MATHEMATICS

AN ALGEBRAIC PROOF OF A THEOREM OF H. HOPF

BY

T. A. SPRINGER

(Communicated by Prof. H. D. KLOOSTERMAN at the meeting of November 28, 1953)

1. H. HOPF has proved with topological methods that there exists over the field of real numbers no commutative and non-associative division algebra with unit ([3], see also [1] and [2]). In other words: *let K be a commutative, but not necessarily associative division algebra with unit over the field of real numbers R. Then K is either R or the field of complex numbers.*

In the present note we shall give an algebraic proof of this theorem.

2. Let K be as above. K is an n-dimensional vector space over R, let (e_i) $(1 \leqslant i \leqslant n)$ be a basis of K over R. Then we have

$$x \cdot y = \sum_{k=1}^{n} f_k(x, y)\, e_k \qquad (x, y \in \mathrm{K}).$$

The assumption that K is a commutative division algebra implies

(1a) $\quad f_k(x, y)$ is a symmetric bilinear form on K,

(1b) $\quad$ if $f_k(x, y) = 0$ $(1 \leqslant k \leqslant n)$, then either $x = 0$ or $y = 0$.

We shall derive a number of consequences from (1a) and (1b).

A) *There exist no complex vectors*[1]) $z \neq 0$ *such that* $f_k(z, z) = 0$ $(1 \leqslant k \leqslant n)$.

Proof. Let $z = x + iy$, $f_k(z, z) = 0$ $(1 \leqslant k \leqslant n)$. Then $f_k(x, x) - f_k(y, y) + 2if_k(x, y) = 0$, which implies $f_k(x, x) = f_k(y, y)$, $f_k(x, y) = 0$. By (1b) we have either $x = 0$ or $y = 0$. Then we find $f_k(y, y) = 0$ or $f_k(x, x) = 0$, which yields, again by (1b), $y = 0$ or $x = 0$. Thus $z = 0$.

B) *There exists a real vector x such that $f_k(x, x) = \varrho_k$ or $f_k(x, x) = -\varrho_k$ $(1 \leqslant k \leqslant n)$, where (ϱ_k) is a set of n arbitrary real numbers.*

Proof. If $x \in \mathrm{K}$, $x = \sum_{k=1}^{n} x_k e_k$, then $f_k(x, x)$ is a homogeneous quadratic polynomial in $x_1, x_2, \ldots, x_n$.

Consider the system of n homogeneous equations in the $(n+1)$ variables $x_0, x_1, \ldots, x_n$

(2) $$f_k(x, x) = \varrho_k x_0^2 \qquad (1 \leqslant k \leqslant n).$$

Since the number of equations is less than the number of variables, (2)

[1]) A complex vector is a vector from the vector space obtained from K by extending the field of coefficients R to the field of complex numbers. Any complex vector z may be written as $z = x + iy$, where x and y are real vectors, i.e. vectors from K.

has a nontrivial complex solution ([4], Kapitel 11). Thus there exists a complex vector $z=x+iy$ and a complex number $x_0=a+ib$, not both zero such that

$$f_k(x+iy, x+iy) = \varrho_k (a+ib)^2 \qquad (1 \leqslant k \leqslant n).$$

It follows that the real vectors x, y and the real numbers a, b satisfy

$$(3) \qquad \begin{cases} f_k(x,x) - f_k(y,y) = \varrho_k(a^2-b^2) \\ f_k(x,y) = \varrho_k ab. \end{cases} \qquad (1 \leqslant k \leqslant n)$$

By A) the case $a+ib=0$ is ruled out, and it is easily seen that $x+iy=0$ is also impossible.

(3) implies

$$f_k(ax+by, bx-ay) = 0 \qquad (1 \leqslant k \leqslant n).$$

By (1b) this is only possible if $ax+by=0$ or $bx-ay=0$. If $a\neq 0$, $b\neq 0$ we have $y=-(a/b)x$ or $y=(b/a)x$. Substitution into the second relation (3) gives $f_k(x,x)=-\varrho_k b^2$ or $f_k(x,x)=\varrho_k a^2$. Thus $f_k(b^{-1}x, b^{-1}x)=-\varrho_k$ in the first case and $f_k(a^{-1}x, a^{-1}x)=\varrho_k$ in the second case.

If $a=0$, $b\neq 0$ the second relation (3) gives $x=0$ or $y=0$. Then the first relation (3) yields $f_k(y,y)=\varrho_k b^2$ or $f_k(x,x)=-\varrho_k b^2$, thus $b^{-1}x$ or $b^{-1}y$ satisfy our requirements. The case $a\neq 0$, $b=0$ is treated in the same way.

C) *If the real numbers ϱ_k are not all equal to zero, the number of complex solutions z of $f_k(z,z)=\varrho_k$ $(1 \leqslant k \leqslant n)$ is 2 or 4, these solutions are either real or purely imaginary.*

Proof. Let $z=x+iy$, $f_k(z,z)=\varrho_k$. Then $f_k(x,x)-f_k(y,y)=\varrho_k$, $f_k(x,y)=0$. By (1b) $x=0$ or $y=0$, which proves the second part of the assertion. In the first case $f_k(y,y)=-\varrho_k$, in the second case $f_k(x,x)=\varrho_k (1 \leqslant k \leqslant n)$. Now $f_k(x,x)=\varrho_k$ $(1 \leqslant k \leqslant n)$ has either 0 or 2 real solutions, for if $f_k(x,x)=f_k(y,y)$, then $f_k(x+y, x-y)=0$ $(1 \leqslant k \leqslant n)$, which implies $x=y$ or $x=-y$ by (1b). Our assertion now follows from B).

3. We now consider again the system (2), we assume that the numbers ϱ_k are not all zero. $f_k(x,x)-\varrho_k x_0^2=0$ represents a quadratic hypersurface V_k in the complex projective n-space of the variables $x_0, x_1, \ldots, x_n$. By A), $x_0\neq 0$ in a point of intersection of the V_k $(1 \leqslant k \leqslant n)$. Thus, by C), the intersection consists of 2 or 4 points. We assert that these points of intersection have multiplicity 1. By a well-known theorem ([5], p. 171) this will follow if we show that the hypersurfaces V_k $(1 \leqslant k \leqslant n)$ have no common tangent in a point of intersection.

Let $A=(a_0, a_1, \ldots, a_n)$ be a point of intersection. We have seen that $a_0\neq 0$. If $(x_0, x_1, \ldots, x_n)$ is a point in P^n, we write $x=\sum_{k=1}^n x_k e_k$. Then the coordinates of a point $(x_0, x_1, \ldots x_n)$ on a line l through A satisfy $x_0=\lambda a_0+\mu b_0$, $x=\lambda a+\mu b$, where b_0 is a complex number and b a complex vector such that $b\neq (b_0/a_0)a$. If l is a tangent to V_k in A, the quadratic equation $f_k(\lambda a+\mu b, \lambda a+\mu b)=$ $=\varrho_k(\lambda a_0+\mu b_0)^2$ must have two roots $\mu=0$, i.e. we must have

$$f_k(a,b) = \varrho_k a_0 b_0.$$

We also have [illegible], thus

(5) $$t(a, a_0 b - b_0 a) = 0.$$

Now by (') we may assume that a is either a real vector $\neq 0$ or a purely imaginary vector $\neq 0$. In the latter case ia is a real vector and

$$t(ia, a_0 b - b_0 a) = 0.$$

If l were a tangent in A to all V_k, (5) would hold for all k, and then (1b) would imply $a_0 b - b_0 a = 0$ or $b = (b_0/a_0)a$, which is impossible. This proves that the $V_k (1 \leq k \leq n)$ have no common tangent in a point of intersection, and as we have mentioned above, this implies that the multiplicity of the points of intersection is 1.

Now by Bezout's theorem ([5], p. 177) the number of points of intersection, which is 2 or 4 by ('), equals the product of the degrees of the n hypersurfaces $V_k (1 \leq k \leq n)$. Thus we have $2^n = 2$ or $2^n = 4$. In the first case $n = 1$ and K = R. In the second case it follows from (') that $f_k(x, x) = \varrho_k (1 \leq k \leq n)$ has a solution for arbitrary ϱ_k. This means that any $a \in$ K is a square in K. Let e denote the unit of K. There exists an element $i \in$ K such that $i^2 = -e$. It is easily seen that i and e are linearly independent, thus they constitute a basis of K over R. This proves that, if $n = 2$, K is the field of complex numbers.

University of Leiden.

REFERENCES

1. BEHREND, F., Über Systeme algebraischer Gleichungen, Compos. Math. 1, 1–19 (1939).
2. HOPF, H., Ein topologischer Beitrag zur reellen Algebra, Comm. Math. Helv. 13, 219–239 (1940).
3. ———, Systeme symmetrischer Bilinearformen und euklidische Modelle der projektiven Räume, Vierteljahrsschrift der Naturforsch. Gesellschaft Zürich, 85, 165–177 (1940).
4. WAERDEN, B. L. v. d., Moderne Algebra.
5. ———, Einführung in die algebraische Geometrie.