

# FIELDS DEFINED BY POLYNOMIALS

LOWELL A. HINRICHS, IVAN NIVEN AND C. L. VANDEN EYNDEN

**1. Introduction.** First we consider the following question, where  $F$  is any field. For what pairs  $P$  and  $Q$  of polynomials in two variables with coefficients in  $F$  do the definitions

$$(I) \quad a \oplus b = P(a, b), \quad a \odot b = Q(a, b),$$

for all  $a$  and  $b$  in  $F$  yield a field  $(F, \oplus, \odot)$ ? It turns out that the answer is different for infinite fields than for finite fields, as shown in §§ 2 and 3.

Next let  $R$  be the field of real numbers. For what quadruples  $P_1, P_2, Q_1, Q_2$  of real polynomials in four variables is  $(R \times R, \oplus, \odot)$  a field, when we set

$$(II) \quad \begin{aligned} (a, b) \oplus (c, d) &= (P_1(a, b, c, d), P_2(a, b, c, d)), \\ (a, b) \odot (c, d) &= (Q_1(a, b, c, d), Q_2(a, b, c, d)), \end{aligned}$$

where  $(x, y)$  denotes an ordered pair of real numbers? This question is partially answered in §§ 4 and 5, and in § 6 it is shown that the polynomials may be of arbitrarily high degree. In § 7 it is proved that if definitions (II) do give a field, it must be isomorphic to the field of complex numbers.

## 2. The one-dimensional case.

**THEOREM 1.** *Let  $F$  be an infinite field. The system  $(F, \oplus, \odot)$  in (I) is a field if and only if*

$$(1) \quad \begin{aligned} P(a, b) &= a \oplus b = a + b + \gamma \\ Q(a, b) &= a \odot b = \gamma\sigma(a + b) + \sigma ab + \gamma^2\sigma - \gamma, \end{aligned}$$

where  $\gamma \in F$ ,  $\sigma \in F$  and  $\sigma \neq 0$ . When these conditions are satisfied the field  $(F, \oplus, \odot)$  is isomorphic to  $F$ , thus  $(F, \oplus, \odot) \cong (F, +, \cdot)$ .

*Proof.* We first assume that  $(F, \oplus, \odot)$  is a field and show that the polynomials  $P$  and  $Q$  have the prescribed form. By associativity we have  $P(P(a, b), c) = P(a, P(b, c))$  identically in  $a, b, c$ . Now if  $P$  is of degree  $n$  in  $a$ , the degrees of the left and right sides of this identity in  $a$  are  $n^2$  and  $n$  respectively. Since  $F$  is infinite it follows

---

Received November 12, 1962, and in revised form June 14, 1963. The first author listed was supported by NSF contract G 19859, the other two authors by NSF contract G 19016.