

ON THE MATRICES OF PERIOD A POWER OF
 p IN JORDAN'S LINEAR CONGRUENCE
 GROUPS, MODULO p^a .

BY DR. ARTHUR RANUM.

(Read before the American Mathematical Society, October 27, 1906.)

Introduction.

IN contrasting Jordan's* linear congruence groups, modulo p^a , with the more general "groups of classes of congruent matrices, modulo (p^{av}) ", which I have recently discovered,† it appears that in general the latter groups cannot be abstractly identical with any of the former groups of the same degree or subgroups thereof, and are therefore new groups of that degree, abstractly as well as concretely. The proof of this assertion given in the paper just referred to depends for its validity on certain properties of Jordan groups to be derived in this note. These properties have to do with the matrices of period a power of p . Moreover a formula is found for the ν th power of any matrix.

The ν th Power of a Matrix.

1. Consider any n -ary matrix $M = (m_{ij})$, where m_{ij} ($i, j = 1, \dots, n$) is the element in the i th row and j th column. Denote its ν th power by $M^\nu = (m_{ij}^{(\nu)})$, where ν is a positive integer. Then $m_{ij}^{(1)} = m_{ij}$ ($i, j = 1, \dots, n$).

For many purposes, including the application to Jordan groups that is to follow, it is convenient to put $m_{ii} = 1 + l_{ii}$, $m_{ij} = l_{ij}$ ($i, j = 1, \dots, n$; $i \neq j$), *i. e.*, to write M in the form

$$\begin{pmatrix} 1 + l_{11} & l_{12} & \cdots \\ l_{21} & 1 + l_{22} & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix},$$

and to express its ν th power in terms of the partial elements l_{ij} ($i, j = 1, \dots, n$). If the symbolic addition and subtraction, as well as multiplication, of matrices be defined in the usual way,

* Jordan, *Traité des substitutions* (1870), pp. 91-110, and in particular pp. 103-105.

† *Transactions Amer. Math. Society*, vol. 8, No. 1 (Jan., 1907), pp. 71-91.

and if the special matrix (δ_{ij}) , where $\delta_{ij} = \begin{cases} 1, & \text{if } i=j \\ 0, & \text{if } i \neq j \end{cases}$, be denoted by I , then we have $(m_{ij}^{(\nu)}) = (\delta_{ij}) + (l_{ij}^{(\nu)})$, *i. e.*, $M = I + L$. Therefore

$$(1) \quad M^\nu = (I + L)^\nu = I + \sum_{\mu=1}^{\nu} \binom{\nu}{\mu} L^\mu,$$

which is equivalent to the n^2 equations

$$(2) \quad m_{ij}^{(\nu)} = \delta_{ij} + \sum_{\mu=1}^{\nu} \binom{\nu}{\mu} l_{ij}^{(\mu)} \quad (i, j = 1, \dots, n),$$

by means of which the elements of M^ν are expressed in terms of the corresponding elements of the powers of L from the first up to the ν th. Moreover, since every element of L^μ is a homogeneous function, of degree μ , of the elements of L , every element $m_{ij}^{(\nu)}$ of M^ν is a non-homogeneous function, of degree ν , of the partial elements l_{ij} ($i, j = 1, \dots, n$) of M , and its terms of degree μ are together equal to $\binom{\nu}{\mu} l_{ij}^{(\mu)}$.

2. To find these terms of degree μ , *i. e.*, to express L^μ ($\mu = 2, \dots, \nu$) in terms of L , there are at least two distinct methods of procedure.

(a) Since $L^\mu = LL^{\mu-1}$, we have the recursion formulas

$$(3) \quad l_{ij}^{(\mu)} = \sum_{k=1}^n l_{ik} l_{kj}^{(\mu-1)} \quad \left(\begin{array}{l} i, j = 1, \dots, n, \\ \mu = 2, \dots, \nu \end{array} \right),$$

by means of which every element of L^μ is expressed in terms of the elements of a single row of L and a single column of $L^{\mu-1}$.

(b) Putting $L^0 = I$ and denoting by d_r ($r = 1, \dots, n$) the sum of the principal $(n-r)$ th minors of the determinant of L , so that d_n is the determinant itself, we can write the identical equation* that L satisfies in the form

$$L^n = \sum_{r=1}^n (-1)^{r-1} d_r L^{n-r}.$$

If $\mu \geq n$, we multiply this equation by $L^{\mu-n}$ ($\mu = n, \dots, \nu$) and derive the equations

$$(4) \quad L^\mu = \sum_{r=1}^n (-1)^{r-1} d_r L^{\mu-r} \quad (\mu = n, n+1, \dots, \nu),$$

* Cayley, "Collected mathematical papers," vol. 2, pp. 482-492. Frobenius, *Crelle's Journal*, vol. 84, pp. 1-16. Taber, *Amer. Jour. of Mathematics*, vol. 12 (1890), pp. 357, 358.

which are equivalent to the recursion formulas *

$$(5) \quad l_{ij}^{(\mu)} = \sum_{r=1}^n (-1)^{r-1} d_r l_{ij}^{(\mu-r)} \quad \left(\begin{array}{l} i, j=1, \dots, n, \\ \mu=n, n+1, \dots, \nu \end{array} \right),$$

in which d_r ($r=1, \dots, n$) is independent of i, j and μ . By means of (5) every element of L_μ ($\mu \cong n$) is expressed in terms of the corresponding elements of the n next lower powers of L and the principal minors of the determinant of L .

3. By repeated applications of (3) or (5) all the powers of L from L^2 to L^ν can be computed, except that if $n > 2$, (3) must be used to find the first $n-1$ powers, after which either (3) or (5) can be used to find the rest. Finally, the substitution of the values so obtained in (2) gives the ν th power of M in the required form.

Jordan Groups: Certain Invariant Subgroups.

4. Let G be an n -ary Jordan group, or linear congruence group, modulo p^a , where p is a prime and a is a positive integer, *i. e.*, G comprises the totality of the n -ary matrices, whose elements are residues of p^a and whose determinants are prime to p , these matrices combining with each other by multiplication. In G consider the invariant subgroup H_b , whose matrices are congruent to the matrix I , modulo p^b ($b \cong a$), and are therefore of the form $I + p^b L$. Clearly $H_0 = G$ itself, and $H_a = I$. If $b > 0$, H_b is of order $p^{n^2(a-b)}$ and its matrices are all of period a power of p . These groups H_0, H_1, \dots, H_a form a series, each of which contains the next in order and therefore all that follow it.

5. If, in order to indicate the fundamental modulus p^a , we introduce the additional subscript a and write G_a for G and $H_{b,a}$ for H_b , then it is clear that $G_a/H_{b,a} = G_b$ ($b=0, \dots, a$), and, more generally, that $H_{b,a}/H_{c,a} = H_{b,c}$ ($b, c=0, \dots, a; b \cong c$).

6. THEOREM 1.† *The commutator of a matrix of H_b and a matrix of H_c is a matrix of H_{b+c} if $b+c \cong a$; while if $b+c \cong a$, every matrix of H_b is commutative with every matrix of H_c .*

Proof. Let $L_b = I + p^b L$ and $M_c = I + p^c M$ be any two

* For the cases $n=2$ and $n=3$ these formulas were derived by direct calculation, without the use of the identical equation, by Weltzien, "Ueber Produkte und Potenzen von Determinanten," Berlin, 1897.

† The first part of this theorem was proved by Jordan for the case $c=1$, *Traité des substitutions*, p. 104.

matrices of H_b and H_c respectively. Then

$$\begin{aligned} L_b M_c &\equiv I + p^b L + p^c M + p^{b+c} LM, \pmod{p^a}, \\ \text{and} \\ M_c L_b &\equiv I + p^b L + p^c M + p^{b+c} ML, \pmod{p^a}. \end{aligned}$$

Therefore, if $b + c \leq a$,

$$\begin{aligned} L_b M_c &\equiv M_c L_b, \pmod{p^{b+c}}, \\ \text{i. e.,} \\ L_b^{-1} M_c^{-1} L_b M_c &\equiv I, \pmod{p^{b+c}}, \end{aligned}$$

which proves the theorem.

Corollaries. Putting $c = a - b$, we see that if $b \leq a/2$, every matrix of H_{a-b} is invariant in H_b . Again, putting $c = b$, we see that if $b \leq a/2$, all the commutators of H_b are contained in H_{2b} ; while if $b \geq a/2$, H_b is abelian. Therefore if a is even ($= 2a'$), $H_{a'}$ is abelian; while if a is odd ($= 2a' - 1$), $H_{a'}$ is abelian.

7. Let the totality of the matrices of H_b that are not contained in its subgroup H_{b+1} be denoted by $H_b - H_{b+1}$. Supposing $a > 1$, consider the subgroups H_1, \dots, H_a , leaving H_0 out of account.

THEOREM 2. *Every matrix of $H_b - H_{b+1}$ ($b = 1, \dots, a - 1$)* is of period p^{a-b} , except when $b = 1$ and $p = 2$.*

Proof. Let $L_b = I + p^b L$ be any matrix of H_b . Then by (1),

$$L_b^{p^{a-b}} \equiv I, \pmod{p^a},$$

and the period of L_b is a divisor of p^{a-b} . Moreover,

$$L_b^{p^{a-b-1}} \equiv I + p^{a-1} L + \binom{p^{a-b-1}}{2} p^{2b} L^2 + \dots, \pmod{p^a},$$

where the remaining terms are all divisible by p^a , and, except when $b = 1$ and $p = 2$, the third term also; so that the congruence reduces to the form

$$L_b^{p^{a-b-1}} \equiv I + p^{a-1} L, \pmod{p^a}.$$

Now if the period of L_b is less than p^{a-b} , L is divisible by p and L_b is contained in H_{b+1} . This proves the theorem.

* A simple example, for $n = 2$, is $\begin{pmatrix} 1 & 0 \\ p & 1 \end{pmatrix}$.

Moreover, it is easy to see that if $p = 2$, $H_1 - H_2$ contains matrices not only of period 2^{a-1} , but also of periods $2^{a-2}, \dots, 2$.*

Jordan Groups: Sylow Subgroups of Order a Power of p.

8. In the n -ary Jordan group G , modulo p^a , consider the totality of matrices of the form

$$M = \begin{pmatrix} 1 + p\lambda_{11} & p\lambda_{12} & \cdots & p\lambda_{1n} \\ \lambda_{21} & 1 + p\lambda_{22} & \cdots & p\lambda_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ \lambda_{n1} & \lambda_{n2} & \cdots & 1 + p\lambda_{nn} \end{pmatrix} = I + L,$$

in which

$$(6) \quad l_{ij} \equiv 0, \pmod p \quad (i, j = 1, \dots, n; i - j \leq 0).$$

It is easy to verify that they form a group of order $p^{n^2(a-1) + \frac{1}{2}n(n-1)}$ and therefore a Sylow subgroup of G .† Call it H and its conjugates $H', H'',$ etc. The greatest common subgroup of $H, H',$ etc., is evidently H_1 , the periods of whose matrices have been determined in § 7.

9. It remains to find the periods of the matrices of $H - H_1$. In order to raise M to the ν th power by means of (1) and (2), it will be necessary to find the p -factors (powers of p that are factors) of the elements of the different powers of L .

From (6) we derive by induction the formula

$$(7) \quad l_{ij}^{(\mu)} \equiv 0, \pmod p \quad (i, j = 1, \dots, n; i - j \leq \mu - 1).$$

For, by (3), we have

$$l_{ij}^{(\mu+1)} = \sum_{k=1}^n l_{ik} l_{kj}^{(\mu)},$$

every term of which, in view of (6)_{ik} and (7)_{kj}, is divisible by p , if $i - j \leq \mu$. Therefore (7) holds for all values of μ .

Moreover,

$$l_{1n}^{(2)} = \sum_{k=1}^n l_{1k} l_{kn}$$

* E. g., the binary matrix $\begin{pmatrix} -1 & 0 \\ 2^{b-1} & -1 \end{pmatrix}$, of period 2^{a-b} ($b = 1, \dots, a - 1$).

† This fact was pointed out to me by Professor Dickson.

is divisible by p^2 . From this fact, by induction, we derive the formula

$$(8) \quad l_{ij}^{(\mu)} \equiv 0, \pmod{p^2} \quad (\mu \geq 2; i, j = 1, \dots, n; i-j \leq \mu-1-n).$$

For we have

$$l_{ij}^{(\mu+1)} = \sum_{k=1}^{i-1} l_{ik}^{(\mu)} l_{kj}^{(\mu)} + \sum_{k=i}^n l_{ik}^{(\mu)} l_{kj}^{(\mu)},$$

which is divisible by p^2 , if $i-j \leq \mu-n$.

The more general formula

$$(9) \quad \begin{aligned} l_{ij}^{(\mu)} &\equiv 0, \pmod{p^{b+1}} \\ [\mu &\geq (b-1)n + 2; i, j = 1, \dots, n, i-j \leq \mu-1-bn], \end{aligned}$$

of which (7) and (8) are special cases, can be proved in a similar manner.

Since $i-j$ is always less than n , (9) gives rise to the formula

$$(10) \quad \begin{aligned} l_{ij}^{(\mu)} &\equiv 0, \pmod{p^b} \\ (b &= 1, 2, \dots; \mu = bn, bn+1, \dots; i, j = 1, \dots, n); \end{aligned}$$

i. e., every element of L^{bn}, L^{bn+1}, \dots is divisible by p^b .

10. If M be chosen such that

$$(11) \quad l_{ij} \equiv 0, \pmod{p} \quad (i, j = 1, \dots, n; i-j \leq k-1),$$

then by a similar process the formulas

$$(12) \quad l_{ij}^{(\mu)} \equiv 0, \pmod{p} \quad (i, j = 1, \dots, n; i-j \leq k\mu-1),$$

and

$$(13) \quad \begin{aligned} l_{ij}^{(\mu)} &\equiv 0, \pmod{p^2} \\ [\mu &\geq 2; i, j = 1, \dots, n; i-j \leq k(\mu-1)-n], \end{aligned}$$

can be derived.

11. We are now prepared to prove

THEOREM 3. *If $p > n-1$, p^a is the highest power of p that is the period of any matrix of the n -ary Jordan group, modulo p^a .*

Proof. Let $M = I + L$ be any matrix of H . Then

$$M^{p^a} \equiv I + \sum_{\mu=1}^{p^a} \binom{p^a}{\mu} L^\mu, \pmod{p^a}.$$

Suppose that the G. C. D. of μ and p^a is p^b . Then it is clear that $\binom{p^a}{\mu}$ is divisible by p^{a-b} . Moreover, since $p \geq n$, therefore $p^b \geq bn$, and $\mu \geq bn$. Consequently, by (10), every ele-

ment of L^μ is divisible by p^b . Therefore, finally,

$$M^{p^a} \equiv I, \pmod{p^a};$$

i. e., the period of every matrix of H is a divisor of p^a . Moreover, matrices whose period is exactly p^a exist in $H - H_1$,* and the theorem is proved.

If $n = 2$, the condition $p > n - 1$ is always satisfied and the theorem is true for all values of p .

If $a = 1$, and $p > n - 1$, the theorem shows that every matrix of $H - I$ is of period p .

12. By a similar argument we derive the more general

THEOREM 4. *If $p^b < n \leq p^{b+1}$, then p^{a+b} is the highest power of p that is the period of any matrix of the n -ary Jordan group, modulo p^a .*

Moreover, matrices of period p^a, \dots, p^{a+b} evidently exist in $H - H_1$.†

13. The question now arises whether $H - H_1$ also contains matrices of lower period than p^a .

THEOREM 5. *If $p > n + 1$, the period of every matrix of $H - H_1$ is exactly p^a .*

Proof. The proof consists in showing that if the period of a matrix M of H is less than p^a , then M must belong to H_1 . Assume that $M^{p^{a-1}} \equiv I, \pmod{p^a}$. Since

$$M^{p^{a-1}} = I + \sum_{\mu=1}^{p^{a-1}} \binom{p^{a-1}}{\mu} L^\mu,$$

it follows that

$$\sum_{\mu=1}^{p^{a-1}} \binom{p^{a-1}}{\mu} L^\mu \equiv 0, \pmod{p^a},$$

which gives rise to the n^2 congruences

$$(14) \quad \sum_{\mu=1}^{p^{a-1}} \binom{p^{a-1}}{\mu} l_{ij}^{(\mu)} \equiv 0, \pmod{p^a} \quad (i, j=1, \dots, n).$$

Remembering that the elements l_{ij} satisfy (6), we wish to show, as a consequence of (14), that they are divisible by p for all values of i and j .

* *E. g.*, if $n = 2$, the matrix $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.

† *E. g.*, if $n = 3, p = 2, a = 1$, and therefore $b = 1$, the matrix $\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$, belonging to $H - I$, is of period 4.

In the first place, of the n^2 congruences (14), those for which $i - j \equiv 0$ are identically satisfied. For, by (7), $l_{ij}^{(\mu)}$ is in this case always divisible by p ; moreover, if the G. C. D. of μ and $p^{\alpha-1}$ is p^b , $\binom{p^{\alpha-1}}{\mu}$ is divisible by $p^{\alpha-b-1}$, and since $p > 1 + n$, $p^b > 1 + bn$, so that, in view of (9), $l_{ij}^{(\mu)}$ ($i - j \equiv 0$) is divisible by p^{b+1} .

Next, in those congruences (14) for which $i - j = 1$, exactly the same reasoning applies to every term except the first. Therefore, those congruences reduce to the form $p^{\alpha-1}l_{ij} \equiv 0, \text{ mod } p^{\alpha}$ ($i - j = 1$), or $l_{ij} \equiv 0, \text{ mod } p$ ($i - j = 1$), which, combined with (6), becomes

$$(15) \quad l_{ij} \equiv 0, \text{ mod } p \quad (i - j \leq 1).$$

If $n = 2$, this proves the theorem. If $n > 2$, this additional limitation on L makes it possible to reduce those congruences (14), for which $i - j = 2, 3$, to a simple form. For, putting $k = 2$ in (12), we see that $l_{ij}^{(\mu)} \equiv 0, \text{ mod } p$ ($\mu > 1; i - j = 2, 3$). Moreover, putting $k = 2$ and $\mu = p$ in (13), and noting that since $p > n + 1$, $2(p - 1) - n > n \geq 3$, we see that, if μ is divisible by p , $l_{ij}^{(\mu)}$ ($i - j = 2, 3$) is divisible by p^2 . A fortiori, if μ is divisible by p^b , $l_{ij}^{(\mu)}$ ($i - j = 2, 3$) is divisible by p^{b+1} . Therefore those congruences (14), for which $i - j = 2, 3$, reduce to the form $p^{\alpha-1}l_{ij} \equiv 0, \text{ mod } p^{\alpha}$ ($i - j = 2, 3$) or $l_{ij} \equiv 0, \text{ mod } p$ ($i - j = 2, 3$).

If $n = 3$ or 4, this proves the theorem. If $n > 4$, another application of (12) and (13), putting $k = 4$, shows that $l_{ij} \equiv 0, \text{ mod } p$ ($i - j = 4, 5, 6, 7$); and by continuing this process we finally see that l_{ij} is divisible by p for all values of i and j , and therefore that the theorem is true for all values of n .

14. If $p \leq n + 1$, it is easy to see that theorem 5 is not true, and that $H - H_1$ contains matrices of period $p, p^2, \dots, p^{\alpha-1}$, as well as p^{α} . Indeed $G - H_1$ contains matrices of period $2, 3, \dots, n, n + 1$, independently of any modulus. *E. g.*, if $n = 4$, $G - H_1$ contains the matrix

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix},$$

which is equivalent to the linear substitution $x'_1 = x_2, x'_2 = x_3,$

$x'_3 = x_4, x'_4 = x_1$, and is therefore of period 4, independently of any modulus. A fortiori, $G - H_1$ contains similar matrices of period 2 and 3. Moreover, the matrix

$$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & -1 & -1 & -1 \end{bmatrix},$$

also of $G - H_1$, is of period 5, independently of any modulus. For it is equivalent to the linear substitution $x'_1 = x_2, x'_2 = x_3, x'_3 = x_4, x'_4 = -x_1 - x_2 - x_3 - x_4$, and if x_0 be defined by the equation $x_0 + x_1 + x_2 + x_3 + x_4 = 0$, then the linear substitution is equivalent to the cyclic permutation $(x_0 x_1 x_2 x_3 x_4)$, which is of period 5.

Jordan Groups: Final Results.

15. By combining the results obtained in §§ 7, 11-14, we see that the periods of the matrices of $H - H_1$ are (a) $p, \dots, p^a, \dots, p^{a+b}$, if $p \leq n - 1$, (b) p, \dots, p^a , if $p = n$ or $n + 1$, (c) p^a , if $p > n + 1$. Moreover, if we divide the matrices of period a power of p into the classes $\Sigma(H - H_1), H_1 - H_2, H_2 - H_3, \dots, H_{a-1} - I$, where $\Sigma(H - H_1) = (H - H_1) + (H' - H_1) + \dots$, we have the means of determining, for any given values of n and p , the exact range of the periods of the matrices in each class.

The following table gives these periods for a few small values of n and p .

	$\Sigma(H - H_1)$	$H_1 - H_2$	$H_2 - H_3 \dots H_{a-1} - I$
$n=2 \begin{cases} p=2 \\ p=3 \\ p=5 \end{cases}$	$2^a, \dots, 2$ $3^a, \dots, 3$ 5^a	$2^{a-1}, \dots, 2$ 3^{a-1} 5^{a-1}	$2^{a-2} \dots 2$ $3^{a-2} \dots 3$ $5^{a-2} \dots 5$
$n=5 \begin{cases} p=2 \\ p=3 \\ p=5 \\ p=7 \end{cases}$	$2^{a+2}, 2^{a+1}, 2^a, \dots, 2$ $3^{a+1}, 3^a, \dots, 3$ $5^a, \dots, 5$ 7^a	$2^{a-1}, \dots, 2$ 3^{a-1} 5^{a-1} 7^{a-1}	$2^{a-2} \dots 2$ $3^{a-2} \dots 3$ $5^{a-2} \dots 5$ $7^{a-2} \dots 7$

The groups of simplest structure are those in which $p > n + 1$. In every such group we have an exhaustive classification of the matrices of period a power of p , viz., those of period p^b ($b = 1, \dots, a - 1$) belong to $H_{a-b} - H_{a-b+1}$, and those of period p^a to $\Sigma(H - H_1)$.

16. As applied to these groups, Theorem 1 can now be stated in the following more significant form :

THEOREM 6. *In an n -ary Jordan group, modulo p^a , for which $p > n + 1$, the commutator of a matrix of period p^b and a matrix of period p^c is a matrix whose period is p^{b+c-a} or a lower power of p , if $b + c \geq a$, while if $b + c \leq a$, every matrix of period p^b is commutative with every matrix of period p^c .*

Under the same restriction that $p > n + 1$ we have the

Corollaries : In the subgroup generated by the matrices of period $p^b (b \geq a/2)$, every matrix of period p^{a-b} is invariant. The commutator of any two matrices of period $p^b (b \geq a/2)$ is a matrix whose period is p^{2b-a} or a lower power of p ; while if $b \leq a/2$, any two matrices of period p^b are commutative. If $b \leq a/2$, the matrices whose periods are divisors of p^b form an abelian subgroup of G .

CORNELL UNIVERSITY,
December, 1906.

ON THE CONSTRUCTION OF AN INTEGRAL OF LAGRANGE'S EQUATIONS IN THE CALCULUS OF VARIATIONS.

BY DR. D. C. GILLESPIE.

(Read before the American Mathematical Society, December 29, 1906.)

1. DARBOUX* has proven the theorem :

$$\text{When (1) } \int_1^2 F(y', y, x) dx \quad \text{and (2) } \int_1^2 F'(y', y, x) dx$$

$$(y' = dy/dx)$$

lead to the same Lagrange equation ; *i. e.*, when the first variation of integrals (1) and (2) equated to zero give the same differential equation (3) $y'' = \omega(y', y, x)$, where $y'' = d^2y/dx^2$, then $F_{y'y'}/F'_{y'y'} = \text{const.}$ (literal subscripts denote partial derivatives) is an intermediary of equation (3).

2. This theorem can be proven with very little algebraic work by making use of Hilbert's † independence theorem (Unabhängigkeitssatz).

* Darboux, *Théorie des surfaces*, vol. 3, pp. 59-65.

† Hilbert's *Vorlesungen über Variationsrechnung*, Winter-Semester, 1904-1905.