§4 Inverses

Inverses are well-behaved in an alternative algebra. Indeed, alternative division algebras can be characterized as those in which $x^{-1}(xy) = y$ and $(yx)x^{-1} = y$ for all x and y, a result which is geometrically significant. We will see in Appendix V that geometries with "enough" translations are precisely those coordinatized by division rings satisfying these inverse condition, therefore precisely those coordinatized by alternative division rings.

There is a general definition of division algebra which is applicable to arbitrary nonassociative algebras. An algebra A is a division algebra if all elements $a \neq 0$ are <u>operator invertible</u> in the sense that the multiplication operators L_a and R_a are bijective. In terms of equations, this means that for nonzero a and arbitrary b there are unique solutions x, y to the equations

$$ax = b$$

$$ya = b$$

(the existence is equivalent to surjectivity of L_a, R_a respectively, and uniqueness to their injectivity). These are the sort of division algebras that coordinatize projective planes, where the uniqueness of solutions is what guarantees that lines intersect the right number of times.

Often one assumes the existence of a unit element, $1a = a1 = a$ for all a. A general division algebra need not have a unit; if it does, for each $a \neq 0$ there will be unique elements a_L, a_R with

$aa_R = 1 = a_L a$. However, it doesn't follow that $a_L = a_R$, or that $a_L(ax) = x$ for all x. Indeed a_L and a_R need not resemble our ordinary concept of inverses at all. The general notion of division algebra is designed with unique solutions of equations in mind, and disregards inverses.

On the other hand, we could call an algebra a division algebra if all $x \neq 0$ had unique (two-sided) inverses $xx^{-1} = 1 = x^{-1}x$. However, this does not imply L_x, R_x are bijective (so the algebra needn't be a division algebra according to the other definition).

It is important that these two notions of invertibility, operator-wise (L_x, R_x being bijective) or element-wise ($xx^{-1} = 1 = x^{-1}x$), coincide for alternative algebras, so that division algebra means what it ought to (in either of the above senses).

We adopt the element approach. An element x in a unital algebra is <u>left invertible</u> with <u>left inverse</u> y if $yx = 1$, <u>right invertible</u> with <u>right inverse</u> y if $xy = 1$, and <u>invertible</u> with <u>inverse</u> y if $xy = yx = 1$. A <u>division algebra</u> is a unital algebra in which all nonzero elements are invertible.

For one-sided inverses we have a

4.1 (One-sided Inverse Theorem) The following are equivalent for elements x,y of a unital alternative algebra:

(i) $xy = 1$

(ii) $L_x L_y = I$

(iii) $R_y R_x = I$.

In this case $[x,y,z] = 0$ for all z.

Proof. Clearly (ii) $\Rightarrow$ (i) since $xy = L_x L_y 1$. Conversely (i) $\Rightarrow$ (ii) since $I = U_1 = U_{xy}$ (by (i)) $= L_x U_y R_x$ (left fundamental), so $L_x L_y = L_x L_y L_x U_y R_x = L_{xyx} U_y R_x$ (left Moufang) $= L_x U_y R_x$ (by (i)) $= I$. Similarly (i) $\Leftrightarrow$ (iii). In this case $[x,y,z] = (xy)z - x(yz) = z - L_x L_y z = 0$ for all z. ∎

For two-sided inverses we have an

4.2 (Inverse Theorem) The following are equivalent for an element in a unital alternative algebra:

(i) x has a left and a right inverse

(ii) x is an invertible element

(iii) L_x is an invertible operator

(iv) R_x is an invertible operator

(v) U_x is an invertible operator

(vi) $1 \in \operatorname{Im} U_x$

(vii) $1 \in \operatorname{Im} L_x \cap \operatorname{Im} R_x$.

In this case the inverse of x is uniquely determined as

$$x^{-1} = L_x^{-1}1 = R_x^{-1}1 = U_x^{-1}x ,$$

x^{-1} is invertible with inverse

(viii) $(x^{-1})^{-1} = x$,

and the multiplication operators

(ix) $L_{x^{-1}} = L_x^{-1}$, $R_{x^{-1}} = R_x^{-1}$, $U_{x^{-1}} = U_x^{-1}$.

If x,y are invertible so is xy and

(x) $(xy)^{-1} = y^{-1}x^{-1}$.

Proof. Clearly (iii) + (iv) $\Rightarrow$ (v) $\Rightarrow$ (vi) $\Rightarrow$ (vii) $\Rightarrow$ (i) since $U_x = L_x R_x = R_x L_x$, and (i) $\Rightarrow$ (ii) since $xy = zx = 1$ implies $y = L_z L_x y$ (by One-Sided Inverse) $= z(xy) = z1 = z$ and $y = z$ is a two-sided inverse. Further (ii) $\Rightarrow$ (iii) since $xy = yx = 1$ implies $L_x L_y = L_y L_x = I$ by the One-Sided Inverse Theorem; conversely (iii) $\Rightarrow$ (ii) since if L_x is surjective there is a y such that $xy = 1$, and if L_x is also injective then $x(yx - 1) = (xy)x - x = x - x = 0$ implies $yx - 1 = 0$ and $yx = 1$. Similarly (ii) $\Leftrightarrow$ (iv). Thus (iii) $\Leftrightarrow$ (iv) $\Rightarrow$ (iii) + (iv).

If y is an inverse of x then $L_x y = R_x y = 1$, $U_x y = x$ imply $y = L_x^{-1}1 = R_x^{-1}1 = U_x^{-1}x$. The relations $L_{x^{-1}} = L_y = L_x^{-1}$ and $R_{x^{-1}} = R_y = R_x^{-1}$ follow from $xy = yx = 1$ and the One-Sided Inverse Theorem; from these we see $U_{x^{-1}} = L_{x^{-1}} R_{x^{-1}} = L_x^{-1} R_x^{-1} = (R_x L_x)^{-1} = U_x^{-1}$ too. This proves (ix). Since $L_y = L_x^{-1}$ is invertible, y is invertible with inverse $L_y^{-1}1 = L_x 1 = x$, establishing (viii).

If x,z are invertible then $U_{xz} = L_x U_z R_x$ is invertible (using left fundamental, (iii), (iv), (v)) so by (iv) xz is invertible with inverse $U_{xz}^{-1}(xz) = (L_x U_z R_x)^{-1}(L_x z) = R_x^{-1} U_z^{-1} L_x^{-1}(L_x z) = R_x^{-1} U_z^{-1} z = R_x^{-1} z^{-1} = R_{x^{-1}} z^{-1}$ $= z^{-1}x^{-1}$ (by (ix)). This finishes (x) and the Theorem. ∎

4.3 Corollary. xyx is invertible $\Leftrightarrow$ x and y are invertible $\Leftrightarrow$ xy and yx are invertible.

Proof. If xyx is invertible so is the operator $U_{xyx} = U_x U_y U_x$ (middle fundamental). Now any time ABA is an invertible operator, A must be invertible: A is surjective since $\operatorname{Im} A \supset \operatorname{Im} ABA = A$, and injective since $\operatorname{Ker} A \subset \operatorname{Ker} ABA = 0$. Thus U_x is invertible, $U_y =$

$U_x^{-1}U_{xyx}U_x^{-1}$ is invertible, so by (v) x and y are invertible.

If xy and yx are invertible, so are $(xy)(yx) = xy^2x$ and $(yx)(xy) = yx^2y$, so by the above x and y are invertible.

If x and y are invertible, so are xy, yx, xyx since by (x) products of invertible elements are invertible. ∎

Warning: Even in associative algebras, invertibility of xy does not guarantee invertibility of x and y.

This shows element invertibility of x coincides with operator-invertibility of L_x (and R_x, and U_x) in a unital algebra. Besides testing for invertibility, these operators can test for unit elements in a (not necessarily unital) algebra.

4.4 (U-Test for Units) If U_x is surjective for some x (equivalently, both L_x and R_x are surjective) then the alternative algebra A necessarily has a unit and x is invertible.

Proof. If L_x is surjective then xe = x for some e. Since U_x is surjective, any element $y \in A$ can be written y = xzx for some z, so $ye = (xzx)e = x\{z(xe)\}$ (left Moufang) $= x\{zx\} = y$ and e is a right unit. Similarly, if fx = x then f is a left unit. Therefore e = f = 1 is the unit element. Once U_x is surjective its image contains 1, so by 4.2 vi x is invertible. ∎

4.5 (L,R-Test for Units) If some L_x is bijective the alternative algebra A has a left unit; if some R_y is bijective then A has a right unit; if some L_x, R_y are bijective then A has unit and x,y are invertible.

Proof. It suffices to prove the first statement (the second follows by symmetry, together they imply the third). Since L_x is surjective we again have $xe = x$ for some e. Any z can be written $z = xw$ for some w, and $x(ez-z) = x(e(xw)-xw) = (xex)w - x^2w$ (left Moufang) $= x^2w - x^2w = 0$. Injectivity of L_x forces $ez - z = 0$, so $ez = z$ and this time e is a left unit. ▪

4.6 (All-L-Test for Units) If all L_x for $x \neq 0$ are surjective, then A is unital and all $x \neq 0$ are invertible (thus A is a division algebra).

Proof. If $x,y \neq 0$ then L_x, L_y are surjective, hence $L_xL_yL_x = L_{xyx}$ is too by left Moufang; in particular, $xy \neq 0$. This shows L_x is injective as well as surjective, so all L_x for $x \neq 0$ are bijective. But as soon as one L_x is bijective we have a left unit e by the L,R-Test, and e must be a right unit as well since $(xe-x)x = x(ex) - x^2 = x^2 - x^2 = 0$ forces $xe - x = 0$ and $xe = x$. Therefore all L_x for $x \neq 0$ are bijective in the unital algebra A, so by the Inverse Theorem all $x \neq 0$ are invertible and A is a division algebra. ▪

Putting these together, we can show that the operator-wise and element-wise definition of division algebra coincide even in the non-unital case.

4.7 (Equivalence Theorem for Division Algebras) An alternative algebra $A \neq 0$ is a division algebra iff all L_x, R_x for $x \neq 0$ are invertible operators.

Proof. In a (unital) division algebra all $x \neq 0$ are invertible as elements, so L_x, R_x are invertible as operators. Conversely, if all L_x, R_x for $x \neq 0$ are invertible (and some $x \neq 0$ exists) then by any of the tests A is unital, and once we have a unital algebra invertibility of all L_x, R_x implies invertibility of all $x \neq 0$. ∎

Exercises

4.1 Prove $xy = 1 \Rightarrow L_x L_y = I$ by showing $E = L_x L_y$ is an idempotent operator with $E\, R_y R_x = I$.

4.2 Prove $xy = yx = 1 \Rightarrow L_x$ invertible by considering xy^2x.

4.3 If $x_1(x_2(\ldots x_n)) = 1 = ((x_n \ldots)x_2)x_1$ show each x_i is invertible.

4.4 If xy is invertible show x has a right and y a left inverse.

4.5 Show that in a unital algebra, L_x surjective $\Rightarrow R_x$ injective (similarly R_x surjective $\Rightarrow L_x$ injective).

4.6 If the left annihilator $A^{\perp,L} = \{z / zA = 0\}$ is zero, show any left unit element is a two-sided unit.

4.7 If A has a.c.c. on subspaces $\operatorname{Ker} L_a$, show L_x surjective $\Rightarrow L_x$ injective. If A has d.c.c. on subspaces of the form $\operatorname{Im} L_a$, show L_x injective $\Rightarrow L_x$ surjective. Conclude that if a unital alternative algebra A has a.c.c. or d.c.c. on subspaces $\operatorname{Ker} L_a$ or $\operatorname{Im} L_a$, then any one-sided inverse is two-sided.

4.8 (Meta-exercise) Take any two of 4.2(i)-(vii) and prove directly that one implies the other.

4.9 Prove $(x^2)^{-1} = (x^{-1})^2$, $(x^3)^{-1} = (x^{-1})^3$. Define powers inductively by $x^{n+2} = U_x x^n$, and prove $(x^n)^{-1} = (x^{-1})^n$ for all n. While you're at it, prove $x^n x^m = x^{n+m}$ (so that the powers could also have been defined by $x^{n+1} = L_x x^n$ or $x^{n+1} = R_x x^n$). Show $L_{x^n} = L_x^n$, $R_{x^n} = R_x^n$, $U_{x^n} = U_x^n$ for all (positive and negative) n.

4.10 Prove in two different ways that if all $x \neq 0$ in a unital algebra A are right invertible then A is a division algebra (dually if they are all left invertible).

4.11 If $A \xrightarrow{F} \tilde{A}$ is a homomorphism with $F(1) = 1$, show $F(x^{-1}) = F(x)^{-1}$.

4.12 If x is invertible show $L_{x^n} = L_x^n$, $R_{x^n} = R_x^n$, $U_{x^n} = U_x^n$, $x^n x^m = x^{n+m}$ for all (positive or negative n, m. Conclude L_x, R_x generate a commutative associative algebra, containing all L_{x^n}, R_{x^n}, U_{x^n}, and that $\Phi[x, x^{-1}]$ is isomorphic to the commutative, associative group ring of an infinite cyclic group.

#2. Problem Set on Moufang Loops

A quasigroup is a set X together with a binary composition $(x,y) \to x\cdot y$ such that left and right multiplications $L_x : y \to x\cdot y$ and $R_x : y \to y\cdot x$ are bijective for each x. A loop is a quasigroup with unit 1, $1\cdot x = x = x\cdot 1$ for all x. Thus a loop is a sort of a "nonassociative group". Such objects appear frequently in geometry; for example, a finite set with a binary composition is a quasigroup if and only if its multiplication table is a Latin square.

In a loop, each element x has a unique left inverse x_L^{-1} and a unique right inverse x_R^{-1} defined by $x_L^{-1}x = 1 = xx_R^{-1}$.

1. A loop L has the left inverse property if

$$(1) \quad x_L^{-1}(xy) = y$$

for all x,y; similarly it has the right inverse property if

$$(2) \quad (yx)x_R^{-1} = y.$$

It is a loop with inverse property if it satisfies (1) and (2). Show that in a loop with inverse property there is a unique inverse, $x_L^{-1} = x_R^{-1} = x^{-1}$, and that

$$(3) \quad (x^{-1})^{-1} = x.$$

Show also that

$$(4) \quad (xy)^{-1} = y^{-1}x^{-1}$$

2. A loop has the left, right, or middle Moufang property if

$$(5)\quad [(xy)x]z = x[y(xz)]$$

$$(6)\quad z[x(yx)] = [(zx)y]x$$

$$(7)\quad [x(yz)]x = (xy)(zx)$$

respectively for all x,y,z. Show that any one of (5), (6), (7) implies flexibility

$$(8)\quad (xy)x = x(yx).$$

In particular, (7) is equivalent to

$$(7)'\quad x[(yz)x] = (xy)(zx).$$

Show that in a loop satisfying (8) the inverse is unique, $x_L^{-1} = x_R^{-1} = x^{-1}$. Use this to show that any one of (5), (6), (7) implies both of (1) and (2), and hence that L is a loop with inverse property.

3. Show that (5), (6), (7), (7)' are all equivalent; a loop satisfying one (hence all) of them is called a Moufang loop. These are sort of "alternative groups". Problem 2 just says that a Moufang loop has the inverse property.

4. It is not true in general that, conversely, every loop with inverse property is a Moufang loop. However, suppose D is a (nonassociative) division ring with unit in the sense that all L_x and R_x for $x \neq 0$ are bijective. Then the nonzero elements form a loop L under multiplication. The fact that L can be imbedded in a ring, so that we have the operation of addition around besides the multiplication $x \cdot y$, makes L a very special kind of loop. Prove that if such an L forms a loop with