NOTE ON ARTIN'S SOLUTION OF HILBERT'S 17TH PROBLEM

BY D. W. DUBOIS

Communicated by R. S. Pierce, March 15, 1967

A uniquely orderable field F and a polynomial $f(X)$ over F are constructed in such a manner that $f(X)$, though positive at every point of F, is not a sum of squares of elements of the rational function field $F(X)$.

Artin's solution of Hilbert's problem asserts [2] that if a rational function assumes no negative values then it is a sum of squares, provided the coefficient field has exactly one order and that order is Archimedean; in Hilbert's formulation the coefficients are rational numbers. For definitions and a more detailed proof of Artin's theorem see Jacobson [6, Chapter VI]. Our example shows that the Archimedean hypothesis in Artin's theorem is not superfluous, contrary to Corollary 2, p. 278 of [8].

Let Q be the field of all rational numbers, let t be an indeterminate, let $Q(t)$ be ordered so that t is positive and infinitesimal and let K be a real closure of $Q(t)$. Let F be the field over $Q(t)$ consisting of all elements of K obtainable from $Q(t)$ by means of a finite sequence of rational operations and square root extractions, exactly as in ruler and compass considerations. Since every positive element of F has its square roots in F, *F has exactly one order*. Set [1, p. 115]

$$f(X) = (X^3 - t)^2 - t^3,$$

where X is a variable. Then *$f(X)$ is not a sum of squares in $F(X)$* (nor even in $K(X)$), since $f(1)$ and $f(t^{1/3})$ have opposite signs. Now we shall show that *$f(X)$ is positive as a function on F*. It has long been known [4], [7] that the ring B of all finite elements of K (u is *finite* if $|u| < n$ for some integer n) is a valuation ring in K. The induced valuation v is a measure of order of magnitude, the significance of $v(a) < v(b)$ being that $a^{-1}b$ is infinitesimal. Denoting by G the value group of K written in additive notation, and observing that G is a torsionfree abelian group, we shall show that G may be identified with (the additive group of) Q, with $v(t) = 1$. The ramification relation $ef \leqq n$ [3, p. 122], together with the algebraic character of K over $Q(t)$, implies that the rank of G is one. Hence [5, §42] G can be embedded in Q so that $v(t)$ maps onto 1; moreover K contains nth roots of t for all n; so the embedding is onto. In other words G can be identified, and now will