$$(5)\qquad \begin{aligned} D^2 &= 1 + (y - e^{-1/x^2})(y - 2e^{-1/x^2}), \quad \text{when } x \neq 0\,; \\ D^2 &= 1 + y^2, \quad \text{when } x = 0\,; \end{aligned}$$

which is precisely the function

$$(6)\qquad \begin{aligned} \phi(x, y) &= (y - e^{-1/x^2})(y - 2e^{-2/x^2}), \quad \text{when } x \neq 0\,; \\ \phi(x, y) &= y^2, \quad \text{when } x = 0\,; \end{aligned}$$

increased by unity; the function $\phi(x, y)$ given by (6) has been studied *; it is at a minimum for any analytic curve in the (x, y) plane through the point (0, 0); but it is not at a minimum in the region about (0, 0). Thus even the knowledge that the distance from a point on the normal to a surface is at a minimum at the foot of the normal for every curve cut out of the surface by an analytic cylinder through the normal, does not prove that the same distance is at a minimum for the surface itself.

COLUMBIA, MO.,
January 11, 1908.

A GEOMETRIC REPRESENTATION OF THE GALOIS FIELD.

BY DR. L. I. NEIKIRK.

(Read before the Chicago Section of the American Mathematical Society, March 30, 1907.)

THE roots of irreducible congruences were first introduced into mathematics by Galois.† Various writers since then have contributed to the theory of irreducible congruences and classes of residues.‡ The greatest progress of recent years was made by Moore.§ He proved that any finite abstract field in which division is unique is an abstract form of the Galois field; that its order is the power of a prime p^n, and that for any order it is unique, being independent of the particular irreducible congruence of degree n used in defining it.

* *Annals of Mathematics*, vol. 8, no. 4 (July, 1907), pp. 172–174. The exact significance of "analytic," as here used, is there specified, and a more general statement of the property quoted is given.

† "Sur la théorie des nombres," *Bulletin des Sciences Math.* de M. Ferrussac (1830); also Œuvres mathématiques d'Evariste Galois, Gauthier-Villars, Paris, 1897.

‡ See the preface of Linear Groups by L. E. Dickson.

§ BULLETIN, December, 1893; Chicago Congress Mathematical Papers, pp. 208–242.

More recently Maclagan-Wedderburn* and Dickson proved simultaneously that any finite field is necessarily commutative.

The object of this paper is to put the Galois field — and, by the above, any finite field — in the concrete form of a geometric representation.†

Consider the equation $f(x) = 0$ of degree n and irreducible in the domain of rational numbers. It has a root j which we may represent in the ordinary way on the complex plane. If we plot all the points

$$c_1 j^{n-1} + c_2 j^{n-2} + \cdots + c_{n-1} j + c_n, \tag{1}$$

the c's being integers, we get a complete geometric representation of the integers of the algebra defined by $f(x) = 0$. This set of points is closed with regard to the ordinary geometric forms of the rational operations addition, subtraction, multiplication, but not division.

The following theorem is due to Jacobi:‡

If the vectors $\omega_1, \omega_2, \cdots, \omega_r$ $(r > 2)$ are not connected by some relation of the form

$$m_1\omega_1 + m_2\omega_2 + \cdots + m_r\omega_r = 0,$$

then integral values of the m's can be chosen making

$$|m_1\omega_1 + m_2\omega_2 + \cdots + m_r\omega_r| < \epsilon,$$

where ϵ may be any arbitrarily small positive quantity.

By this theorem all the points of the set (1) for $n > 2$ are limiting points, and the set forms an enumerable assemblage, dense around its own points.

Consider the Galois field defined by the irreducible congruence $f(x) \equiv 0 \pmod{p}$.§ We apply to this the representation given by (1) by distinguishing two kinds of points, viz., reduced points for which the c's are positive and less than p, and the remaining points called congruent points.‖ In particular, the points

$$(\bar{c}_1 + k_1 p) j^{n-1} + (\bar{c}_2 + k_2 p) j^{n-2} + \cdots + (\bar{c}_{n-1} + k_{n-1} p) j + (\bar{c}_n + k_n p)$$

* *Transactions Amer. Math. Society*, vol. 6 (1905), pp. 349-352.

† The geometric representation of residues to a prime modulus $(n = 1)$ is given by Dickson, Linear Groups, p. 3, and will not be considered here.

‡ Ges. Werke, vol. 2, pp. 27-32; also see Clebsch and Gordan's Theorie der Abel'schen Functionen, § 38.

§ This constitutes a farther restriction on $f(x)$.

‖ The exceptional case $x^2 + x + 1 \equiv 0 \pmod{2}$ noted by Galois (Works, footnote p. 17) is only an apparent and not a real exception here.

are said to be congruent to each other and to the reduced point

$$\bar{c}_1 j^{n-1} + \bar{c}_2 j^{n-2} + \cdots + \bar{c}_{n-1} j + \bar{c}_n.$$

When two reduced points are combined by the geometric forms of addition, subtraction, and multiplication the result is in general a point of set (1), not a reduced point but congruent to some definite third reduced point. This gives a geometric interpretation of the above three rational operations in the Galois field.

Let ω be a primitive root among the reduced points. Consider the points

$$\omega, \omega^2, \cdots, \omega^{p^n-1} \ (\equiv 1); \tag{2}$$

no two of these are congruent points. The quotient of two of these, $\omega^s \div \omega^r = \omega^{s-r}$ $(s > r)$, gives a definite point in set (2). If $r > s$, it will be necessary to multiply ω^s by ω^{p^n-1} before performing the operation of division.

The geometric operation of division in the Galois field is performed in the following manner. Points in set (2) congruent to the two reduced points given are combined by the ordinary geometric form of division; the resulting point of set (2) is congruent to a definite third reduced point. This completes the four rational operations in the Galois field.

Only a limited number of points of set (1) are used in all possible operations between the reduced points. This geometric representation of the Galois field is not unique, as an indefinitely large number of choices of j may be made. In particular, we may always chose j real if we wish, as is always possible, to make the constant term of $f(x)$ negative.

If $j = \rho(\cos\theta + i \sin\theta) = \rho\epsilon^{i\theta}$, then the elements of the Galois field are given in the form

$$\bar{c}_1 \rho^{n-1} \epsilon^{i(n-1)\theta} + \bar{c}_2 \rho^{n-2} \epsilon^{i(n-2)\theta} + \cdots + \bar{c}_{n-1} \rho \epsilon^{i\theta} + \bar{c}_n.$$

UNIVERSITY OF ILLINOIS,
URBANA, ILL.