MULTIPLICATION FROM OTHER OPERATIONS

S. KOHN AND D. J. NEWMAN

Abstract. Given the operations of subtraction and reciprocal-taking we show that the operation of multiplication is determined in any field. The amusing difference is that for characteristic 2 it is not given by a formula while for other characteristics, it is.

The identity
\[ xy = ((x + y - 2)^{-1} - (x + y + 2)^{-1})^{-1} - ((x - y - 2)^{-1} - (x - y + 2)^{-1})^{-1} \]
shows how multiplication of real numbers is determined from the operation of subtraction and the taking of reciprocals. In more colorful language: a machine which can perform subtractions and take reciprocals can be programmed to multiply. (The cases of 0 denominators being easily interpreted.)

The formula, (1), is in fact valid in a much wider setting. It holds (with the previously mentioned conventions) in any field of characteristic not 2. In a field of characteristic 2, however, it is totally useless and meaningless and the question arises as to what happens in such fields. The answer is somewhat surprising. In a field of characteristic 2:

(2)

The operations of subtraction and taking reciprocals do determine multiplication,

but

(3)

there is no formula for the product in terms of iterated subtractions and reciprocals!

To prove (2) observe first the identity
\[ x^2 = x + \frac{1}{\frac{1}{x} + \frac{1}{1 + x}} \]
which shows that the square of every element is determined (the square of 0 being 0 and of 1 being 1).
Next note that the equation

\[ \frac{1}{t + x^2} + \frac{1}{t + y^2} + \frac{1}{t} = 0 \]

has the unique solution \( t = xy \) (unless \( x \) or \( y \) is 0 or 1 in which case the product is determined anyway). (4) and (5) together, then, prove that \( xy \) is determined. To prove (3) we consider the set, \( \overline{A} \), obtained from the symbols \( x, y, 1 \) by applying the operation of subtraction and the taking of reciprocals and reducing coefficients (mod 2). \( S \) will then consist of certain rational functions and it is our purpose to prove that \( xy \in \overline{A} \).

Consider in fact the set, \( B \), of rational functions, \( (P(x, y)/Q(x, y)) \) (mod 2), with the property that \( P(x, y)Q(x, y) \) has no terms \( x^m y^n \) with both \( m \) and \( n \) odd. This definition is meaningful since \( PR \cdot QR \) has the property iff \( P \cdot Q \) does. We show

\[ \overline{A} = B. \]

First we show that \( S \subseteq T \). (Actually this is all that is necessary to establish (3) but we will include the other inclusion for the sake of completeness.)

Clearly \( 1, x, y \in T \) and \( B \) is closed under reciprocals. That it is closed under addition can be seen also. Namely let \( P/Q \in \overline{B}, R/S \in \overline{B} \), their sum is \( (PS + QR)/QS \) and we examine \( (PS + QR)QS = PQ \cdot S^2 + RS \cdot Q^2 \). By hypothesis neither of these terms contains a monomial with both exponents odd. Thus their sum contains no such monomial and so indeed \( P/Q + R/S \in \overline{B} \). The proof is complete.

Finally we prove that \( T \subseteq S \), we have

\[ x^2 y = x + \frac{1}{\frac{1}{x} + \frac{1}{y}} \]

and so we may conclude that

\[ R, S \in \overline{A} \Rightarrow R^2 A \subseteq S. \]

From this we conclude inductively that \( x^m, y^n \in S \) for all \( m, n \).

This fact again combined with (8) yields

\[ x^{2m} y^n \quad \text{and} \quad x^m y^{2n} \]

and in particular
(10) the square of any polynomial is in $\mathbb{A}$.

Now let $P/Q \in \mathbb{B}$. Then each term of $P \cdot Q$ is either of the form $x^{2m}y^n$ or $x^m y^{2n}$. Clearly this continues to hold for $P \cdot Q^2$ and so, by (9), we conclude that $P \cdot Q^2 \in \mathbb{A}$. By (10), however, $Q^2 \in \mathbb{A}$ and so by (8) we find that $P \cdot Q^3 \cdot (1/Q^2)^2 \in \mathbb{A}$. Since this is equal to $P/Q$ we are done.

Belfer Graduate School of Science, Yeshiva University, New York, New York 10033