AN INVARIANTIVE INVESTIGATION OF IRREDUCIBLE BINARY MODULAR FORMS*

BY

LEONARD EUGENE DICKSON

1. A fundamental system of invariants of the group of all binary linear transformations in a finite field is shown in §§ 2–6 to consist of two invariants, one the product of the distinct linear forms and the other the product of the distinct irreducible quadratic forms, where in each case no two factors have a constant ratio. The product π_m of the irreducible forms of degree m can be expressed in terms of the fundamental invariants; this is accomplished in §§ 7–9 by means of the remarkable three-term recursion formula (15).

Two forms shall be said to belong to the same class if and only if one of them can be transformed into a constant multiple of the other by a linear transformation of determinant unity in the field. It is shown in § 10 that there are as many classes of irreducible binary forms of degree m as there are irreducible factors of π_m when expressed as a function of a certain pair of invariants. The choice of the latter is different in the two cases $p = 2$, $p > 2$, where p is the modulus of the field; this is due to the fact that, in the respective cases, there are one or two similarity transformations of determinant unity. The investigation is completed for the values of m less than 8. The difficulties encountered increase as the number of factors of m increases. Certain problems arise for which the present invariantive theory affords an indirect solution, whereas a direct solution appears to be quite difficult (cf. end of § 10, and end of § 17). For $m = 6$, it was necessary to enumerate the irreducible cubics in the $GF[p^n]$ whose roots are squares in the $GF[p^{3n}]$ and have a given sum.

Determination of a Fundamental System of Invariants, §§ 2–6.

2. Let G be a group of finite order g composed of linear homogeneous transformations on $m\,(m > 1)$ variables with coefficients in any given field F. The term point will be used in the sense of homogeneous coördinates, so that $(x_1, \cdots, x_m)$ is identified with $(\mu x_1, \cdots, \mu x_m)$, while $(0, \cdots, 0)$ is excluded.

* Presented to the Society, September 7, 1910.

A transformation which leaves every point unaltered is necessarily a similarity transformation

$$x_i' = ax_i \qquad (i=1, \cdots, m). \tag{1}$$

In fact, by employing the points all but one of whose coördinates are zero, we see that the transformation is of the form

$$x_i' = a_i x_i \qquad (i=1, \cdots, m).$$

Then by employing the points all but two of whose coördinates are zero, we see that the a_i are equal. Let γ be the number of transformations (1) contained in G, and set $\omega = g/\gamma$. We assume that $\omega > 1$. Any point is one of at most ω distinct conjugates under G. A point is called special if it is one of fewer than ω conjugates, that is, if it is invariant under at least one transformation other than (1) of the group G. If a point P is invariant under T and if S replaces P by P', then P' is invariant under $S^{-1}TS$. To determine all special points it therefore suffices to employ a representative of each set of conjugate transformations other than (1), obtain the points invariant under the representative, select the distinct points so obtained, and find the conjugates to each under G.

3. Let G be the group of all binary linear homogeneous transformations of determinant unity in the Galois field $GF[p^n]$ of order p^n. The order of G is

$$g = p^n(p^{2n}-1). \tag{2}$$

Within G any transformation with irreducible characteristic determinant $\Delta(\rho)$ is equivalent to a transformation *

$$T = \begin{pmatrix} \alpha & -1 \\ 1 & 0 \end{pmatrix}, \qquad \Delta(\rho) = \rho^2 - \rho\alpha + 1.$$

The only points invariant under T are $(\rho, 1)$, where $\Delta(\rho) = 0$. The transformations of G which leave $(\rho, 1)$ unaltered are

$$\begin{pmatrix} b & -c \\ c & b-c\alpha \end{pmatrix}, \qquad b^2 - \alpha bc + c^2 = 1,$$

namely, the transformations commutative with T. The quadratic condition may be written in the form

$$(b-\rho c)^{p^n+1} = 1,$$

where ρ is a root of $\Delta(\rho) = 0$, and hence has p^n+1 sets of solutions in the $GF[p^n]$. Thus $(\rho, 1)$ is one of $p^{2n}-p^n$ conjugate points under G. The resulting system of special points is therefore $(e\rho+f, 1)$, where e is any element

* These Transactions, vol. 2 (1901), p. 117.

$\neq 0$ of the $GF[p^n]$ and f is any element. Such a point together with $(e\bar{\rho}+f, 1)$, where $\bar{\rho}$ is the second root of $\Delta(\rho)=0$, determine a quadratic form $x^2+\cdots$ which vanishes only for these two points. Hence a relative invariant under G is given by the product Q of the $\frac{1}{2}(p^{2n}-p^n)$ irreducible quadratic forms $x^2+\cdots$. We have *

$$Q=\frac{x^{p^{2n}-1}-y^{p^{2n}-1}}{x^s-y^s}=\sum_{j=0}^{p^n} x^{s(p^n-j)}y^{sj} \qquad (s=p^n-1). \tag{3}$$

Consider next a transformation S for which

$$\Delta(\rho)=(\rho-\kappa)(\rho-\kappa^{-1}),$$

where κ is in the $GF[p^n]$. There exists a linear function l which S replaces by κl. If $\kappa^2\neq 1$, S is therefore equivalent within G with $\left(\begin{smallmatrix}\kappa & 0\\ 0 & \kappa^{-1}\end{smallmatrix}\right)$, which leaves only (1, 0) and (0, 1) unaltered. If $\kappa^2=1$, S is equivalent to

$$S_\beta=\begin{pmatrix}\pm 1 & 0\\ \beta & \pm 1\end{pmatrix}.$$

Since S_0 is of type (1), we may set $\beta\neq 0$; then S_β leaves only $(0,1)$ invariant. Hence when $\Delta(\rho)$ is reducible, the resulting system of special points is composed of the p^n+1 points $(1,0)$ and $(a,1)$, where a ranges over the field. There results the relative invariant

$$L=y\prod_a(x-ay)=x^{p^n}y-xy^{p^n}. \tag{4}$$

4. **Lemma.** *If an integral function is invariant under the group G of all m-ary linear homogeneous transformations of determinant unity in the $GF[p^n]$, it is an absolute invariant of G.*

The group G is generated † by transformations of the type $B_{rs\lambda}$, which alters only one variable x_r, replacing it by $x_r+\lambda x_s$. If B multiplies a function by μ, B^p multiplies it by μ^p. Now B is of period p. Hence $\mu^p=1$. Employing the power p^{n-1}, we get

$$\mu^{p^n}=\mu=1.$$

5. We may now prove that any integral invariant I of the binary group G is an integral function of the invariants Q and L. If I vanishes for a special point it has the factor Q or L. It remains to investigate the invariants I which vanish for no special point. The number of transformations (1) contained in G is

$$\gamma=1 \text{ if } p=2, \qquad \gamma=2 \text{ if } p>2. \tag{5}$$

* DICKSON, *Linear Groups* (Leipzig, 1903), page 17.

† *Linear Groups*, page 78.

Any non-special point is one of $\omega = g/\gamma$ conjugates under G. Now the forms

$$q = Q^{(p^n+1)/\gamma}, \qquad l = L^{p^n(p^n-1)/\gamma} \tag{6}$$

are of degree ω. Let F_{p^n} be the field composed of all roots of all algebraic equations with coefficients in the $GF[p^n]$. The invariant I vanishes for a set of ω conjugate points; if (c, d) is one of these points, the ratio $c:d$ belongs to the field F_{p^n}. Hence we can determine τ in the latter field such that $q(c, d) + \tau l(c, d) = 0$. Thus I has the factor $q + \tau l$, and I is a product of such linear functions of q, l. If I has its coefficients in the $GF[p^n]$, and τ is a root of an equation of degree t irreducible in the $GF[p^n]$, the presence of the factor $q + \tau l$ in I implies that of the conjugate factors $q + \tau^{p^{nt}} l$ and hence of a function of degree t in q and l with coefficients in the $GF[p^n]$.

Theorem. *Any integral invariant with coefficients in the $GF[p^n]$ of the binary group G is an integral function of Q and L with coefficients in the $GF[p^n]$.*

6. The transformation which leaves y unaltered and replaces x by Dx, where $D^s = 1$, leaves Q unaltered and replaces L by DL. Hence Q is an absolute invariant and L a relative invariant of weight unity under the group G' of all binary transformations in the $GF[p^n]$. Hence *any absolute invariant of G' is expressible in terms of Q and L^s, where $s = p^n - 1$.*

The invariants π_m $(m > 2)$ investigated in § 7 are absolute invariants under G' which vanish for no special points. Hence they are expressible in terms of invariants (6) in such a manner that, for $p > 2$, l occurs only to even powers, and in view of the homogenity q occurs only to even powers. Hence, for any p, they are expressible in terms of J and K, where

$$J = Q^{p^n+1}, \qquad K = L^{sp^n}. \tag{7}$$

The Invariants π_m as Functions of the Fundamental Invariants, §§ 7–9.

7. For $m > 1$, let π_m denote the product of all binary forms of degree m which are irreducible in the $GF[p^n]$ and have unity as the coefficient of x^m. Let

$$m = q_1^{r_1} q_2^{r_2} \cdots q_\mu^{r_\mu}, \tag{8}$$

where $q_1, \cdots, q_\mu$ are the distinct prime factors > 1 of m. Set

$$F_t = \frac{x^{p^{nt}-1} - y^{p^{nt}-1}}{x^s - y^s} \qquad (s = p^n - 1). \tag{9}$$

Thus $F_1 = 1$, $F_2 = Q$. It follows readily from *Linear Groups*, page 18, that

$$\pi_m = \frac{F_m \Pi F_{m/q_iq_j} \Pi F_{m/q_iq_jq_kq_l} \cdots}{\Pi F_{m/q_i} \Pi F_{m/q_iq_jq_k} \cdots}, \tag{10}$$

in which the first product in the numerator extends over the $\frac{1}{2}\mu(\mu-1)$ combinations of $q_1, \cdots, q_\mu$ two at a time, and similarly for the remaining products. By § 6, $\pi_m (m>2)$ is an integral function of J and K of degree

$$d_m = \frac{p^{nm} - \sum p^{\frac{nm}{q_i}} + \sum p^{\frac{nm}{q_i q_j}} - \sum p^{\frac{nm}{q_i q_j q_k}} + \cdots}{p^n(p^{2n}-1)}, \tag{11}$$

For example, if m is an odd prime,

$$\pi_m = F_m, \; d_m = \frac{p^{n(m-1)}-1}{p^{2n}-1} \qquad (m \text{ an odd prime}). \tag{12}$$

8. Since $d_3 = 1$, $\pi_3 = F_3$ is a linear function of J and K. By (3),

$$Q^{p^n} = \sum_{k=0}^{p^n} x^{sp^n(p^n-k)} y^{skp^n}.$$

Hence by (5),

$$J = \sum_{j,\,k=0}^{p^n} x^{s(p^{2n}+p^n-t)} y^{st} \qquad (t = kp^n + j). \tag{13}$$

The terms of (13) given by $j = p^n$ and $k < p^n$ are

$$\sum_{k=0}^{s} x^{s(p^{2n}-kp^n)} y^{sp^n(1+k)} = \sum_{k=0}^{s} x^{p^{2n}(s-k)+kp^n} y^{kp^{2n}+p^n(s-k)}.$$

But every coefficient in the expansion of $(a-b)^s$ is congruent to unity modulo p. Hence the preceding sum equals, in the field,

$$(x^{p^{in}} y^{p^n} - x^{p^n} y^{p^{2n}})^s = (L^{p^n})^s = K. \tag{14}$$

Next the terms of (13) with $k = p^n$ are

$$\sum_{j=0}^{p^n} x^{s(p^n-j)} y^{s(p^{2n}+j)} = \sum_{\tau=p^{2n}}^{p^{2n}+p^n} x^{s(p^{2n}+p^n-\tau)} y^{s\tau}.$$

When the last sum is combined with the terms of (13) given by $j < p^n$, $k < p^n$, and hence by $t = 0, 1, \cdots, p^{2n}-1$, we get

$$\sum_{t=0}^{p^{2n}+p^n} x^{s(p^{2n}+p^n-t)} y^{st} = \frac{x^{p^{3n}-1} - y^{p^{3n}-1}}{x^s - y^s} = F_3.$$

It follows that $\pi_3 = J - K$.

9. We make use of the following identity:

$$(x^{sp^n} - y^{sp^n})(x^{p^{tn}-1} - y^{p^{tn}-1}) = (x^{p^{2n}-1} - y^{p^{2n}-1})(x^{p^{tn}-p^n} - y^{p^{tn}-p^n}) - (xy)^{sp^n}(x^s - y^s)(x^{p^{tn}-p^{2n}} - y^{p^{tn}-p^n}),$$

where $s = p_n - 1$. We divide by $(x^s - y^s)(x^{sp^n} - y^{sp^n})$ and insert the factor $x^{sp^{2n}} - y^{sp^{2n}}$ in the numerator and denominator of the last term. By (14),

$$\frac{(xy)^{sp^n}(x^{sp^{2n}} - y^{sp^{2n}})}{x^{sp^n} - y^{sp^n}} = (xy)^{sp^n}(x^{sp^n} - y^{sp^n})^{p^n-1} = (x^{p^{2n}}y^{p^n} - x^{p^n}y^{p^{2n}})^s = K.$$

Hence we obtain the recursion formula

$$F_t = QF_{t-1}^{p^n} - KF_{t-2}^{p^{2n}} \qquad (F_1 = 1,\ F_2 = Q). \tag{15}$$

Taking $t = 3$ and applying (7) and (12), we get

$$\pi_3 = F_3 = J - K, \tag{16}$$

in agreement with § 8. By (10) and (15) for $t = 4$,

$$\pi_4 = F_4/Q, \qquad F_4 = QF_3^{p^n} - KQ^{p^{2n}}.$$

Applying (16) and (7) we get

$$\pi_4 = J^{p^n} - J^{p^n-1}K - K^{p^n}. \tag{17}$$

In a similar manner,

$$\pi_5 = J^{p^{2n}+1} - J^{p^{2n}}K - J^{p^{2n}-p^n+1}K^{p^n} - JK^{p^{2n}} + K^{p^{2n}+1}, \tag{18}$$

$$\pi_6 = J^{p^{3n}+p^n-1} - J^{p^{3n}-p^{2n}+p^n-1}K^{p^{2n}} - J^{p^n-1}K^{p^{3n}} - K^{p^n}\left(\frac{J^{p^{3n}} - K^{p^{3n}}}{J - K}\right), \tag{19}$$

$$\pi_7 = J^{p^{2n}-p^n+1}(J^{p^n} - K^{p^n})(J^{p^{4n}} - J^{p^{4n}-p^{3n}}K^{p^{3n}} - K^{p^{4n}}) - JK^{p^{2n}}(J^{p^{4n}} - K^{p^{4n}}) - K\pi_5^{p^{2n}}. \tag{20}$$

The Number of Classes of Irreducible Forms of Degree m, §§ 10–17.

10. Let $\phi(x, y) = x^m + \cdots$ be an irreducible binary form in the $GF[p^n]$. Let $\phi_1 = \phi, \phi_2, \cdots, \phi_k$ be the distinct forms having unity as the coefficient of x^m which are equivalent to a constant multiple of ϕ under the group G of determinant unity. By § 4, the product $P_m = \phi_1 \cdots \phi_k$ is an absolute invariant of G. By § 5, if $m > 2$, P_m is an integral function with coefficients in the $GF[p^n]$ of the invariants q and l, defined by (6). The function $P_m(q, l)$ is obviously irreducible in the field.

Two binary forms shall be said to belong to the same class if and only if one of them is equivalent to a constant multiple of the other under the group G of all binary transformations in the $GF[p^n]$ of determinant unity.

The preceding remarks lead to the

Theorem. *There are as many classes of irreducible binary forms of degree m as there are irreducible factors in the $GF[p^n]$ of the invariant $\pi_m(q, l)$.*

To decide whether or not two given forms ϕ and ψ belong to the same class, we employ a root $\rho = x/y$ of $\phi = 0$ and a root $\sigma = x/y$ of $\psi = 0$, each belonging to the $GF[p^{nm}]$, and determine the values of q/l for $x/y = \rho$ and σ, respectively. According as these values of q/l are the roots of the same factor or different irreducible factors of $\pi_m(q, l)$, the given forms ϕ and ψ belong to the same or different classes.

Since these values of q/l belong to the $GF[p^{nm}]$, *the irreducible factors of* $\pi_m(q, l)$ *are of degree* m *or a divisor of* m.

11. We proceed to the investigation of the irreducible factors of the function $\pi_m(J, K)$ when $p = 2$, and those of this function with J and K replaced by q^2 and l^2 when $p > 2$.

From (16) we conclude that *the cubic forms fall into a single class if* $p = 2$, *and into two classes if* $p > 2$.

For $m = 4$, set $K = \rho J$ in (17). Thus π_4 vanishes only if

$$\rho^{p^n} = 1 - \rho.$$

Then ρ belongs to the $GF[p^{2n}]$ since

$$\rho^{p^{2n}} = 1 - \rho^{p^n} = \rho.$$

For $p = 2$, ρ does not belong to the $GF[2^n]$. Hence π_4 is the product of 2^{n-1} irreducible quadratic factors

$$(K - \rho J)(K - \rho^{p^n} J) = K^2 - KJ + tJ^2,$$

where

$$t = \rho^{p^n+1} = \rho - \rho^2. \tag{21}$$

Hence,* for $p = 2$, t must be a root of

$$t + t^2 + t^4 \cdots + t^{2^{n-1}} = 1. \tag{22}$$

The latter has 2^{n-1} roots in the $GF[2^n]$. Thus, *for* $p = 2$, *the quartic forms fall into* 2^{n-1} *classes differentiated by the roots of* (22).

Next, let $p > 2$. The only value of ρ in the $GF[p^n]$ is $\rho = \frac{1}{2}$. The corresponding factor $q^2 - 2l^2$ is reducible if $p^n = 8l \pm 1$, irreducible if $p^n = 8l \pm 3$. For the remaining $p^n - 1$ values of ρ, $\rho^2 - \rho + t$ is irreducible, so that t has the $\frac{1}{2}(p^n - 1)$ values in the $GF[p^n]$ for which $1 - 4t$ is a not-square. For $l/q = \lambda$, we have $\lambda^2 = \rho$. Now λ will belong to the $GF[p^n]$ only when ρ is a square in the latter field and hence, by (21), only when

$$t^{(p^n-1)/2} = \rho^{(p^{2n}-1)/2} = 1.$$

* In accord with *Linear Groups*, p. 29, formula (23) for $\lambda = \nu = 1$, $p = 2$.

The condition is therefore that t be a square in the $GF[p^n]$. The number of squares t for which $1-4t$ is a not-square is $\frac{1}{4}(p^n-1)$ or $\frac{1}{4}(p^n-3)$ according as -1 is a square or a not-square. Indeed,* $1-\xi^2=\mu\eta^2$, where μ is a not-square, has $p^n\pm 1$ sets of solutions according as -1 is a square or a not-square. The sets $\xi=\pm 1$, $\eta=0$ are here excluded. We have now shown that, when t has any one of the $\frac{1}{2}(p^n-1)$ values for which $\rho^2-\rho+t$ is irreducible in the $GF[p^n]$, $f(\lambda)=\lambda^4-\lambda^2+t$ is irreducible when t is a not-square, but is reducible when t is a square. In the latter case, set $t=\tau^2$. Then the factors of $f(\lambda)$ are

$$\lambda^2\pm\lambda\sqrt{1+2\tau}+\tau, \tag{23}$$

where τ is that square root of t for which $1+2\tau$ is a square. A partial summary of our results for $p>2$ is given in the following table giving the number of irreducible factors of $\pi_4(q, l)$:

p^n	linear	quadratic	quartic	total number
$8k+1$	2	$\frac{1}{2}(p^n-1)$	$\frac{1}{4}(p^n-1)$	$\frac{1}{4}(3p^n+5)$
$8k-1$	2	$\frac{1}{2}(p^n-3)$	$\frac{1}{4}(p^n+1)$	$\frac{1}{4}(3p^n+3)$
$8k+3$	0	$\frac{1}{2}(p^n-1)$	$\frac{1}{4}(p^n+1)$	$\frac{1}{4}(3p^n-1)$
$8k-3$	0	$\frac{1}{2}(p^n+1)$	$\frac{1}{4}(p^n-1)$	$\frac{1}{4}(3p^n+1)$.

In the following examples we give all the irreducible factors:

$p^n=3$. q^2-2l^2, $l^4-l^2q^2-q^4$.

$p^n=5$. q^2-2l^2, $l^2\pm 2lq-q^2$, $l^4-l^2q^2+2q^4$.

$p^n=7$. $q\pm 3l$, $l^2\pm 2lq-2q^2$, $l^4-l^2q^2+tq^4$ $(t=3, 6)$.

$p^n=9$, $i^2\equiv i+1 \pmod 3$. $q\pm(i+1)l$, $l^2\pm ilq-iq^2$, $l^2\pm(2i+1)lq-(2i+1)q^2$, $l^4-l^2q^2+tq^4$ $(t=i, 2i+1)$.

$p^n=11$. q^2-2l^2, $l^2\pm 5lq+q^2$, $l^2\pm 4lq+2q^2$, $l^4-l^2q^2+tq^4$ $(t=6, 7, 8)$.

For $p>2$, the irreducible quartic forms fall into $6k+2$, $6k$, $6k+2$, or $6k-2$ classes, according as $p^n=8k+1$, $8k-1$, $8k+3$, or $8k-3$, respectively.

Classes of Irreducible Quintic Forms.

12. For quintic forms, (18) vanishes for $K=\rho J$ if

$$\rho^{p^{2n}+1}-\rho^{p^{2n}}-\rho^{p^n}-\rho+1=0. \tag{24}$$

* *Linear Groups*, page 46.

As remarked at the end of § 10, each root of (24) belongs to the $GF[p^{5n}]$. We may give a direct proof as follows.

$$\rho^{p^{2n}} = 1 + \frac{\rho^{p^n}}{\rho - 1}, \qquad \rho^{p^{3n}} = 1 + \frac{1}{\rho - 1} + \frac{\rho}{(\rho - 1)(\rho^{p^n} - 1)},$$

$$\rho^{p^{4n}} = 1 + \frac{\rho}{\rho^{p^n} - 1}, \quad \rho^{p^{5n}} = 1 + \frac{\rho^{p^n}}{\rho^{p^n}/(\rho - 1)} = \rho.$$

If a root of (24) belongs to the $GF[p^n]$, it satisfies the equation

$$\rho^2 - 3\rho + 1 = 0. \tag{25}$$

For $p = 2$, a root of (25) satisfies the equation $\rho^3 \equiv 1$ and hence belongs to the $GF[2^n]$ if and only if n is even. *If $p = 2$, the quintic forms fall into $\frac{1}{5}(2^{2n} + 1)$ or $2 + \frac{1}{5}(2^{2n} - 1)$ classes, according as n is odd or even.* For example, the 6 irreducible quintic forms in the $GF[2]$ are equivalent.

For $p > 2$, we must consider (24) for ρ replaced by λ^2. By § 10, the resulting equation for λ has all its roots in the $GF[p^{5n}]$. If one of its roots belongs to the $GF[p^n]$, it must satisfy the equation

$$\lambda^4 - 3\lambda^2 + 1 = (\lambda^2 + \lambda - 1)(\lambda^2 - \lambda - 1) = 0. \tag{25'}$$

Hence $(2\lambda \pm 1)^2 = 5$, so that $p = 5$ or $p^n = 5k \pm 1$. In the respective cases, we obtain the factors $l \pm 2q$ or

$$l + \tfrac{1}{2}(1 \pm \sqrt{5})q, \qquad l - \tfrac{1}{2}(1 \pm \sqrt{5})q.$$

Hence, if $p > 2$, the irreducible factors are of the following types:

p^n	linear	quintic
5^n	2	$2 \cdot 5^{2n-1}$
$5k \pm 1$	4	$\frac{2}{5}(p^{2n} - 1)$
$5k \pm 2$	0	$\frac{2}{5}(p^{2n} + 1)$

For example, if $p^n = 3$, the factors are

$$\lambda^5 - \lambda^4 - \lambda^3 + \lambda^2 + 1, \ \lambda^5 + \lambda^4 - \lambda^3 - \lambda^2 - 1, \ \lambda^5 - \lambda^4 + 1, \ \lambda^5 + \lambda^4 - 1.$$

For $p > 2$, the irreducible quintic forms fall into

$$2(5^{2n-1} + 1), \ 4 + \tfrac{2}{5}(p^{2n} - 1), \ \tfrac{2}{5}(p^{2n} + 1)$$

classes, according as $p = 5$, $p^n = 5k \pm 1$, or $p^n = 5k \pm 2$.

Classes of Irreducible Sextic Forms.

13. For sextic forms, (19) vanishes for $K = \rho J$ if

$$1-\rho^{p^{2n}}-\rho^{p^{3n}}-\rho^{p^{2n}}\left(\frac{1-\rho^{p^{n}}}{1-\rho}\right)=0. \tag{26}$$

For $\rho=1$ the final term is a multiple of p, so that $\rho=1$ is not a root. For $p=2$ or $p=3$, there is no root in the $GF[p^n]$, while for $p>3$, the only root is $\rho=\frac{1}{3}$.

We determine the roots of (26) which belong to the $GF[p^{2n}]$ by a simple device. Any such root satisfies the equation

$$1-\rho-\rho^{p^{n}}=\rho^{p^{n}}\left(\frac{1-\rho^{p^{n}}}{1-\rho}\right). \tag{27}$$

The first member equals its p^n-th power. Hence

$$\rho^n=1-\rho-s, \tag{28}$$

where s is an element of the $GF[p^n]$. Hence (27) gives

$$s=\frac{(1-\rho-s)(\rho+s)}{1-\rho}$$

$$\rho^2+\rho(s-1)+s^2=0. \tag{29}$$

Hence any root of (26) which belongs to the $GF[p^{2n}]$, but not to the $GF[p^n]$, satisfies an equation of type (29) irreducible in the $GF[p^n]$. Conversely, any root ρ of an irreducible equation (29) is a root of (26). Indeed, the second root is ρ^{p^n} and the sum of the roots is $1-s$; thus (28) and hence also (27) is satisfied. Now, for $p>2$, (29) is irreducible if and only if $(1+s)(1-3s)$ is a not-square in the $GF[p^n]$. We readily verify* that this is the case for the following number of values of s:

$$\tfrac{1}{2}(p^n-3) \text{ if } p^n=3l+2, \qquad \tfrac{1}{2}(p^n-1) \text{ if } p=3 \text{ or } p^n=3l+1. \tag{30}$$

For $p>2$, we must investigate the reducibility of (29) when ρ is replaced by λ^2. By the product of the roots,

$$\rho^{p^n+1}=s^2, \qquad \rho^{(p^{2n}-1)/2}=+1,$$

so that ρ is a square in the $GF[p^{2n}]$. Hence the quartic in λ is reducible. Its factors are

$$\lambda^2+a\lambda\pm s, \qquad \lambda^2-a\lambda\pm s,$$

where $a^2=1-s\pm 2s$. The product of the two values for a^2 is the not-square $(1+s)(1-3s)$, so that one value is a square.

* By means of *Linear Groups*, p. 48, § 66. Note that -3 is a square or not-square according as $p^n=3l+1$ or $3l+2$.

Examples. If $p^n = 3$, then $s = 1$ and

$$\lambda^4 + 1 = (\lambda^2 + \lambda - 1)(\lambda^2 - \lambda - 1).$$

If $p^n = 5$, then $s = -2$, and

$$\lambda^4 + 2\lambda^2 - 1 = (\lambda^2 + 2\lambda - 2)(\lambda^2 - 2\lambda - 2).$$

If $p = 2$, we multiply (29) by $(s-1)^{-2}$ and set

$$\sigma = \rho(s-1)^{-1}, \qquad t = s^2(s^2+1)^{-1}.$$

Then $\sigma^2 + \sigma + t = 0$. This is irreducible if and only if t is one of the 2^{n-1} roots of (22) in the $GF[2^n]$. Unless $t = 1$, the corresponding value of s is uniquely determined in the field. But $t = 1$ is a root of (22) if and only if n is odd. Hence the number of values of s for which (29) is irreducible in the $GF[2^n]$ is

(31) $\qquad 2^{n-1} - 1$ for n odd, $\qquad 2^{n-1}$ for n even.

The number is zero for $n = 1$; for $n = 2, 3, 4$, s is a root of

$$s^2 + s + 1 = 0, \qquad s^3 + s + 1 = 0, \qquad (s^4 + s + 1)(s^4 + s^3 + 1) = 0.$$

It remains to determine the roots of (26) which belong to the $GF[p^{3n}]$. These must satisfy the equation

$$\rho + \rho^{p^n} + \rho^{p^{2n}} = 1. \tag{32}$$

Conversely, any root of the latter belongs to the $GF[p^{3n}]$ and, with the exception of $\rho = 1$ when $p = 2$, satisfies (26). A root of (32) belongs to the $GF[p^n]$ only when $3\rho = 1$. Hence the irreducible cubic factors of (26) are of the form $\rho^3 - \rho^2 + \cdots$ and their number is

$$3^{2n-1} \text{ if } p = 3, \qquad \tfrac{1}{3}(p^{2n} - 1) \text{ if } p \neq 3. \tag{33}$$

By § 15, these factors give all the existing irreducible cubics $x^3 - x^2 + \cdots$.

The irreducible factors of (26) are of degree 6 or a divisor of 6. Denote by L, Q, C the number of linear, quadratic and cubic factors, respectively. Then the number of degree 6 is

$$S = \tfrac{1}{6}(p^{3n} + p^n - 1 - L - 2Q - 3C).$$

By the above results we have, whether $p = 2$ or $p > 2$,

$$\begin{aligned} &S = \tfrac{1}{6}(p^{3n} - p^{2n} + 2) \text{ for } p^n = 3l + 2, \\ &S = \tfrac{1}{6}(p^{3n} - p^{2n}) \text{ for } p = 3 \text{ or } p^n = 3l + 1. \end{aligned} \tag{34}$$

In view of (31), (33), (34), we have the

Theorem. *If $p = 2$, the number of classes of irreducible sextic forms is $\frac{1}{6}(2^{3n} + 2^{2n} + 3\cdot 2^n - 6)$ for n odd, $\frac{1}{6}(2^{3n} + 2^{2n} + 3\cdot 2^n - 2)$ for n even.*

For $p^n = 2$ this number is 2. The irreducible factors of (26) are then

$$\rho^3 + \rho^2 + 1, \qquad \rho^6 + \rho^5 + 1.$$

Irreducible Cubics whose Roots are Squares with a given Sum.

14. For sextic forms when $p > 2$ there remains the difficult problem: to determine which of the cubics

$$C = \rho^3 - \rho^2 + a\rho - b \tag{35}$$

are irreducible and give irreducible sextics when ρ is replaced by λ^2, and which give reducible sextics. The first or second case arises according as ρ is a not-square or a square in the $GF[p^{3n}]$, namely, according as b is a not-square or a square in the $GF[p^n]$. In fact,

$$b = \rho\cdot\rho^{p^n}\cdot\rho^{p^{2n}}, \qquad b^{(p^n-1)/2} = \rho^{(p^{3n}-1)/2}.$$

In the second case, $b = e^2$, and $\lambda^6 - \lambda^4 + a\lambda^2 - e^2$ has the factors

$$\lambda^3 \pm c\lambda^2 + \tfrac{1}{2}(c^2 - 1)\lambda \pm e, \tag{36}$$

where

$$c^4 - 2c^2 - 8ec + 1 - 4a = 0.$$

This quartic has the resolvent cubic

$$y^3 + 2y^2 - 4(1 - 4a)y - 8(1 - 4a) - 64e^2 = 0.$$

We set $y = 2z$ and multiply the resulting equation by 8, and get

$$z^3 + z^2 + (4a - 1)z - 1 + 4a + 8b = 0.$$

If in the cubic $8C = 0$ we replace ρ by $\frac{1}{2}(z + 1)$, we obtain the preceding cubic. Hence the resolvent cubic is irreducible, so that* the quartic has one and but one root c in the $GF[p^n]$. The unique pair of factors of the sextic in λ are therefore of the form (36).

To determine the irreducible cubics (35) in which $b = e^2$,

$$C = \rho^3 - \rho^2 + a\rho - e^2 \qquad (e \neq 0), \tag{37}$$

we proceed indirectly and find those which are reducible.

(*a*) First, let C have a linear factor $\rho - k$ and an irreducible quadratic factor. The latter must be of the form $\rho^2 + (k-1)\rho + ks^2$, where $s^2 = e^2/k^2 \neq 0$.

* Bulletin of the American Mathematical Society, vol. 13 (1906), p. 5, middle of p. 7.

The quadratic is irreducible if and only if $(k-1)^2-4ks^2$ is a not-square. Let ν be a fixed not-square and let $p^n = 4l \pm 1$, the upper or lower sign holding according as -1 is a square or a not-square. Then

$$(k-1)^2 - 4ks^2 = \nu z^2$$

has $p^n \mp 1$ sets of solutions s, z when k is any chosen not-square, $p^n \pm 1$ sets when k is any chosen square $\neq 1$, while for $k=0$ or 1 the solutions are obvious. After excluding the sets in which either $s=0$ or $z=0$, and dividing by 4, we obtain the number of values of $s^2 \neq 0$ for which $(k-1)^2-4ks^2$ is a not-square. If -1 is a square the number of sets s^2, k, and hence the number of irreducible quadratics, is

$$\tfrac{1}{4}(p^n-1)\cdot\tfrac{1}{2}(p^n-1) + \tfrac{1}{4}(p^n-1)\cdot\tfrac{1}{2}(p^n-3) = \tfrac{1}{4}(p^n-1)(p^n-2).$$

If -1 is a not-square, the number is

$$\tfrac{1}{4}(p^n+1)\cdot\tfrac{1}{2}(p^n-1) + \tfrac{1}{4}(p^n-3)\cdot\tfrac{1}{2}(p^n-3) + \tfrac{1}{2}(p^n-1) = \tfrac{1}{2}(p^{2n}-p^n+2).$$

In the following examples we give all the irreducible quadratics: For $p^n=3$, $s^2=1$, $k=\pm 1$. For $p^n=5$, $s^2=1$, $k=2, 3, 4$. For $p^n=7$, $s^2=1$, $k=1, 3, 5$; $s^2=2$, $k=1, 2, 4, 6$; $s^2=4$, $k=1, 3, 5, 6$. For $p^n=11$, $s^2=1$, $k=1, 5, 7, 8, 9, 10$; $s^2=3$, $k=1, 2, 6, 7, 8$; $s^2=4$, $k=1, 2, 5, 6, 9$; $s^2=5$, $k=1, 3, 4, 7, 8, 10$; $s^2=9$, $k=1, 2, 3, 4, 6, 10$. For $p^n=9$, $i^2 \equiv -1 \pmod 3$, $s^2=1$, $k=\pm i+1, \pm i-1$; $s^2=\pm i$, $k=-1, i, -i, \mp i+1, \mp i-1$.

(b) Next let (37) have three roots in the $GF[p^n]$. Either all three are squares or only one root is a square.

(b_1) Let the three roots be squares. We seek the number of systems of three squares s_i with the sum unity, two systems being identified if they are composed of the same s_i in different orders.

If t is the number of systems with $s_1 = s_2 = s_3$, we have

$$(38) \qquad t=0 \text{ if } p=3 \text{ or } p^n = 12k \pm 5, \qquad t=1 \text{ if } p^n = 12k \pm 1.$$

Let μ be the number of sets with $s_1 = s_2$. Now $x^2+2y^2=1$ has p^n-1 or p^n+1 sets of solutions according as -2 is a square or a not-square. Of these, 4 or 2 have $xy=0$, according as 2 is a square or a not-square, namely, according as $p^n = 8l \pm 1$ or $8l \pm 3$. Hence

$$\mu = \tfrac{1}{4}(p^n-5) \text{ if } p^n = 8l+1, \qquad \tfrac{1}{4}(p^n-3) \text{ if } p^n = 8l-1 \text{ or } 8l+3,$$
$$\tfrac{1}{4}(p^n-1) \text{ if } p^n = 8l+5.$$

The number of sets s_i in which exactly two are equal is therefore $3(\mu - t)$.

Next, the total number of sets of solutions of *

$$x^2 + y^2 + z^2 = 1$$

is $p^{2n} \pm p^n$ according as $p^n = 4l \pm 1$. These include $p^n \mp 1$ sets with $z = 0$. Hence the numbers of sets of squares s_i whose sum is unity is

$$k = \tfrac{1}{8}\{ p^{2n} \pm p^n - 3(p^n \mp 1 - 4) - 6 \}.$$

Hence there are $\tfrac{1}{6}\{ k - 3(\mu - t) - t \}$ systems in which s_1, s_2, s_3 are all distinct. As shown above, there are $\mu - t$ systems in which exactly two of the s_i are equal, and t systems with all three equal. The total number of systems is therefore $\tfrac{1}{6}(k + 3\mu + 2t)$.

(b_2) Let one of the roots be a square s and the other two not-squares n_1, n_2. If the latter are equal, we employ the $p^n - 1$ or $p^n + 1$ sets of solutions of $x^2 + 2\nu y^2 = 1$, according as -2 is a not-square or a square, namely, according as $p^n = 8l - 1$, $8l - 3$ or $p^n = 8l + 1$, $8l + 3$. Now there are two sets of solutions with $x = 0$ if 2 is a not-square, namely, if $p^n = 8l \pm 3$. Hence the number of sets s, $n_1 = n_2$ is

$$N = \tfrac{1}{4}(p^n - 1) \text{ if } p^n = 8l + 1, \qquad \tfrac{1}{4}(p^n - 3) \text{ if } p^n = 8l - 1 \text{ or } 8l + 3,$$
$$\tfrac{1}{4}(p^n - 5) \text{ if } p^n = 8l + 5.$$

The total number of sets of solutions of $x^2 + \nu y^2 + \nu z^2 = 1$ is $p^{2n} \pm p^n$ according as $p^n = 4l \pm 1$. These include $p^n \mp 1$ sets with $x = 0$ and $p^n \pm 1$ sets with $y = 0$. Hence the total number of sets s, n_1, n_2 is

$$M = \tfrac{1}{8}\{ p^{2n} \pm p^n - (p^n \mp 1) - 2(p^n \pm 1 - 2) - 2 \}.$$

The total number of systems is therefore $\tfrac{1}{2}(M - N) + N = \tfrac{1}{2}M + \tfrac{1}{2}N$. Now

$$\tfrac{1}{6}k + \tfrac{1}{2}M = \tfrac{1}{12}(p^{2n} \pm p^n - 3p^n + 3),$$

while $N + \mu = \tfrac{1}{2}(p^n - 3)$ for all values of p^n. Hence the number of cubics (37) with three roots in the $GF[p^n]$ is $\tfrac{1}{12}(p^{2n} \pm p^n - 6) + \tfrac{1}{3}t$, according as $p^n = 4l \pm 1$.

Combining this number with the number obtained in case (a), we get

$$\tfrac{1}{3}(p^{2n} - 2p^n + t) \text{ if } p^n = 4l + 1, \qquad \tfrac{1}{3}(p^{2n} - p^n + t) \text{ if } p^n = 4l - 1.$$

The total number of cubics (37) is $\tfrac{1}{2}(p^n - 1)p^n$. Hence, by (38), we obtain the

Theorem. *The number of irreducible cubics* (37) *is*

* *Linear Groups*, p. 48.

$$(39)\qquad \begin{aligned} &\tfrac{1}{6}(p^n \mp 1)(p^n \pm 2) \text{ if } p^n = 12k \pm 1, \\ &\tfrac{1}{6}p^n(p^n \pm 1) \text{ if } p^n = 12k \pm 5, \text{ or if } p = 3 \text{ and } \pm 1 = (-1)^n. \end{aligned}$$

A check upon the above results is afforded by the following examples which give all systems of three elements in the $GF[p^n]$ whose sum is unity and whose product is a square:

$p^n = 3$, none; $p^n = 5$, $1, 1, 4; 1, 2, 3$; $p^n = 7$, $4, 2, 2; 2, 3, 3; 4, 5, 6$;

$p^n = 3^2$, $i^2 \equiv -1 \pmod 3$, $1, 1, 2; i, -i, 1; 1, i \pm 1, -i \mp 1;$

$-1, i+1, -i+1; \pm i, \pm i - 1, \pm i - 1;$

$p^n = 11$, $4, 4, 4; 3, 4, 5; 5, 9, 9; 3, 2, 7; 3, 10, 10;$

$4, 2, 6; 5, 8, 10; 9, 7, 7; 9, 6, 8;$

$p^n = 13$, $1, 1, 12; 1, 3, 10; 1, 4, 9; 3, 12, 12; 9, 9, 9; 1, 2, 11; 1, 5, 8;$

$1, 6, 7; 3, 5, 6; 4, 2, 8; 4, 5, 5; 9, 7, 11; 10, 2, 2; 10, 6, 11; 12, 7, 8.$

By excluding the resulting cubics and those given by the examples under case (a), we find the only irreducible cubics (37) are those in which a, e^2 is one of the following sets:

$p^n = 3$, $2, 1$; $p^n = 5$, $1, -1; 3, -1; 0, 1; 4, 1; 3, 1;$

$p^n = 7$, $0, 1; 3, 1; 5, 1; 1, 2; 5, 2; 2, 4; 5, 4;$

$p^n = 9$, $i^2 \equiv -1 \pmod 3$, $0, -1; 1, -1; \pm i, -1; -1, 1;$

$\pm i + 1, 1; \pm i - 1, 1; 0, \pm i; 1, \pm i; \pm i - 1, \mp i;$

$p^n = 11$, $3, 1; 7, 1; 0, 3; \pm 1, 3; 2, 3; \pm 2, 4; 6, 4; 7, 4;$

$8, 4; 0, 5; 7, 5; 10, 5; 1, 9; 2, 9; 3, 9; 5, 9.$

15. The investigation made in § 14 enables us to determine the number N_{g_s} of irreducible cubics $x^3 - gx^2 + hx + k$, in which g is a given element and k ranges over the squares, and the corresponding number N_{gn} when k ranges over the not-squares.

Let C_g be the number of all the irreducible cubics $x^3 - gx^2 + \cdots$ in which g is a given element. If ρ is a root of such a cubic,

$$(40)\qquad \rho + \rho^{p^n} + \rho^{p^{2n}} = g, \qquad \rho^{p^{3n}} = \rho.$$

Since the latter equation follows from the former, we conclude that (40_1) has p^{2n} roots in the $GF[p^{3n}]$. If such an element ρ is distinct from ρ^{p^n} it is a root of a cubic irreducible in the $GF[p^n]$. Now a common root of $\rho = \rho^{p^n}$ and (40_1)

makes $3\rho = g$, so that the two equations have a single solution if $p \neq 3$, no solution if $p = 3$, $g \neq 0$, and 3^n solutions if $p = 3$, $g = 0$. Hence

(41) $C_g = \frac{1}{3}(p^{2n}-1)$ if $p \neq 3$, $C_0 = \frac{1}{3}(3^{2n}-3^n)$ if $p=3$, $C_{g'} = 3^{2n-1}$ if $p=3$, $g' \neq 0$.

For any p, the total number of irreducible cubics is therefore $\frac{1}{3}p^n(p^{2n}-1)$, in agreement with § 7. Conversely, if* $p \neq 3$, the latter result implies (41), since $x' = x + \frac{1}{3}(g + g')$ transforms each $x^3 - gx^2 + \cdots$ into a cubic $x^3 - g'x^2 + \cdots$.

If ν is a fixed not-square in the $GF[p^n]$, (40_1) gives

$$\nu\rho + (\nu\rho)^{p^n} + (\nu\rho)^{p^{2n}} = \nu g.$$

First, let ρ be a square in the $GF[p^{3n}]$. Since ν is a not-square in the $GF[p^{3n}]$, $\nu\rho$ is a not-square. Hence

$$N_{0s} = N_{0n}, \qquad N_{gs} = N_{g'n},$$

where one of the elements g, g' is any square and the other any not-square. Thus *if σ is any square and ν any not-square in the $GF[p^n]$,*

(42) $N_{0s} = N_{0n} = \frac{1}{2}C_0$, $N_{\nu n} = N_{\sigma s} = N_{1s}$, $N_{\nu s} = N_{\sigma n} = C_1 - N_{1s}$,

where C_0 and C_1 are given by (41) *and N_{1s} is given by* (39).

16. We may now enumerate the irreducible factors in the $GF[p^n]$, $p > 2$, of the function of degree $d = 2(p^{3n} + p^n - 1)$ derived from (26) by replacing ρ by λ^2. First, if $p \neq 3$, $\lambda^2 - \frac{1}{3}$ has $t + 1$ factors, where t is defined by (38). Next, there are $2r$ further irreducible quadratic factors, where r is defined by (30). Again, there are $2N_{1s}$ irreducible cubic factors and N_{1n} irreducible sextic factors, all derived from the cubic functions of ρ (§ 14). The remaining factors are irreducible sextics; their number is therefore

$$\tfrac{1}{6}(d - e - 4r - 6N_{1s} - 6N_{1n}) \quad (e = 0 \text{ if } p = 3,\ e = 2 \text{ if } p \neq 3).$$

Thus if $\beta = 0$ when $p = 3$, $\beta = t + \frac{2}{3}$ if $p \neq 3$, the total number of factors is

$$\tfrac{1}{6}d + \beta + \tfrac{4}{3}r + N_{1s}.$$

Hence we may state the following

Theorem. *The number of classes of irreducible sextics in the $GF[p^n]$, $p > 2$, is $\frac{1}{6}(2p^{3n} + p^{2n} + 7p^n - a)$, $a = -2$ if $p^n = 12k + 1$, $a = 10$ if $p^n = 12k + 5$, $a = 6$ if $p = 3$, n even; $\frac{1}{6}(2p^{3n} + p^{2n} + 5p^n - b)$, $b = 2$ if $p^n = 12k - 5$, $b = 6$ if $p^n = 12k - 1$ or if $p = 3$, n odd.*

* By means of $x' = gx$ we conclude that, for any p, $C_g = C_1$ if $g \neq 0$. The value of C_0 was determined otherwise in Bulletin of the American Mathematical Society, l. c., pp. 3, 4.

For $p^n = 3$, the 12 irreducible factors* are

$$\lambda^2 \pm \lambda - 1,\ \lambda^3 \pm \lambda^2 \mp 1,\ \lambda^6 - \lambda^4 + 1,\ \lambda^6 - \lambda^4 + \lambda^2 + 1,$$
$$\lambda^6 \pm \lambda^5 - \lambda^4 + \lambda^2 - 1,\ \lambda^6 \pm \lambda^5 \pm \lambda^3 - 1,\ \lambda^6 \pm \lambda^5 \mp \lambda^3 + 1.$$

For $p^n = 5$, the 50 irreducible factors are 34 sextics† and

$$\lambda^2 - 2,\ \lambda^2 \pm 2\lambda - 2,\ \lambda^3 \pm \lambda^2 \pm 2,\ \lambda^3 \pm 2\lambda^2 - \lambda \pm 2,\ \lambda^3 \mp 2\lambda^2 - \lambda \pm 1,$$
$$\lambda^3 + 2\lambda \pm 1,\ \lambda^3 \pm \lambda^2 \pm 1,\ \lambda^6 - \lambda^4 - \lambda^2 - 3,\ \lambda^6 - \lambda^4 + \lambda^2 - 3,\ \lambda^6 - \lambda^4 - 2.$$

For $p^n = 7$, the 128 irreducible factors are 98 sextics† and

$$\lambda^2 - 5,\ \lambda^2 \pm 3\lambda + 1,\ \lambda^2 \pm 3\lambda - 2,\ \lambda^2 \pm 2\lambda + 3,\ \lambda^3 \pm 2\lambda^2 - 2\lambda \pm 1,\ \lambda^3 \pm \lambda^2 \pm 1,$$
$$\lambda^3 \pm 3\lambda^2 + 4\lambda \pm 1,\ \lambda^3 \pm \lambda^2 \pm 3,\ \lambda^3 \pm 3\lambda^2 + 4\lambda \pm 3,\ \lambda^3 + 3\lambda \pm 2,\ \lambda^3 \pm 2\lambda^2 - 2\lambda \mp 2,$$
$$\lambda^6 - \lambda^4 + 4\lambda^2 - 6,\ \lambda^6 - \lambda^4 + 6\lambda^2 - 3,\ \lambda^6 - \lambda^4 - 3,\ \lambda^6 - \lambda^4 + \lambda^2 - 5,\ \lambda^6 - \lambda^4 + 5\lambda^2 - 3,$$
$$\lambda^6 - \lambda^4 + 2\lambda^2 - 6,\ \lambda^6 - \lambda^4 + 3\lambda^2 - 5,\ \lambda^6 - \lambda^4 + 4\lambda^2 - 3,\ \lambda^6 - \lambda^4 + 6\lambda^2 - 5.$$

Classes of Irreducible Septic Forms.

17. For septic forms we set $K = \rho J$ in (20) and obtain an equation of degree $d = p^{4n} + p^{2n} + 1$ in ρ, having d roots in the $GF[p^{7n}]$. For $\rho^{p^n} = \rho$, the equation becomes

$$1 - 5\rho + 6\rho^2 - \rho^3 = 0. \tag{43}$$

If $p = 2$, a root of (43) belongs to the exponent 7 and hence belongs to the $GF[2^n]$ if and only if 7 is a divisor of $2^n - 1$, namely, if n is a multiple of 3. In the latter case there are 3 linear and $\frac{1}{7}(d-3)$ irreducible septic factors. But if n is prime to 3, all the factors are septics. For example, if $n = 1$, 2, or 3, the number of septic factors is 3, 39, or 594, respectively. *If $p = 2$, the number of classes of irreducible septic forms is $3 + \frac{1}{7}(d-3)$ or $\frac{1}{7}d$, according as n is a multiple of 3 or prime to 3.*

If we set $\rho = \sigma + 2$ in (43), we get‡

$$\sigma^3 - 7\sigma - 7 = 0. \tag{44}$$

Hence if $p = 7$, $\rho = 2$ is the only root in the $GF[p^n]$. Upon replacing ρ by λ^2 we obtain the linear factors $\lambda \pm 3$ and $\frac{1}{7}(2d-2)$ irreducible septic factors. *For $p = 7$, the number of classes of irreducible septic forms is* $2 \cdot 7^{4n-1} + 2 \cdot 7^{2n-1} + 2$.

*Two factors with an ambiguous sign are obtained from the same irreducible function of ρ.

†The omitted sextics are by pairs factors of an irreducible sextic in $\rho = \lambda^2$.

‡This cubic is a resolvent for the seventh roots of unity. For its numerical solution see SERRET, *Algèbre Supérieure*, vol. 1, pp. 338, 343.

For $p \neq 2$, $p \neq 7$, we determine the number N of distinct roots of (43) in the $GF[p^n]$ by the following indirect process. Since the equation of degree d has $d - N$ roots in the $GF[p^{7n}]$, not belonging to the $GF[p^n]$, it has

$$E = \tfrac{1}{7}(p^{4n} + p^{2n} + 1 - N)$$

irreducible septic factors. Thus E must be an integer. Since the discriminant of (43) or (44) is the square 7^2, we have $N = 0$ or 3 (Bulletin, l. c., p. 1). Now p^{2n} is of the form $7l + s$, where $s = 1, 2$ or 4. Thus E is an integer only when $N = 3, 0$ or 0, respectively. Hence for $p \neq 2$, $p \neq 7$, the cubic (43) has 3 roots in the $GF[p^n]$ if $p^n = 7k \pm 1$, no root if $p^n = 7k \pm 2, \pm 3$. In the former case, each root r is a square in the $GF[p^n]$; for, if not, each root of $\lambda^2 = r$ would belong to the $GF[p^{2n}]$ and not to the $GF[p^n]$, whereas all the roots of the λ-equation belonging to the $GF[p^{7n}]$. Hence if $p^n = 7k \pm 1$, $p > 2$, there are six linear factors. For example,

$$p^n = 13,\ \lambda \pm 2,\ \lambda \pm 4,\ \lambda \pm 8;\quad p^n = 29,\ \lambda \pm 4,\ \lambda \pm 8,\ \lambda \pm 10;$$

$$p^n = 41,\ \lambda \pm 3,\ \lambda \pm 10,\ \lambda \pm 15;\quad p^n = 43,\ \lambda \pm 9,\ \lambda \pm 16,\ \lambda \pm 20.$$

For $p \neq 2$, $p \neq 7$, the number of classes of irreducible septics is

$$6 + \tfrac{2}{7}(p^{4n} + p^{2n} - 2) \text{ or } \tfrac{2}{7}(p^{4n} + p^{2n} + 1),$$

according as p^n is or is not of the form $7k \pm 1$.

THE UNIVERSITY OF CHICAGO,
July 14, 1910.