

INFINITE-DIMENSIONAL QUADRATIC FORMS ADMITTING COMPOSITION

IRVING KAPLANSKY

In [2] Albert proved that a finite-dimensional absolute-valued algebra over the reals is necessarily alternative (and hence the reals, complexes, quaternions, or Cayley numbers). In [3] he extended this from finite-dimensional to algebraic algebras. Recently, Wright [9] succeeded in removing the assumption that the algebra is algebraic. Wright proceeds by proving that the norm springs from an inner product, and then that the algebra is algebraic. Now if the norm $|x|$ comes from an inner product, then $|x|^2$ is a quadratic form in x , and moreover the assumption $|xy| = |x||y|$ means that it is a quadratic form admitting composition. Thus Albert's finite-dimensional theorem can be proved by combining Wright's result with Hurwitz's classical theorem on quadratic forms admitting composition. The main purpose of this paper is to make a similar method possible in the infinite-dimensional case by providing a suitable generalization of Hurwitz's theorem. The result is essentially that infinite-dimensional quadratic forms cannot admit composition, except in the rather trivial case of purely inseparable fields of characteristic two.

In the concluding moments of the proof we rely heavily on the recent developments in the theory of alternative rings. Until then the paper is quite self-contained and elementary, and the style of the argument is very close to that of [1], [5], and [8].

Let A be a vector space over a field F . The function $g(x)$ from A to F is a quadratic form if

$$(1) \quad g(\lambda x) = \lambda^2 g(x)$$

for $\lambda \in F$, $x \in A$, and further the function f defined by

$$(2) \quad f(x, y) = g(x + y) - g(x) - g(y)$$

is bilinear in x and y . We say that g is nonsingular if $g(x) = f(x, A) = 0$ implies $x = 0$. If the characteristic is not two, this is equivalent to the nonsingularity of f , the latter meaning that $f(x, A) = 0$ implies $x = 0$. The form g is said to admit composition if there exists a bilinear product xy from $A \times A$ to A with

$$(3) \quad g(xy) = g(x)g(y).$$

Received by the editors March 20, 1953.

We can, and shall, regard the product xy as making A into an algebra.

We propose to assume outright that A has a unit element. In the finite-dimensional case, or in the infinite-dimensional case if A is a division algebra, it is known that this entails no loss of generality. For completeness we sketch this reduction. Take $a \in A$ with $g(a) \neq 0$, and set $b = a^2/g(a)$; then by (1) we have $g(b) = 1$. The mapping $R_b: x \rightarrow xb$ preserves the form g and hence is a one-to-one map of A into itself. In either of the two cases cited, R_b must then automatically be onto. (In the general case, it seems unlikely that R_b could fail to be onto for every possible choice of b , but I have been unable to rule out this possibility.) A similar discussion applies to $L_b: x \rightarrow bx$. Now define a new product on A by $x \cdot y = (xR_b^{-1})(yL_b^{-1})$. We still have $g(x \cdot y) = g(x)g(y)$, and relative to the new product b^2 is a two-sided unit element.

We now formulate and prove our theorem.

THEOREM. *Let A be an algebra with unit element over a field F . Suppose that A carries a nonsingular quadratic form g satisfying (3) for all x, y in A . Then: (a) A is alternative, (b) except for the case where A has characteristic two and is a purely inseparable field over F , A is finite-dimensional and of dimension 1, 2, 4, or 8, (c) A is either simple or the direct sum of two copies of F , (d) $g(x) = x^*x$ where $x \rightarrow x^*$ is an involution of A .*

PROOF. We begin the proof by showing that $g(1) = 1$. Now g cannot be identically 0, for then so is f by its definition (2), contradicting the assumed nonsingularity of the form. Choose y so that $g(y) \neq 0$, and set $x = 1$ in (3); the result is $g(y) = g(1)g(y)$, whence $g(1) = 1$. As is customary, we identify scalar multiples of the unit element with elements of F ; with this convention we have $g(\lambda) = \lambda^2$ for λ in F . Since $g(x^2) = g(x)^2$ by (3), we find in particular that the quadratic form takes the same value at x^2 and $g(x)$.

We proceed to dispose of the case where f is identically 0 (which is possible of course only for characteristic two). Then (2) tells us that the mapping $x \rightarrow g(x)$ is an additive homomorphism of A into F . Since by (3) the mapping is always multiplicative, we find that it is actually a ring homomorphism of A into F . Now the nonsingularity of g (in the case $f \equiv 0$) is precisely equivalent to the fact that the kernel of this homomorphism is 0. In other words, $x \rightarrow g(x)$ is a ring isomorphism of A into F . At this point we already know that A is an integral domain, and is in particular associative. For any x in A , we saw in the preceding paragraph that g coincides at x^2 and $g(x)$.

Hence $g(x) = x^2$. This shows that A is a field; indeed for $x \neq 0$ the inverse of x is $x/g(x)$. Moreover A is purely inseparable over F , with the square of every element of A lying in F . This concludes the discussion of the case $f \equiv 0$. We remark that quadratic forms of this kind do indeed exist in the infinite-dimensional case (as well as for finite dimensions of the form 2^n); a suitable base field can be obtained by adjoining an infinite number of indeterminates to any field of characteristic two.

In the remainder of the proof we assume that f is not identically 0, from which we shall shortly deduce that f is actually nonsingular. Our main tool is the result of linearizing (3) with the aid of (2). Thus on setting $x = a + b$ we get

$$(4) \quad f(ay, by) = f(a, b)g(y),$$

and on further linearizing with respect to y :

$$(5) \quad f(ac, bd) + f(ad, bc) = f(a, b)f(c, d).$$

Suppose that $f(y, A) = 0$ for $y \neq 0$. Then, by the nonsingularity of g , $g(y) \neq 0$. On setting $a = 1$ in (4) we deduce $f(1, b) = 0$. This holds for any b , so that $f(1, A) = 0$. Now set $a = c = 1$ in (5). The conclusion is that $f(b, d) = 0$ for any b and d . This contradicts our assumption that f is not identically 0, and we have thereby proved that f is nonsingular.

Set $b = 1$ and $c = ae$ in (5):

$$(6) \quad f(a \cdot ae, d) + f(ad, ae) = f(a, 1)f(ae, d).$$

According to (4), or rather its symmetric analogue, $f(ad, ae) = g(a)f(d, e)$. We make this substitution in (6), and after reorganizing we have $f(z, d) = 0$ where we have written

$$z = a \cdot ae - f(1, a)ae + g(a)e.$$

Since this is true for any d , we have $z = 0$. In particular the special case $e = 1$ gives us

$$(7) \quad a^2 - f(1, a)a + g(a) = 0.$$

Multiply (7) on the right by e , and compare the result with $z = 0$. We find in this way that $a \cdot ae = a^2e$, the left half of the alternative law. Similarly we prove the other half, and we now know that A is alternative.

Define $a^* = f(1, a) - a$. This is at any rate a linear mapping of A into itself. By (2) we have $f(1, 1) = g(2) - 2g(1)$. Since $g(1) = 1$ and $g(2) = 4$, we find $f(1, 1) = 2$. From this we compute that $1^* = 1$ and

$a^{**} = a$. Equation (7) asserts precisely that $g(a) = a^*a$. The remaining point we wish to verify is that $*$ is an anti-automorphism: $(ab)^* = b^*a^*$. To do this we linearize (7), that is we replace a by $a+b$ and then cancel the terms which are quadratic in a and b . We find

$$(8) \quad ab + ba - f(a, 1)b - f(b, 1)a + f(a, b) = 0.$$

Next set $a = c = 1$ in (5) and change notation, getting

$$(9) \quad f(1, ab) + f(a, b) = f(1, a)f(1, b).$$

By combining (8) and (9) we find precisely the equation $(ab)^* = b^*a^*$.

Let us summarize: we know that A is an alternative algebra with unit element, and that it has an involution $*$ such that $a + a^*$ and a^*a are in F for every a ; indeed a^*a coincides with the given quadratic form $g(a)$. The next step in determining the structure of A will be separated out as a lemma; this lemma is presumably well known but does not seem to be explicitly recorded anywhere.

LEMMA. *Let A be an algebra over a field F . Suppose that A has a unit element, that it admits an involution $*$ such that $x + x^*$ and x^*x are in F for every x , and that the quadratic form given by x^*x is nonsingular. Then: either A is simple, or it is the direct sum of two copies of F (with the involution interchanging the summands).*

PROOF OF THE LEMMA. We first prove that A is $*$ -simple in the sense that it has no $*$ -ideals other than 0 and A . Suppose that $I \neq A$ is a two-sided ideal in A , satisfying $I = I^*$. We note that I cannot contain any nonzero elements of F (for otherwise $I = A$). This shows that $a + a^* = a^*a^* = 0$ for any a in I . Let us write f for the bilinear form corresponding to x^*x ; thus $f(x, y) = x^*y + y^*x = (y^*x)^* + y^*x$. If x is in I so is y^*x , and it follows that $f(x, y) = 0$ for any y in A . By the nonsingularity of the quadratic form we have $x = 0$, and hence $I = 0$.

We have thus proved that A is $*$ -simple. Next let J denote any proper ideal in A . Then $J \cap J^*$ and $J + J^*$ are both $*$ -ideals; so we must have $J \cap J^* = 0$, $J + J^* = A$, that is, $A = J \oplus J^*$. Since $a + a^*$ is in F for every a , this decomposition is possible only if J is one-dimensional, i.e., A is a direct sum of two copies of F . The alternative is that A is actually simple, and this completes the proof of the lemma.

We are now ready to conclude the proof of the main theorem. The hypotheses of the lemma are valid for our algebra A . Putting aside the case where A is the direct sum of two copies of F , we may assume that A is simple. Let Z denote its center; Z is a field over F . First suppose that A is not associative. Then by the general theorem of Kleinfeld [7] on simple alternative rings, A is an 8-dimensional

Cayley-Dickson algebra over Z . (In the special case at hand we could also get what is needed out of [3] and [4]; if A has an idempotent, [4] applies, while otherwise A is a division algebra and [3] applies.) Suppose on the other hand that A is associative. Then the fact, given by (7), that every element of A satisfies a quadratic equation is known to imply finite-dimensionality of A over Z ; we can for example cite Theorems 5 and 7 of [6].

Once it is known that $[A:Z]$ is finite, we are on familiar ground, and elementary arguments show that A must also be finite-dimensional over F , with dimension equal to 1, 2, 4, or 8. (Indeed Z must coincide with F , except when A is a quadratic field over F .) We have thereby completed the proof of the theorem.

BIBLIOGRAPHY

1. A. A. Albert, *Quadratic forms permitting composition*, Ann. of Math. vol. 43 (1942) pp. 161-177.
2. ———, *Absolute valued real algebras*, Ann. of Math. vol. 48 (1947) pp. 495-501.
3. ———, *Absolute valued algebraic algebras*, Bull. Amer. Math. Soc. vol. 55 (1949) pp. 763-768.
4. ———, *On simple alternative rings*, Canadian Journal of Mathematics vol. 4 (1952) pp. 129-135.
5. H. Freudenthal, *Oktaven, Ausnahmegruppen und Oktavengeometrie*, Utrecht, 1951.
6. N. Jacobson, *Structure theory for algebraic algebras of bounded degree*, Ann. of Math. vol. 46 (1945) pp. 695-707.
7. E. Kleinfeld, *Simple alternative rings*, Ann. of Math. vol. 58 (1953) pp. 544-547.
8. Y. V. Linnik, *Quaternions and Cayley numbers; some applications of the arithmetic of quaternions*, Uspehi Matem. Nauk vol. 4 no. 5 (1949) pp. 49-98 (Russian).
9. F. B. Wright, *Absolute valued algebras*, Proc. Nat. Acad. Sci. U.S.A. vol. 39 (1953) pp. 330-332.

UNIVERSITY OF CHICAGO