \vec{u} \wedge \vec{v}$ (as above), and with $\vec{u}$ directed along the axis of the rotation. Let θ be a real number, specifying the angle of rotation, and let q be the quaternion

$$\begin{aligned} q &= \cos\frac{\theta}{2} + \left(\sin\frac{\theta}{2}\right)\vec{u} \\ &= \cos\frac{\theta}{2} + l\sin\frac{\theta}{2}\,i + m\sin\frac{\theta}{2}\,j + n\sin\frac{\theta}{2}\,k, \end{aligned}$$

where

$$\vec{u} = (l, m, n), \quad l^2 + m^2 + n^2 = 1.$$

Then

$$q^{-1} = \overline{q} = \cos\frac{\theta}{2} - \left(\sin\frac{\theta}{2}\right)\vec{u},$$

since

$$\begin{aligned}
q\,\overline{q} &= \left(\cos\frac{\theta}{2} + \sin\frac{\theta}{2}\,\vec{u}\right)\left(\cos\frac{\theta}{2} - \sin\frac{\theta}{2}\,\vec{u}\right) \\
&= \cos^2\frac{\theta}{2} + \left(\sin^2\frac{\theta}{2}\right)\,\vec{u}\,.\,\vec{u} \\
&\qquad - \left(\sin^2\frac{\theta}{2}\right)\,\vec{u}\wedge\vec{u} \\
&= \cos^2\frac{\theta}{2} + \sin^2\frac{\theta}{2} \\
&= 1.
\end{aligned}$$

Also we find that

$$\begin{aligned}
q^2 &= \left(\cos\frac{\theta}{2} + \sin\frac{\theta}{2}\,\vec{u}\right)\left(\cos\frac{\theta}{2} + \sin\frac{\theta}{2}\,\vec{u}\right) \\
&= \cos^2\frac{\theta}{2} - \left(\sin^2\frac{\theta}{2}\right)\,\vec{u}\,.\,\vec{u} \\
&\qquad + 2\sin\frac{\theta}{2}\,\cos\frac{\theta}{2}\,\vec{u} + \left(\sin^2\frac{\theta}{2}\right)\,\vec{u}\wedge\vec{u} \\
&= \cos^2\frac{\theta}{2} - \sin^2\frac{\theta}{2} + 2\sin\frac{\theta}{2}\,\cos\frac{\theta}{2}\,\vec{u} \\
&= \cos\theta + \sin\theta\,\vec{u}.
\end{aligned}$$

Let us now calculate the quaternion products $q\vec{u}\,\overline{q}$, $q\vec{v}\,\overline{q}$ and $q\vec{w}\,\overline{q}$. We first note that

$$\vec{u}\,\overline{q} = \overline{q}\,\vec{u}, \quad \vec{v}\,\overline{q} = q\vec{v}, \quad \vec{w}\,\overline{q} = q\vec{w}.$$

Therefore

$$\begin{aligned}
q\vec{u}\,\overline{q} &= q\overline{q}\,\vec{u} = \vec{u}, \\
q\vec{v}\,\overline{q} &= q^2\vec{v} = (\cos\theta + \sin\theta\,\vec{u})\vec{v} \\
&= \cos\theta\vec{v} + \sin\theta\vec{w}, \\
q\vec{w}\,\overline{q} &= q^2\vec{w} = (\cos\theta + \sin\theta\,\vec{u})\vec{w} \\
&= \cos\theta\vec{w} - \sin\theta\vec{v}
\end{aligned}$$

Thus if we define $T\colon \mathbb{R}^3 \to \mathbb{R}^3$ to be the transformation that sends a vector $\vec{r}$ to $q\vec{r}\,\overline{q}$, then T fixes the vector $\vec{u}$, rotates the vector $\vec{v}$ about the direction of $\vec{u}$ through an angle θ towards $\vec{w}$, and rotates $\vec{w}$ about the direction of $\vec{u}$ through an angle θ towards $-\vec{v}$. This transformation T is therefore a rotation about the direction of $\vec{u}$ through an angle θ.