PACIFIC JOURNAL OF MATHEMATICS
Vol. 74, No. 1, 1978

ALGEBRAIC NUMBERS, A CONSTRUCTIVE DEVELOPMENT

W. JULIAN, R. MINES AND F. RICHMAN

The theory of algebraic numbers is developed in the context of abstract fields with equality and inequality. Of classical interest is that any commutative local ring without nilpotent elements may be considered a field in this context. Procedures are given for deciding whether two complex algebraic numbers are equal or not, for factoring polynomials over algebraic number fields and for deciding whether a given algebraic number is in a given algebraic number field.

The purpose of this paper is to provide a constructive development of algebraic numbers, that is, complex roots of nonzero polynomials with rational coefficients. The constructive theory of complex numbers that we need is provided by Bishop [1]. For simplicity and power we use an axiomatic definition of a field with equality and inequality modeled on Bishop's complex numbers. By using conventional notation we make the subject appear similar to the classical development, while retaining the constructive finitistic interpretation.

A side effect of this axiomatic approach is that our fields can be interpreted classically as commutative local rings without nilpotent elements, with the maximal ideals consisting of those elements that are not different from zero. This gives some classical insight into the constructivist's notion of numbers that are not known to be zero or to be different from zero, and clarifies the problems that the constructivist faces in proving theorems about fields. Heyting [3] and others have given intuitionistic axioms for fields before but their axioms are more restrictive and their development emphasizes logical subtleties.

The real, complex, and p-adic numbers, as developed by Bishop, are examples of fields with elements x and y for which one can neither assert $x = y$ nor assert $x \neq y$. A field having the property that for each pair of elements x and y either $x = y$ or $x \neq y$ is called a *discrete field*. One might think that classical field theory would go through *in toto* for discrete fields, but this is not the case. For example, the characteristic of a discrete field need not be ∞ or a finite prime number, and it is not always possible to factor a polynomial into a product of irreducible polynomials.

Some peculiarly constructive questions about algebraic numbers which we shall consider are: