

THE SQUARE ROOT AND THE RELATIONS OF ORDER*

BY

OSWALD VEBLEN

One of the most obvious discriminations between positive and negative numbers is that the former possess square roots in the field of reals while the latter do not. This distinction, however, has not yet been used in any of the current systems of postulates. On the contrary, an order relation, $<$, is usually introduced as an undefined symbol.

Though the existence of a square root cannot be deduced from order relations without the use of a continuity assumption of some sort, it turns out to be very easy to infer the order relations from postulates about the existence of a square root. Suppose we are given a field, defined by one of the numerous sets of postulates published in the *Transactions* by HUNTINGTON, MOORE and DICKSON. This field contains a unique mark, 0, such that $x + 0 = x = 0 + x$ for every mark x , and a unique mark, 1, such that $1x = x$ for every mark x . A mark, a , is called a square if there exists a mark, x , such that $xx = a$. If not a square, a mark is called a not-square. Now add the postulates: †

α) The mark -1 is a not-square.

β) If marks x and y are not-squares, then $x + y$ is a not-square.

The postulate *α)* shows that the marks 2 and 0 are distinct and thus that division by 2 is possible.

Theorem 1. If x and x' are such that $x + x' = 0$, then either x or x' is a square, whereas the other is a not-square.

Proof. If x and x' were both not-squares, then by *β)*, $x + x'$ would be a not-square, whereas zero is a square. The mark $x' = -1 \cdot x$ and hence by the theorem that the product of a square and a not-square is a not-square, if one of the marks x , x' is a square the other is a not square.

Theorem 2. If x and y are squares, then $x + y$ is a square.

* Presented to the Society (Chicago) April 22, 1905. Received for publication November 20, 1905.

† That these postulates are independent is shown by the examples:

α) Any Galois field, $GF(2^n)$.

β) Any Galois field, $GF(p^n)$, where $p > 2$.

Proof. The marks $-x$ and $-y$ are not-squares; hence

$$(-x) + (-y) = -(x + y)$$

is a not-square; and hence, by theorem 1, $x + y$ is a square.

Definition. If and only if the mark $a - b$ is a square which is not zero, $a > b$. If and only if the mark $a - b$ is a not-square, $a < b$.

Theorem 3. If $a \neq b$, either $a > b$ or $a < b$. If $a > b$ then $b < a$; if $a < b$ then $b > a$. If $a < b$ or $b < a$, then $a \neq b$. The inequalities $a > b$ and $a < b$ cannot both be true.

These statements are all evident consequences of the definition and the fact that $a - b$ is either a square or a not-square and cannot be both.

Theorem 4. If $a > b$ and $b > c$, then $a > c$.

Proof. By hypothesis, $a - b$ and $b - c$ are both squares. Hence, by theorem 2, $(a - b) + (b - c) = a - c$ is also a square.

Theorem 5. If $a < b$, then there is a mark, c , such that $a < c$ and $c < b$. Likewise for any mark, a , there are marks d and e such that $a < d$ and $e < a$.

Proof. The mark $d = (b - a)/2$ must, by hypothesis and theorem 2, be a square. Hence $a + d > a$ and $b = a + 2d > a + d$. So we have $a + d$ as the mark, c , required by the first part of the theorem. The rest of the theorem is proved in a similar way.

Theorem 6. If $a > 0$ and b is any mark, $a + b > b$. If $a < 0$ and b is any mark, $a + b < b$.

Proof. In the first case, $a + b - b = a > 0$, and in the second case, $a + b - b = a < 0$.

Theorem 7. If $a > 0$ and $b > 0$, then $ab > 0$. If $a < 0$ and $b > 0$, then $ab < 0$. If $a < 0$ and $b < 0$, then $ab > 0$.

Proof. These three statements are direct consequences of the propositions that the product of two squares is a square, that the product of a square and a not-square is a not-square and that if b is a square $-1 \cdot b$ is a not-square. The corollary is direct that if $a > 0$ and $b > 1$, $ab > a$. For, writing b in the form $1 + e$, $a(1 + e) - a = ae$ is evidently a square.

It is now evident, on comparison, for instance, with HUNTINGTON'S set of postulates for real algebra on page 39, volume 6 of this journal, that our field satisfies all the conditions of the real number system except that of continuity. We therefore suggest as an elegant way of stating the postulates for the real number system in terms of the undefined symbols, $+$ and \times , a set consisting of postulates for a field in general, postulates α) and β), and a continuity postulate. This latter might take the form:

If $[a]$ and $[b]$ are two sets of marks such that $a - b$ is for every a of $[a]$ and b of $[b]$ a square, not zero, then there exists a mark d such that for every a of $[a]$, $a - d$ is a square and for every b of $[b]$, $d - b$ is a square.

What may be thought of as the geometric analogue of the above determination of order relations has been carried out by M. PIERI on page 24 of his paper, *I Principii della Geometria di Posizione*, published in the *Memorie dell' Accademia Reale delle Scienze di Torino* for 1898. Two point-pairs, AB and CD , are said not to separate or to separate according as there exist or do not exist two points H, H' which are harmonically conjugate both with respect to AB and to CD . Determining the points HH' is equivalent to finding the double points of the involution in which AB and CD are pairs of conjugate points and is therefore a problem of the second degree.
