A TWO-FOLD GENERALIZATION OF FERMAT'S THEOREM.

Presented to the American Mathematical Society, February 29, 1896.

BY PROFESSOR ELIAKIM HASTINGS MOORE.

Formulation of the generalized Fermat theorem III $[k+1, n; p]$. §§ 1–4.

1. In *Gauss's* congruence notation *Fermat's theorem* is:

I_1 $$a^p - a \equiv 0 \pmod{p}$$

where p is any prime and a is any integer:
or, otherwise expressed,

I_2 *The two rational integral functions of the indeterminate X with integral coefficients*

$$X^p - X, \quad \prod_{a=0}^{a=p-1} (X+a)$$

are identically congruent ($\equiv$) $\pmod{p}$:

$$X^p - X \equiv \prod_{a=0}^{a=p-1} (X+a) \pmod{p}.$$

We write I_2 thus:

I_3 *The two forms in the two indeterminates X_0, X_1,*

$$D[2,1;p](X_0, X_1) \equiv X_0 X_1^p - X_0^p X_1,$$

$$P[2,1;p](X_0, X_1) \equiv X_0 \cdot \prod_{a_0=0}^{a_0=p-1} (a_0 X_0 + X_1),$$

are identically congruent $\pmod{p}$:

$$D[2,1;p](X_0, X_1) \equiv P[2,1;p](X_0, X_1) \pmod{p}.$$

2. We proceed in two steps to a two-fold generalization of Fermat's theorem I_3.

II. *The two forms in the $k+1$ indeterminates $X_0, X_1, \cdots, X_k$,*

(1) $D[k+1, 1; p](X_0, X_1, \cdots, X_k) \equiv | X_j^{p^i} |$ $\quad (i, j = 0, 1, \cdots, k)$,

(2) $P[k+1, 1; p](X_0, X_1, \cdots, X_k) \equiv \prod^* \sum_g a_g X_g$ $\quad (g = 0, 1, \cdots, k)$,

—where the product $\prod^*$ embraces the $(p^{k+1} - 1)/(p-1)$ linear forms $\sum_{g=0}^{g=k} a_g X_g$ whose coefficients a_g $(g=0, 1, \cdots, k)$ are integers selected from the series $0, 1, \cdots, p-1$, in all possible ways, only

so that for every particular form, first, the coefficients a_g *are not all* 0, *and, second, of the coefficients* a_g *not* 0 *the one with largest index* g *is* 1 —— *are identically congruent* (mod p):

$$D[k+1, n; p](X_0, X_1, \cdots, X_k) \equiv P[k+1, n; p](X_0, X_1, \cdots, X_k).$$

When we collect into a *class* the totality of integers congruent to one another (mod p), and denote the p incongruent classes by p *marks*, we have in this system of p marks a *field* $F[p]$ *of order* p *and rank 1*. The marks of the field $F[p]$ may be combined by the four fundamental operations of algebra—addition, subtraction, multiplication, division, —the operations being subject to the ordinary abstract operational laws of algebra, the results of these operations being in every case uniquely determined and belonging to the field. *Congruences* ($\equiv$) (mod p) are in the field *equalities* ($=$), and *identical congruencies* ($\equiv$) are *identities* ($\equiv$). The restatement of II in the terminology of the field $F[p]$ is given by setting $n=1$ in its generalization III (§ 3).

3. The second step of generalization of I_3 rests upon *Galois's* generalization of the field $F[p]$ to the *Galois-field* $GF[p^n]$ of *order* p^n, *modulus* p, *and rank* n. This field of p^n marks a is uniquely defined for every p=prime, n=positive integer. (I have elsewhere proved that every field of finite order s is a Galois-field of order $s=p^n$.)

A form, that is, a rational integral function of certain indeterminates, $X_0, X_1, \cdots, X_k$, is said to *belong* to the $GF[p^n]$ if its coefficients belong to (are marks a of) the $GF[p^n]$. A *linear homogeneous form* $\sum_{g=0}^{g=k} a_g X_g$ belonging to the $GF[p^n]$ is called *primitive* if not all its coefficients a_g are 0, and if of the coefficients a_g not 0 the one with largest index g is 1.

We have then:

III. *The two forms in the* $k+1$ *indeterminates*, $X_0, X_1, \cdots, X_k$,

$$(3)\quad D[k+1, n; p](X_0, X_1, \cdots, X_k) \equiv |X_j^{p^{ni}}| \qquad (i, j=0, 1, \cdots, k),$$

$$(4)\quad P[k+1, n; p](X_0, X_1, \cdots, X_k) \equiv \prod{}^* \sum_g a_g X_g \qquad (g=0, 1, \cdots, k),$$

—*where the product* $\prod^*$ *embraces the* $(p^{n(k+1)}-1)/(p^n-1)$ *distinct primitive linear homogeneous forms* $\sum_{g=0}^{g=k} a_g X_g$ *belonging to the* $GF[p^n]$ — *are identical:*

$$D[k+1, n; p](X_0, X_1, \cdots, X_k) \equiv P[k+1, n; p](X, X_1, \cdots, X_k).$$

The forms D, P whose identity theorem III affirms have the three characteristic positive integers or *characters* $k+1$, n, p. It is convenient to attach these characters to the notation III for the theorem, and thus to speak of the theorem III $[k+1, n; p]$. This theorem requires proof only for $k \geqq 1$, since for $k=0$, $D \equiv X_0$, $P \equiv X_0$.

4. For the proof of III $[k+1, n; p]$ we need *Galois's* onefold generalizations of the *Fermat theorems* I:

II$_1'$ *Every mark* a *of the* $GF[p^n]$ *satisfies the equation*

$$a^{p^n} - a = 0.$$

whence,

II$_2'$ *The two forms in the indeterminate* X

$$X^{p^n} - X, \qquad \prod_{a \mid p^n} (X + a)$$

belonging to the $GF[p^n]$ *are identical:*

$$X^{p^n} - X \equiv \prod_{a \mid p^n} (X + a),$$

(where, as always, the subscript-remark $a \mid p^n$ means that the mark a is to run over the p^n marks of the $GF[p^n]$), and further,

II$_3'$ *The two forms in the two indeterminates* X_0 X_1,

$$D[2, n; p](X_0, X_1) \equiv X_0 X_1^{p^n} - X_0^{p^n} X_1,$$
$$P[2, n; p](X_0, X_1) \equiv \prod{}^{*} (a_0 X_0 + a_1 X_1),$$

— *where the product* $\prod^{*}$ *embraces the* p^n+1 *distinct primitive linear homogeneous forms* $a_0 X_0 + a_1 X_1$ *belonging to the* $GF[p^n]$ — *are identical:*

$$D[2, n; p](X_0, X_1) \equiv P[2, n; p](X_0, X_1).$$

A (known) corollary to II$_1'$ is also needed. We denote by $\wedge_h$ the substitution on the p^n marks a of the $GF[p^n]$ which replaces every mark a by a^{p^h}; obviously $\wedge_c \wedge_d = \wedge_{c+d}$ while by II$_1'$, $\wedge_n = \wedge_0 = 1$. We denote by $F_h(X_0, X_1, \cdots, X_k)$ the result obtained by applying the substitution Λ_h to the mark-coefficients of a form $F(X_0, X_1, \cdots, X_k)$ belonging to the $GF[p]$, so that $F_n(X_0, X_1, \cdots, X_k) \equiv F_0(X_0, X_1, \cdots, X_k) \equiv F(X_0, X_1, \cdots, X_k)$. Since in the involution of a multinomial to the p^{th} power the say *intermediate* multinomial coefficients are all divisible by p, we have in the $GF[p^n]$ of modulus p,

$$F_h(X_0, X_1, \cdots, X_k)^p \equiv F_{k+1}(X_0^p, X_1^p, \cdots, X_k^p),$$

whence

II$_1'$ Cor. $\quad F(X_0, X_1, \cdots, X_k)^{p^n} \equiv F(X_0^{p^n}, X_1^{p^n}, \cdots, X_k^{p^n}),$

where $F(X_0, X_1, \cdots, X_k)$ *is any form of the* $GF[p^n]$.

The theorem III$[k+1, n; p]$ bears the same relation to Galois's Fermat's theorem II$'$: $\mathrm{II}_3' \equiv$ III$[2, n; p]$: that the theorem II $\equiv$ III$[k+1, 1; p]$ bears to Fermat's theorem I : $\mathrm{I}_3 \equiv$ III$[2, 1; p]$. I am communicating then one-fold generalizations II, III of the known theorems I, II$'$; of these II may be looked at as a theorem in the ordinary Gauss-congruence theory, while its generalization III is a theorem in the Galois-field theory.

I give three proofs A, B, C of the general theorem III$[k+1, n; p]$. The proof A depends upon considerations involving the $GF[p^n]$ of rank n alone, and accordingly for $n=1$ this proof A of III$[k+1, 1; p] \equiv$ II may be exhibited in the terminology of the ordinary Gauss-congruence theory. The proofs B and C however depend upon considerations involving the wider $GF[p^{mn}]$ of rank mn $(m \geqq 2k^2)$; they throw a sharper light upon the essential meaning of the theorem III$[k+1, n; p]$ for every n.

Proof A of the theorem III $[k+1, n; p]$. § 5.

Proof by two-based induction. We know that III$[1, n; p]$ and III$[2, n; p] \equiv \mathrm{II}_3'$ are true. On the supposition that III$[l-1, n; p]$ and III$[l, n; p]$ $(l > 1)$ are true we prove that III$[l+1, n; p]$ is true.

5. In the determinant $U = | u_{ij} |$ $(i, j=0, 1 \cdots\cdots, l)$ we denote by U_{ij} the minor complementary to u_{ij}, and have*

$$(5) \qquad (-1)^{l+1} \begin{vmatrix} U_{l1}, & U_{l0} \\ U_{01}, & U_{00} \end{vmatrix} \equiv U. \; | u_{ij} | \qquad \left(\begin{smallmatrix} i=1, 2 \cdots, l-1 \\ j=2, 3, \cdots, l \end{smallmatrix}\right)$$

We set now

$$u_{ij} = X_j^{p^{ni}} \qquad (i, j=0, 1, \cdots, l),$$

so that we have

$$(6) \quad \begin{aligned} &D[l+1, n; p](X_0, X_1, \cdots, X_l) \equiv + U, \\ &D[l-1, n; p](X_2^{p^n}, X_3^{p^n}, \cdots X_l^{p^n}) \equiv | u_{ij} | \; \left(\begin{smallmatrix} i=1, 2, \cdots, l-1 \\ j=2, 3, \cdots, l \end{smallmatrix}\right), \\ &D[l, n; p](X_0, X_2, \cdots, X_l) \equiv (-1)^{l+1} U_{l1}, \\ &D[l, n; p](X_1, X_2, \cdots, X_l) \equiv (-1)^l U_{l0}, \\ &D[l, n; p](X_0^{p^n}, X_2^{p^n}, \cdots, X_l^{p^n}) \equiv - U_{01}, \\ &D[l, n; p](X_1^{p^n}, X_2^{p^n}, \cdots, X_l^{p^n}) \equiv + U_{00}. \end{aligned}$$

Then by substituting the values (6) in the identity (5) and remembering II_1' Cor. and the definition (3) of $D[2, n; p]$ (Y_0, Y_1), we have the fundamental identity

* See, for instance, Scott's *Determinants*, p. 57, No. 6.

$$(7)\ D[2,n;p]\Big(D[l,n;p](X_0,X_2,\cdots,X_l),D[l,n;p](X_1,X_2,\cdots X_l)\Big)$$
$$\equiv D[l+1,n;p](X_0,X_1,\cdots,X_l)\cdot D[l-1,n;p](X_2,X_3,\cdots X_l)^{p^n}.$$

Now, using always the Π^* in the sense defined in the enunciation of III, we have by hypothesis:

$$(8_1)\ \mathrm{III}[2,n;p]:\ D[2,n;p](Y_0,Y_1)\equiv P[2,n;p](Y_0,Y_1)\equiv \Pi^*(\beta_0 Y_0+\beta_1 Y_1)\equiv Y_0\cdot\prod_{\beta\,|\,p^n}(\beta Y_0+Y_1),$$

$$(8_2)\ \mathrm{III}[l-1,n;p]:\ D[l-1,n;p](Y_0,Y_1,\cdots,Y_{l-2})\equiv P[l-1,n;p](Y_0,Y_1,\cdots,Y_{l-2})\equiv\Pi^*\sum_{h=0}^{h=l-2}\beta_h Y_h,$$

$$(8_3)\ \mathrm{III}[l,n;p]:\ D[l,n;p](Y_0,Y_1,\cdots,Y_{l-1})\equiv P[l,n;p](Y_0,Y_1,\cdots,Y_{l-1})\equiv\Pi^*\sum_{h=0}^{h=l-1}\beta_h Y_h.$$

By (8_2) the left side of the identity (7) is

$$(9)\ D[l,n;p](X_0,X_2,\cdots,X_l)\cdot\prod_{\beta\,|\,p^n}\Big(\beta\,D[l,n;p](X_0,X_2,\cdots,X_l)+D[l,n;p](X_1,X_2,\cdots,X_l)\Big),$$

which, using II_1' and II_1' Cor. in the addition of the determinants, is

$$(10)\qquad D[l,n;p](X_0,X_2,\cdots,X_l)\cdot\prod_{\beta\,|\,p^n}D[l,n;p](\beta X_0+X_1,X_2,\cdots,X_l),$$

which by (8_3) is

$$(11)\ \Pi^*(\delta_0 X_0+\delta_2 X_2+\cdots+\delta_l X_l)\cdot\prod_{\beta\,|\,p^n}\Pi^*\Big(\gamma_1(\beta X_0+X_1)+\gamma_2 X_2+\cdots+\gamma_l X_l\Big).$$

We compare the product (11) with the product (12),

$$(12)\qquad P[l+1,n;p](X_0,X_1,\cdots,X_l)\equiv\Pi^*(\alpha_0 X_0+\alpha_1 X_1+\alpha_2 X_2+\cdots+\alpha_l X_l).$$

The factors of (12) are the primitive linear homogeneous forms $\sum_{g=0}^{g=l}\alpha_g X_g$ with no omissions and no repetitions. Every factor of (11) is likewise such a form. And in (11) every such form $\sum_{g=0}^{g=l}\alpha_g X_g$ occurs at least once; any such form $\sum_{g=0}^{g=l}\alpha_g X_g$

with $a_1 \neq 0$ occurs (since $l > 1$) once and only once, viz., under that Π^* of the second set in (11) whose forms have $\beta = a_0 / a_1$; any such form $\sum_{g=0}^{g=l} a_g X_g$ with $a_1 = 0$, $a_0 \neq 0$, occurs once and only once, viz., under the single Π^* of the first set in (11); any such form $\sum_{g=0}^{g=l} a_g X_g$ with $a_1 = 0$, $a_0 = 0$, occurs in all $1 + p^n$ times, viz., once and of course only once under every Π^* of (11). Thus the product (11) is:

$$(13) \quad P[l+1, n; p](X_0, X_1, \cdots, X_l) \cdot \left(\Pi^* \sum_{g=2}^{g=l} a_g X_g \right)^{p^n}.$$

When we substitute (13) for the left side of the identity (7) and divide out* the second factors, which are identical by the hypothesis (8_2), we have the desired identity

$$(14) \quad \mathrm{III}[l+1, n; p]:$$
$$P[l+1, n; p](X_0, X_1, \cdots, X_l) \equiv D[l+1, n; p](X_0, X_1, \cdots, X_l).$$

Proof B of the theorem III$[k+1, n; p]$. §§ 6–11.

Direct proof of the identity III♮$[k+1, n; p]$

$$\mathrm{III}\natural \quad D[k+1, n; p](X_0, X_1, \cdots, X_k) \equiv$$
$$D[k, n; p](X_0, X_1, \cdots, X_{k-1}) \cdot \prod_{\substack{a_r \mid p^n \\ (r=0, \cdots, k-1)}} \left(\sum_{r=0}^{r=k-1} a_r X_r + X_k \right).$$

6. *From the identity* III♮$[l+1, n; p]$ *for* $l = 1, 2, \cdots, k$, *and in view of the definition* (3) $D[1, n; p](X_0) \equiv X_0$, *we have*

$$(15) \quad D[k+1, n; p](X_0, X_1, \cdots, X_k) \equiv X_0 \cdot \prod_{l=1}^{l=k} \prod_{\substack{a^r \mid p^n \\ (r=0, \cdots, l-1)}} \left(\sum_{r=0}^{r=l-1} a_r X_r + X_l \right),$$

viz., *the identity called for by the theorem* III$[k+1, n; p]$.

7. *We introduce the* $GF[p^{mn}]$ *of modulus* p *and rank* mn *where* m *is any integer* $m \geqq 2k^2 \geqq k+1$. The $GF[p^{mn}]$ contains the $GF[p^n]$. The forms entering the theorems III$[k+1, n; p]$, III♮$[k+1, n; p]$ belong to the $GF[p^n]$, and the theorems then to the $GF[p^n]$-theory, but the forms belong also to the wider $GF[p^{mn}]$, and the proofs B, C of III♮ and III make use of this fact.

*As to the fact that the quotient-forms so obtained are identical, see, for instance, the theorem (3) § 3 of the memoir by WEBER: *Die allgemeinen Grundlagen der Galoisschen Gleichungstheorie* (*Mathematische Annalen*, vol. 43, pp. 521–549, 1893.)

8. The small Greek letters $\alpha, \beta, \gamma, \cdots$, as heretofore designate marks of the $GF[p^n]$, and the large Greek letters A, B, Γ, $\cdots$, marks of the $GF[p^{mn}]$.

Any t marks A_r $(r=1, 2, \cdots, t)$ of the $GF[p^{mn}]$ determine in the $GF[p^{mn}]$ an *additive-group* $[A_1, A_2, \cdots, A_t \mid GF[p^n]]$ with the *basis-system* $A_1, A_2, \cdots, A_t$ and *field of reference* $GF[p^n]$ containing all possible marks A expressible in the form

$$A = \sum_{r=1}^{r=t} \alpha_r A_r \tag{16}$$

where the $\alpha_r (r=1, 2, \ldots, t)$ are marks of the field of reference $GF[p^n]$.

The p^{tn} marks $A(16)$ are distinct if the particular mark $A = 0$ occurs only once, viz., with the coefficients α_r all 0. In this case, when of course $t \leqq m$, the additive-group has the *order* p^{tn} and *rank* t, and the t marks A_r are *linearly independent with respect to** *the* $GF[p^n]$, and obviously any t' of the t marks are likewise linearly independent. If $t < m$, not all the marks of the $GF[p^{mn}]$ are in this additive-group of rank t, and any external mark A_{t+1} forms with the t marks A_r a system of $t+1$ linearly independent marks, and thus extends the additive-group of rank t to one of rank $t+1$. We take as a start any mark $A_1 \neq 0$, and by the preceding remarks may affirm: (a) There exist systems of l marks $A_1, A_2, \cdots, A_l$ of the $GF[p^{mn}]$ linearly independent with respect to the $GF[p^n]$ for every l, $l = 1, 2, \cdots, m$; (b) every additive-group $[A_1, A_2 \cdots, A_t \mid GF[p^n]]$ may be exhibited as an additive-group of some rank $l \leqq t$ based upon such a system of l linearly independent marks chosen from amongst the original t basal marks A_r.

9. We take now any system of $k+1$ (not necessarily distinct) marks B_g $(g=0, 1, \cdots, k)$ of the $GF[p^{mn}]$ and consider the two marks

$$\Delta \equiv D[k+1, n;\, p]\ (B_0, B_1, \ldots B_k) \equiv |B_j^{p^{ni}}| \quad (i, j=0, \cdots, 1, k), \tag{17}$$

$$\Pi \equiv P[k+1, n;\, p](B_0, B_1, \cdots, B_k) \equiv \Pi^* \sum_g \alpha_g B_g \quad (g = 0, 1, \cdots, k). \tag{18}$$

Clearly $\Pi = 0$ if and only if the marks B_g are linearly dependent. And further, since from an equation,

$$\sum_{j=0}^{j=k} \alpha_j B_j = 0,$$

*In the sequel the $GF[p^n]$ is always the field of reference.

we have, by II_1' Cor., the $k+1$ equations,

$$\left(\sum_{j=0}^{j=k} a_j B_j\right)^{p^{ni}} \equiv \sum_{j=0}^{j=k} a_j B_j^{p^{ni}} = 0 \qquad (i=0,1\ldots,k),$$

we see that if the marks B_g are linearly dependent, then $\triangle=0$.

(In passing we notice that the remark just made concerning Π and the theorem $\mathrm{III}[k+1, n; p]$ yield the theorem:

A necessary and sufficient condition that $k+1$ marks B_g $(g=0, 1,\cdots, k)$ of a $GF[p^{mn}]$ (m any integer) shall be linearly dependent with respect to the $GF[p^n]$ is the vanishing of the determinant $\triangle \equiv | B_j^{p^{ni}} |$ $(i, j=0, 1\cdots, k)$. (If $m < k+1$, then $\triangle$ vanishes for every system of $k+1$ marks B_g). This yields its still more important corollary:

The rank of the additive-group $[B_0, B_1\cdots, B_k \mid GF[p^n]]$ is the same as the rank of the matrix $(B_j^{p^{ni}})$ $(i, j=0, 1,\cdots, k)$, where a matrix (u_{ij}) $\binom{i=0,1,\ldots,k}{j=0,1,\ldots,l}$ is said to have the *rank* r if its every sub-determinant of order $r'>r$ vanishes while at least one sub-determinant of order $r'=r$ does not vanish.

It would not be difficult to establish this theorem and its corollary independently of the theorem $\mathrm{III}[k+1, n; p]$.)

10. Next we consider a system of $k (k+1 \leqq m)$ linearly independent marks A_r $(r=0, 1,\cdots, k-1)$, and select from the p^{kn} marks A of the additive-group $[A_1, A_2\cdots, A_k \mid GF[p^n]]$ any $k+1$ marks B_g $(g=0, 1, \cdots, k)$. These marks B_g are linearly dependent, for otherwise the additive-group based on them would have the order $p^{(k+1)n}$, whereas it is contained in the additive-group of order p^{kn} based on the k marks A_r. For these marks B_g then (§ 9) $\triangle=0$, $\Pi=0$, and so

$$(19)\quad D[k+1, n; p](B_0, B_1,\cdots, B_k) = P[k+1, n; p](B_0, B_1,\cdots, B_k).$$

11. We take now any system of $2k^2 (2k^2 \leqq m)$ linearly independent marks $E_{rs}\binom{r=0,1,\ldots,k-1}{s=1,2,\ldots,2k}$ and split it up at once into k systems of $2k$ linearly independent (§8) marks.

The system $E_{rs} (s=1, 2,\cdots 2k)$ determines the additive-group $[E_{r1}, E_{r2}, \cdots, E_{r2k} \mid GF[p^n]]$ containing besides the mark 0 $p^{2kn}-1$ marks A_r of the form $A_r = \sum_{s=1}^{s=2k} \varepsilon_{rs} E_{rs}$, where the ε_{rs} are marks of the $GF[p^n]$ not all 0. We select from each additive-group any mark A_r $(A_r \neq 0)$ $(r=0, 1,\cdots, k-1)$. These k marks A_r are linearly independent, and determine the additive-group $[A_0, A_1,\cdots, A_{k-1} \mid GF[p^n]]$ containing

p^{kn} marks A of the form $A = \sum_{r=0}^{r=k-1} a_r A_r$. By §10 we have for every such mark A

(20) $$D[k+1, n; p](A_0, A_1, \cdots, A_{k-1}, A) = 0.$$

Hence the equation for X_k

(21) $$D[k+1, n; p](A_0, A_1, \cdots, A_{k-1}, X_k) = 0.$$

which is of degree p^{kn} in the unknown X_k with the leading coefficient $D[k, n; p](A_0, A_1, \cdots, A_{k-1})$ has as roots the p^{kn} marks A of the form $A = \sum_{r=0}^{r=k-1} a_r A_r$. Since the marks A are given equally well in the form $A = -\sum_{r=0}^{r=k-1} a_r A_r$, we have the identity in the indeterminate X_k:

(22) $$D[k+1, n; p](A_0, A_1, \cdots, A_{k-1}, X_k) \equiv$$
$$D[k, n; p](A_0 A_1, \cdots A_{k-1}) \cdot \prod_{\substack{a_r \mid p^n \\ (r=0, 1, \ldots, k-1)}} \left(\sum_{r=0}^{r=k-1} a_r A_r + X_k\right).$$

Now consider the two forms in the $k+1$ indeterminates $X_0, X_1, \cdots, X_k$:

(23) $$D[k+1, n; p](X_0, X_1, \cdots, X_{k-1}, X_k),$$
$$D[k, n; p](X_0, X_1, \cdots, X_{k-1}) \cdot \prod_{\substack{a_r \mid p^n \\ (r=0, \ldots, k-1)}} \left(\sum_{r=0}^{r=k-1} a_r X_r + X_k\right).$$

We affirm their identity: this is the theorem III ♮ $[k+1, n; p]$. Denoting by $C(X_0, X_1, \cdots, X_{k-1})$, $C'(X_0, X_1, \cdots, X_{k-1})$ the coefficients of any certain same power of X_k in the respective forms (23), we prove the identity in the k indeterminates $X_0, X_1, \cdots, X_{k-1}$:

(24) $$C(X_0, X_1, \cdots, X_{k-1}) \equiv C'(X_0, X_1, \cdots, X_{k-1}).$$

In the first place these forms are of degree $\leqq p^{kn}$ in each indeterminate. Further by (22)

(25) $$C(A_0, A_1, \cdots, A_{k-1}) = C'(A_0, A_1, \cdots, A_{k-1})$$

where for $r = 0, 1, \cdots, k-1$ A_r is any of the $p^{2kn}-1$ $(p^{2kn}-1 > p^{kn})$ marks $A_r \neq 0$ of the additive-group $[E_{r1}, E_{r2}, \cdots, E_{r2k} \mid GF[p^n]]$. The desired identity (24) follows then by the *identity-theorem* (which is proved in the Galois-field theory just as is the corresponding theorem in the theory of the ordinary general algebraic field):

Identity-theorem. If the two forms of the $GF[p^{mn}]$
$$C(Y_1, Y_2, \cdots, Y_l), \quad C'(Y_1, Y_2, \cdots, Y_l)$$

contain the l indeterminates $Y_1, Y_2, \cdots, Y_l$ to degrees respectively less than the numbers $y_1, y_2, \cdots, y_l$, and if to each indeterminate Y_h $(h=1, 2, \cdots, l)$ a certain system of y_h distinct marks A_h may be associated in such a way that the two marks obtained from the two forms by substituting for each indeterminate Y_h any mark A_h of its associated set are equal:

$$C(A_1, A_2, \cdots, A_l) = C'(A_1, A_2, \cdots, A_l):$$

then the two forms are identical:

$$C(Y_1, Y_2, \cdots, Y_l) \equiv C'(Y_1, Y_2, \cdots, Y_l).$$

Proof C of the theorem III $[k+1, n; p]$. §§ 12–14.

Proof by one-based induction. We know that III $[2,n;p] \equiv \mathrm{II}_3'$ is true. On the supposition that III $[l, n; p]$ $(l>1)$ is true we prove that III $[l+1, n; p]$ is true.

12. By interchanging two adjacent columns of the determinant $| X_j^{p^{ni}} |$ $(i,j=0, 1,\cdots,l)$ we have:

$$(26) \qquad \begin{aligned} &D[l+1, n; p](\cdots,X_h,X_{h+1},\cdots)\equiv \\ &-D[l+1, n; p](\cdots,X_{h+1},X_h,\cdots). \end{aligned}$$

13. To prove the corresponding property for the product $P[l+1, n; p](X_0,X_1,\cdots,X_l)$ we need the Galois-field generalization of *Wilson's theorem:*

II_2' Cor. 1 $\qquad \prod'_{a \,|\, p^n} a=-1 \qquad (a \neq 0),$

whence

II_2' Cor. 2 $\qquad \prod'_{a \,|\, p^n} a^{p^{hn}}=-1 \qquad (a \neq 0)$ (*h any integer*),

even for $p=2$, since in a Galois-field of modulus $p=2$ the marks $+1, -1$ are equal.

In view of the definition (4) the two products

$$(27) \qquad \begin{aligned} &P[l+1, n; p](\cdots,X_h, X_{h+1},\cdots), \\ &P[l+1, n; p](\cdots,X_{h+1},X_h,\cdots) \end{aligned}$$

obviously differ only in the factors $\sum_{g=0}^{g=l} a_g X_g$, $\sum_{g=0}^{g=l} \beta_g X_g$ containing both X_h and X_{h+1} and no X_g with $g>h+1$, that is, in the products

$$(28) \qquad \prod'_{\substack{a \,|\, p^n \\ (a \neq 0)}} \prod_{\substack{a_g \,|\, p^n \\ (g=0, \ldots, h-1)}} \left(\sum_{g=0}^{g=h-1} a_g X_g + a X_h + X_{h+1} \right),$$

$$\prod'_{\substack{\beta \,|\, p^n \\ (\beta \neq 0)}} \prod_{\substack{\beta_g \,|\, p^n \\ (g=0, \ldots, h-1)}} \left(\sum_{g=0}^{g=h-1} \beta_g X_g + \beta X_{h+1} + X_h \right).$$

Setting, for any $\alpha \neq 0, \beta = 1/\alpha, \beta_g = \alpha_g/\alpha$ $(g=0, 1, \cdots, h-1)$, we find easily that the first product (28) is the second product (28) multiplied by $\prod'_{\alpha \mid p^n} \alpha^{p^{hn}} (\alpha \neq 0)$, *i. e.*, ($\text{II}_2'$ Cor. 2) by -1. Hence indeed:

$$(29) \qquad P[l+1, n; p](\cdots, X_h, X_{h+1}, \cdots) \equiv -P[l+1, n; p](\cdots, X_{h+1}, X_h, \cdots).$$

We have from (26) (29):

$$(30) \qquad D[l+1, n; p](X_0, \cdots, X_{h-1}, X_h, X_{h+1}, \cdots, X_l) \equiv (-1)^{l-h} D[l+1, n; p](X_0, \cdots, X_{h-1}, X_{h+1}, \cdots, X_l, X_h),$$

$$(31) \qquad P[l+1, n; p](X_0, \cdots, X_{h-1}, X_h, X_{h+1}, \cdots, X_l) \equiv (-1)^{l-h} P[l+1, n; p](X_0, \cdots, X_{h-1}, X_{h+1}, \cdots, X_l, X_h).$$

14. Now the two forms

$$(32) \qquad D[l+1, n; p](X_0, X_1, \cdots, X_l), P[l+1, n, p](X_0, X_1, \cdots, X_l)$$

are of degree p^{ln} in each of the $l+1$ indeterminates X_h $(h=0, 1, \cdots, l)$; the respective coefficients of $X_l^{p^{nl}}$ are obviously

$$(33) \qquad D[l, n; p](X_0, X_1, \cdots, X_{l-1}), P[l, n; p](X_0, X_1, \cdots, X_{l-1}),$$

and hence by (30, 31, 33) the respective coefficients of $X_h^{p^{nl}}$ $(h=0, 1, \cdots, l)$ are

$$(34) \qquad (-1)^{l-h} D[l, n; p](X_0, \cdots X_{h-1}, X_{h+1}, \cdots, X_l), \quad (-1)^{l-h} P[l, n; p](X_0, \cdots, X_{h-1}, X_{h+1}, \cdots, X_l).$$

From (34) and our hypothesis that III $[k+1, n; p]$ is true for $k+1=l$ it follows that the form

$$(35) \qquad D[l+1, n; p](X_0, X_1, \cdots, X_l) - P[l+1, n; p](X_0, X_1, \cdots, X_l)$$

is of degree less than p^{ln} in each of the $l+1$ indeterminates X_h $(h=0, 1, \cdots, l)$. We take in the $GF[p^{mn}]$ $(m \geqq k \geqq l)$ any system of l marks $A_r (r=0, 1 \cdots, l-1)$ linearly independent with respect to the $GF[p^n]$, and associate with each indeterminate X_h $(h=0, 1, \cdots, l)$ the p^{ln} marks $A = B_h$ of the additive-group based on the marks A_r. Then, since by § 10 (19) for every such system of $l+1$ (linearly dependent) marks B_h $(h=0, 1, \cdots, l)$ we have

$$(36) \qquad D[l+1, n; p](B_0, B_1, \cdots, B_l) - P[l+1, n; p](B_0, B_1, \cdots B_l) = 0,$$

by the identity-theorem (§ 11) we have the desired identity III$[l+1, n; p]$:

$$D[l+1, n; p](X_0, X_1, \cdots, X_l) - P[l+1, n; p](X_0, X_1, \cdots, X_l) \equiv 0.$$

THE UNIVERSITY OF CHICAGO,
January 30, 1896.