THE SUBGROUPS OF THE QUATERNARY ABELIAN LINEAR GROUP*

BY

HOWARD H. MITCHELL

1. Introduction

With the possible exception of the binary modular groups there is no finite linear group which is of more importance in analysis and geometry than what is known as the *abelian*† linear group. In the investigations of Hermite and Jordan the coefficients were taken as rational integers reduced modulo p (a prime), in which case it is the Galois group of the equation for the p-section of the periods of hyperelliptic functions.‡ It is also the group of isomorphisms of a certain type of commutative group and is isomorphic with certain systems of collineation groups.§

For the case of four variables and the modulus 3, it is the group of the equation for the 27 straight lines on a general cubic surface‖ as well as the group for the problem of reducing a binary sextic to the canonical form $T^2 - U^3$. One of the collineation groups with which it is isomorphic in this case is the quaternary G_{25920}, which has received considerable attention.

If the coefficients of the transformations, instead of being integers reduced modulo p, are taken as marks of a general Galois field $GF(p^n)$, a more general group is obtained which has been investigated by Dickson.¶ This group requires an even number of variables and has a certain invariant bilinear function analogous to that for the ordinary continuous group in space which

* Presented to the Society at New York, April 25, 1914.

† This group is called abelian on account of its connection with abelian functions. It is not commutative.

‡ Cf. Jordan, *Traité des substitutions*, pp. 171–186; 354–369; Witting, Mathematische Annalen, vol. 29 (1886), p. 157; Dissertation (Göttingen, 1887); Burkhardt, Mathematische Annalen, vol. 38 (1891), p. 163.

§ Cf. Jordan, loc. cit., pp. 420–450; Witting, loc. cit.; Burkhardt, loc. cit.; Dickson, these Transactions, vol. 1 (1900), pp. 30–38; the author, Bulletin of the American Mathematical Society, vol. 20 (1913), pp. 134–138.

‖ Cf. Jordan, loc. cit., pp. 316–319; Dickson, *Linear Groups*, pp. 303–307; Coble, Johns Hopkins University Circular (1908) no. 7, pp. 80–88.

¶ Quarterly Journal of Mathematics, vol. 29 (1897), pp. 169–178, vol. 31 (1899), pp. 383–4; *Linear Groups*, pp. 89–109.

has an invariant linear complex. It is called *general* or *special* according as this function is left relatively (to within a factor in the field) or absolutely invariant. The first has an invariant subgroup of order $p^n - 1$ consisting of all the transformations which multiply each variable by the same mark of the field, and the second has for $p > 2$ an invariant subgroup of order 2 which contains a transformation changing the sign of each variable. The quotient group of the second with respect to its invariant subgroup of order 2, Dickson has denoted by the symbol, $A(2m, p^n)$, $2m$ representing the number of variables. For $p = 2$ the *special* group is itself represented by this symbol. These groups are simple except for $m = 1$, $p^n = 2, 3$ and $m = 2$, $p^n = 2$.

The object of this paper is the determination of the maximal subgroups of the $A(2m, p^n)$ for $m = 2$ and $p > 2$, although incidentally some other subgroups are noticed. For this purpose we consider the collineation group in a modular space* having an invariant linear complex. The group of all such collineations is $(1, 1)$ isomorphic with the quotient group of the *general* linear group with respect to its invariant subgroup of order $p^n - 1$. For $p > 2$ it contains an invariant subgroup of index 2, each transformation in which multiplies the linear function of the plücker line coördinates by a square in the field. This multiplier may be made unity by multiplying each coefficient of the collineation by the same properly chosen factor. This group is thus $(1, 1)$ isomorphic with the quotient group of the *special* linear group with respect to its invariant subgroup of order 2, i. e. with Dickson's $A(4, p^n)$. We shall depart slightly from Dickson's notation and shall represent the whole collineation group by $A_\nu(p^n)$ and its invariant subgroup by $A_1(p^n)$.

Although considerable work has been done on the determination of the subgroups, the problem seems to have been completely solved only for $n = 1$, $p = 3$.† For the general case Dickson has found a complete list of conjugate operators,‡ and has discussed a number of the subgroups.§ He has also shown that for $n = 1$, $p > 3$ there is no subgroup of index less than

$$p^3 + p^2 + p + 1.\|$$

The author has obtained a complete set of maximal subgroups in the general case. The possible subgroups whose orders are prime to the modulus p were

* Cf. Veblen and Bussey, these Transactions, vol. 7 (1906), pp. 241–259.

† Dickson, these Transactions, vol. 5 (1904), pp. 126–166. Jordan had previously shown that there was no subgroup of index less than 27 (loc. cit., pp. 319–329).

‡ These Transactions, vol. 2 (1901), pp. 103–138.

§ These Transactions, vol. 1 (1900), pp. 91–96; vol. 4 (1903), pp. 371–386; vol. 5 (1904), pp. 1–38; Quarterly Journal of Mathematics, vol. 32 (1900), pp. 42–63; Bulletin of the American Mathematical Society, vol. 10 (1903), pp. 178–184.

‖ These Transactions, vol. 6 (1905), pp. 48–57. Cf. also Jordan, loc. cit., p. 666, note *E*.

determined in a previous paper.* They were found to be the same as the ordinary finite groups which have an invariant linear complex.

With the exception of a few groups which exist only for particular moduli the subgroups whose orders are divisible by p are found to be of two general types. Those of the first type are the $A_1(p^k)$, if k is a factor of n, and the $A_\nu(p^k)$, if $2k$ is a factor of n. Those of the second type are analogous to the ordinary continuous groups which have an invariant linear complex. They have an invariant point and plane, a congruence (three types), a quadric (two types), or a twisted cubic.

As a check on our list of maximal subgroups we find that they agree with Dickson's† for the special case $n = 1$, $p = 3$. For this case he found them to be of indices 27, 36, 40, 40, 45. We also find that for $p^n > 3$ there is no subgroup of index less than $p^{3n} + p^{2n} + p^n + 1$, a result due to him‡ for $n = 1$.

2. General Properties of the Group

There are three types of transformations of period p in $A_1(p^n)$ if $p > 3$ and two types if $p = 3$. The first, which we shall refer to as *central elations*, leave fixed all the points in a plane and all the planes and lines through a point in that plane. All the lines in the plane of fixed points which pass through the point of fixed planes belong to the invariant complex.

The transformations of the second type leave invariant all the points on a line and every line of a flat pencil through each point of the axis. We shall refer to them as *skew elations*. The axis belongs to the complex as do also two of the above mentioned pencils. The coördinates of these pencils need not be in the $GF(p^n)$ however.

The transformations of the third type have a single invariant point, an invariant line through that point and an invariant plane through that line. All the lines in the fixed plane which pass through the fixed point belong to the complex. The path curves are conics in the fixed plane and twisted cubics outside of that plane. If $p = 3$ these transformations are of period 9.

There are two types of transformations of period 2 in $A_1(p^n)$.§ Both of them leave invariant all the points on each of two skew lines, but in the one case these lines are lines of the complex and in the other they are axes of a congruence contained by the complex. In the former case the coördinates of these lines are or are not in the $GF(p^n)$ according as p^n has the form $4l + 1$ or $4l - 1$. In the latter case their coördinates are always in the $GF(p^n)$.

* These Transactions, vol. 14 (1913), pp. 123–142. This paper will be referred to as Transactions I.

† Loc. cit.

‡ Loc. cit.

§ For a more general result see Dickson, *Linear Groups*, § 289; Annals of Mathematics, ser. 2, vol. 6 (1905), p. 148.

3. Groups Containing Central Elations

We proceed now to prove

THEOREM 1. *The only subgroups of* $A_1(p^n)$ *which contain central elations are*:

(1) *groups having an invariant point and plane with coördinates in the* $GF(p^n)$;

(2) *groups having an invariant line of the complex with coördinates in the* $GF(p^n)$;

(3) *groups having an invariant congruence hyperbolic with respect to the* $GF(p^n)$;

(4) *groups of the same type and order as* $A_1(p^k)$, *where* k *is a factor of* n;

(5) *groups of the same type and order as* $A_\nu(p^k)$, *where* $2k$ *is a factor of* n.

We consider a particular subgroup of $A_1(p^n)$ and suppose that the largest subgroup it contains which consists of central elations with common center and axial plane is of order p^k. We denote such a group by (E_1). If all the other centers of elations are in the axial plane of (E_1), either that plane or a line in that plane through the center of (E_1) must remain invariant. If this is not the case we may suppose the existence of a second group of elations (E_2) with center not in the axial plane of (E_1).

These two additive groups leave invariant in common the line joining their centers and the line of intersection of their axial planes. The group generated cannot by hypothesis contain an additive group of elations of higher order than p^k. Hence its order on the line joining the centers must be

$$\tfrac{1}{2}(p^k + 1)p^k(p^k - 1)$$

or $60\,(p^k = 3)$.* The group itself is of twice this order, since it contains an invariant reflection whose axes are axes of the invariant congruence. We shall first assume either that $p^k > 3$ or that if $p^k = 3$ no group of order $2 \cdot 60$ of this type is present. The exceptional case will be considered later.

In the general case, if the invariant complex be $p_{14} + p_{23} = 0$, every group of the sort described may be shown to be conjugate under $A_\nu(p^n)$ with that generated by

$$(E_1) : [x_1, x_2 + \lambda x_3, x_3, x_4], \qquad (E_2) : [x_1, x_2, \lambda x_2 + x_3, x_4],$$

where λ takes all values in the $GF(p^k)$.

Either the invariant congruence of this group must remain fixed or else there will be elations with centers not on either of the two axes. We denote one such group of elations by (E_3). The line through its center which is in the congruence is a line of the complex and hence must be in the axial plane of (E_3).

* The binary modular groups for the general Galois field were first determined by E. H. Moore and Wiman. For a new determination of these groups and for references to the earlier work the reader may consult a paper by the author in these Transactions, vol. 12 (1911), pp. 207–211.

The center of (E_3) must be in one of the $p^k + 1$ planes conjugate with the axial planes of (E_1) and (E_2) under the group generated by them. For the group (E_3) cannot be commutative with both (E_1) and (E_2) and hence we may suppose that it is not commutative with (E_2). Hence (E_2) and (E_3) must generate a group of the same sort as the above and this will contain an invariant reflection. This reflection and the one commutative with (E_1) and (E_2) must generate a dihedral group of order $2p$ under which the reflections are conjugate. If the center of (E_3) does not lie in one of the $p^k + 1$ planes mentioned above, its center will be conjugate under this group with a point on the line joining the centers of (E_1) and (E_2), which is distinct from any of the $p^k + 1$ centers on that line. But this is impossible. Hence the center of (E_3) must be in one of the $p^k + 1$ planes and we may suppose that it is in the axial plane of (E_1).

Since the group generated by (E_1) and (E_2) is invariant under all transformations of the form

$$[\alpha x_1 + \beta x_4, x_2, x_3, \gamma x_1 + \delta x_4],$$

where $\alpha, \beta, \gamma, \delta$ are any marks of the $GF(p^n)$ such that $\alpha\delta - \beta\gamma = 1$, it follows that we may choose the center of (E_3) as $(1\ 1\ 0\ 0)$. In order that (E_2) and (E_3) shall generate a group of order $(p^k + 1)p^k(p^k - 1)$ the latter must be given by

$$[x_1 + \lambda(x_3 + x_4), x_2 + \lambda(x_3 + x_4), x_3, x_4].$$

We then find that the group of the points in the invariant plane, $x_4 = 0$, is of order $(p^k + 1)p^k(p^k - 1) \cdot p^{2k}$. There is in addition a group of elations of order p^k leaving fixed all the points in $x_4 = 0$. For in the group generated by (E_1) and (E_3) are contained all the transformations

$$[x_1 + \lambda(x_3 + x_4), x_2 - \lambda(x_3 - x_4), x_3, x_4].$$

The group conjugate with (E_3) under the reflection commutative with (E_1) and (E_2) is

$$[x_1 - \lambda(x_3 - x_4), x_2 + \lambda(x_3 - x_4), x_3, x_4].$$

As products of these we obtain a group of elations of order p^k having $(1\ 0\ 0\ 0)$ and $x_4 = 0$ for center and axial plane. Hence the group generated by (E_1), (E_2), and (E_3) is of order $p^{4k}(p^{2k} - 1)$.

If now $(1\ 0\ 0\ 0)$ and $x_4 = 0$ do not remain invariant there must be a group of elations (E_4) with center not in $x_4 = 0$. Its center must lie in at least one of each set of $p^k + 1$ planes similar to those considered above. Hence it must lie in one of the lines through $(1\ 0\ 0\ 0)$ in which $p^k + 1$ of these planes meet. There are p^{2k} of these lines and they are all conjugate under the group generated by (E_1), (E_2), and (E_3). Hence we may take

a center on $x_2 = 0$, $x_3 = 0$, and since that group is invariant under any elation with center $(1\ 0\ 0\ 0)$ and axial plane $x_4 = 0$, we may suppose it to be $(0\ 0\ 0\ 1)$. The group (E_4) must then be given by

$$[x_1, x_2, x_3, \lambda x_1 + x_4].$$

Under the group now generated there are $p^{3k} + p^{2k} + p^k + 1$ conjugate groups of elations, their centers being the points with coördinates in the $GF(p^k)$. The subgroup which leaves $(1\ 0\ 0\ 0)$ and $x_4 = 0$ invariant must be of order at least $1/2(p^k - 1) \cdot p^{4k}(p^{2k} - 1)$. For the group generated by (E_4) and the additive group having $(1\ 0\ 0\ 0)$ and $x_4 = 0$ for center and axial plane must contain the transformation $[\epsilon x_1, x_2, x_3, \epsilon^{-1} x_4]$, where ϵ is a primitive root in the $GF(p^k)$. In $x_4 = 0$ this is an homology of period $p^k - 1$, whereas in the group generated by (E_1), (E_2), and (E_3) there are no homologies in that plane of higher period than 2.

The order of the whole group generated must then be at least

$$\tfrac{1}{2}(p^{4k} - 1)p^{4k}(p^{2k} - 1).$$

But this is exactly the order of $A_1(p^k)$ and all four groups of elations are contained by that group.

If $A_1(p^k)$ is a subgroup of $A_1(p^n)$, k must be a factor of n, and if $A_\nu(p^k)$ is a subgroup of $A_1(p^n)$, $2k$ must be a factor of n. The groups of either of these types form a single conjugate set under $A_\nu(p^n)$. If n/k is odd the groups of the type of $A_1(p^k)$ also form a single conjugate set under $A_1(p^n)$. If n/k is even, the groups of the type of $A_1(p^k)$ or $A_\nu(p^k)$ each form two conjugate sets under $A_1(p^n)$.

The subgroup of all transformations in $A_1(p^n)$ which leave invariant a point and a plane through it whose coördinates are in the $GF(p^n)$ is of order $1/2\, p^{4n}(p^{2n} - 1)(p^n - 1)$. The subgroup of all such transformations which leave invariant a line of the complex with coördinates in the $GF(p^n)$ is of the same order. The subgroup of all such transformations which leave invariant a congruence which is hyperbolic with respect to the $GF(p^n)$ is of order $p^{2n}(p^{2n} - 1)^2$. The groups of each of these three types form a single conjugate set under $A_1(p^n)$.

We still have to consider the case where $p^k = 3$ and the group generated by two elations is of order $2 \cdot 60$. Such a group is generated by

$$(E_1) : [x_1, x_2 + x_3, x_3, x_4]; \qquad (E_2) : [x_1, x_2, ix_2 + x_3, x_4],$$

where $i^2 = -1$. It may be proved just as in the general case that the centers of all elations which can exist must be in one of the axial planes of this group. We consider therefore a third elation, whose center and axial plane we may take to be $(1\ 1\ 0\ 0)$ and $x_3 + x_4 = 0$. It must generate with (E_2) a group

of order $2 \cdot 12$ or $2 \cdot 60$. The reflection invariant under this group is

$$(R) : [-x_1 + 2x_2, x_2, x_3 + 2x_4, -x_4].$$

The group generated by (E_1) and (E_2) contains the transformation

$$(S) : [x_1, ix_2, -ix_3, x_4].$$

It is readily found that the group generated by the elations which are conjugate with (E_1) under the group generated by (R) and (S) contains a group of elations of order 3^2 having $(1\ 0\ 0\ 0)$ and $x_4 = 0$ for center and axial plane. But this is contrary to our assumption that $p^k = 3$.

4. Groups Containing Skew Elations but no Central Elations

We establish the following theorems:

Theorem 2. *Any subgroup of $A_1(p^n)$ which does not contain central elations cannot contain two skew elations with different axes if the axis of either is a fixed line of the other.*

If E_1 and E_2 are two skew elations with the same invariant complex and such that each leaves fixed the axis of the other, then it is easy to prove that $E_1^{-1} E_2^{-1} E_1 E_2$ is a central elation. If E_1 leaves fixed the axis of E_2, but E_2 does not leave fixed the axis of E_1, then $E_2^{-1} E_1 E_2$ and E_1 will have different axes but each will leave fixed the axis of the other. Hence a central elation will appear in this case also.

Theorem 3. *In any subgroup of $A_1(p^n)$ which does not contain central elations any two skew elations with different axes must leave invariant in common either all the lines of a regulus or the two axes of a congruence.*

Two skew elations with different axes must leave invariant the two axes of a congruence if their axes intersect, one of which is in the plane of their axes and the other of which passes through the point of intersection of their axes. If their axes do not intersect they must leave invariant at least one line in common, since their product can leave fixed no points which are not on a line left invariant by both. If they leave invariant only one line in common there must be in all cases among the products of their powers transformations with two fixed points on that line. Some power of such a transformation must be a skew elation having the invariant line for axis. But this is impossible, since its axis would be left invariant by the skew elations which generate the group. Hence the two generating skew elations must leave invariant either the two axes of a congruence or all the lines of a regulus.

Theorem 4. *Any subgroup of $A_1(p^n)$ which contains skew elations, but no central elations, and which leaves invariant the two axes of a congruence, must be $(1, 1)$ or $(2, 1)$ isomorphic with the groups of the points on the two axes, with the exception of three groups of order $2 \cdot 4 \cdot 3$, $2 \cdot 4 \cdot 12$, $2 \cdot 4 \cdot 24$, which exist for $p = 3$.*

We notice that if there are any transformations which leave invariant all the points on one axis, the group generated by them must form an invariant subgroup. If there are any such transformations which are of period p on the second axis either they are central elations or some of their powers are central elations. The group on an axis cannot contain an invariant subgroup of order prime to p except for $p = 3$, in which case it must be of order 12 or 24. This readily leads to the exceptional groups noted in the theorem.

THEOREM 5. *Any subgroup of $A_1(p^n)$, which contains skew elations but no central elations, and which leaves invariant the two axes of a congruence, must contain subgroups of order $1/2\, p(p^2 - 1)$ which leave invariant all the lines of a regulus, provided that no point on either axis remains fixed.*

Any group of the sort described in the theorem must contain one or more subgroups which are of order $1/2p(p^2 - 1)$ on each axis of the congruence. In such a subgroup there will be skew elations whose product is of period 2 on each axis. But any such transformation in $A_1(p^n)$ may easily be shown to be a skew perspectivity leaving fixed all the points on each of two lines in the congruence. Since the product of the two skew elations can leave invariant no point which is not on a line left invariant by both, it follows that they must leave invariant in common all the lines of a regulus.

THEOREM 6. *Any subgroup of $A_1(p^n)$ containing an additive group of skew elations of higher order than 3, but no central elations, must leave invariant a point and plane, a congruence, or a quadric.*

An additive group of skew elations with a common axis will leave invariant either a pencil of lines (i. e., all the lines of the pencil) through each point of the axis, two pencils neither of which belongs to the complex, a single pencil belonging to the complex, or no pencils whatever. We denote the largest subgroup of the whole additive group which leaves invariant a pencil through each point of the axis by $H^{(R)}$ and suppose that its order is p^k.

If no point or line remains invariant under the group, $H^{(R)}$ must be contained either by a group leaving invariant all the lines of a regulus or by a group leaving invariant the two axes of a congruence. The latter must however contain subgroups of the former type and some of these will contain $H^{(R)}$. The largest group containing $H^{(R)}$ which leaves invariant all the lines of a regulus must be of order $1/2p^k(p^{2k} - 1)$, $p^k(p^{2k} - 1)$, or 60 $(p^k = 3)$. We denote one such group by $G^{(R)}$.

If there is another skew elation having the same axis as $H^{(R)}$, it must generate with $G^{(R)}$ a group having an invariant congruence. This congruence cannot be parabolic, since in that case there would be skew elations present having but one invariant line in common. The group generated must be of order $1/2p^m(p^{2m} - 1)$ or $p^m(p^{2m} - 1)$ on each axis of the congruence, m being a multiple of k. We denote this group by $G^{(C)}$ and its additive subgroup of order p^m, which is commutative with $H^{(R)}$, by $H^{(C)}$.

The group $G^{(C)}$ must contain subgroups of order $1/2(p^m - 1)$ or $p^m - 1$ on each axis of the congruence, which permute the operators of $H^{(C)}$ among themselves. Some of these will contain cyclic subgroups of order $1/2(p^k - 1)$ or $p^k - 1$ which belong to $G^{(R)}$. These are skew perspectivities which leave invariant all the points on each of two axes of elations in $G^{(R)}$. A group of order $1/2(p^m - 1)$ or $p^m - 1$ which leaves two such axes invariant must be of period on each of them greater than or equal to $p^k + 1$.* The period will clearly be greater than this unless $m = 2k$, in which case it may conceivably be $1/2(p^k + 1)$. In this case however $G^{(R)}$ would contain a skew perspectivity of order $p^k - 1$ and hence would be of order $p^k(p^{2k} - 1)$. It therefore contains also skew perspectivities of order $p^k + 1$. Under $G^{(C)}$ one of these would be commutative with the one of order $p^k - 1$. Hence the period on the two axes of elations could not in this case be less than $p^k + 1$.

If now there are other skew elations which have the same axis as $H^{(C)}$, there must be other groups of the same sort as $G^{(C)}$ containing $G^{(R)}$. There must then be more than one cyclic group leaving fixed two particular axes of elations in $G^{(R)}$ and the period of neither on these axes can be less than $p^k + 1$. The group generated by these cyclic groups must in all cases contain transformations which are of period p on each axis. Either such a transformation is a skew elation or else a power of it is a skew elation. But this is impossible since it would leave fixed the two axes of elations in $G^{(R)}$.

Hence in all cases the whole additive group of skew elations having a common axis must leave invariant either a pencil through each point of the axis or else two pencils. We will show that in the latter case a congruence (the invariant congruence of $G^{(C)}$) must remain invariant. Suppose this is not the case. Then there must be an elation with axis not in the congruence. It must generate with $H^{(R)}$ a group having either an invariant congruence or else an invariant regulus. In the former case there will be in the group generated subgroups of the latter type and not more than one of these can be in $G^{(C)}$. Any one of these must be of order $1/2p^k(p^{2k} - 1)$, and one of them must generate with $H^{(C)}$ a group of order $1/2p^m(p^{2m} - 1)$. The axes of the invariant congruence of this group will meet the axis of $H^{(C)}$ in the same points as the axes of the invariant congruence of $G^{(C)}$, i. e., the two points through which pass the two invariant pencils.

Hence $H^{(C)}$ will be left invariant by more than one metacyclic group, for the whole metacyclic group in a $G^{(C)}$ which leaves $H^{(C)}$ invariant can leave invariant but one congruence, as may be readily shown. The group generated by two transformations which permute the operators of $H^{(C)}$ in the same way, but which have different invariant congruences, will contain skew elations

* $G^{(R)}$ cannot now be of order 60, since $G^{(C)}$ would in that case contain a subgroup of order 360 permuting the same ten axes of elations and hence leaving the same regulus invariant.

with the same axis as $H^{(C)}$, which permute the lines of the two pencils. But this is impossible, as shown above.

We suppose finally that the entire additive group of skew elations is identical with $H^{(R)}$, i. e., leaves invariant a pencil of lines through each point of the axis. We will show that if $p^k > 3$ a regulus (the invariant regulus of $G^{(R)}$) must remain invariant. For if there be a skew elation not in $G^{(R)}$ it must generate with $H^{(R)}$ either a $G^{(C)}$ or another $G^{(R)}$. In the latter case the two $G^{(R)}$ must generate a $G^{(C)}$. If $p^k > 3$ every $G^{(C)}$ contains an additive group of order p^m, where m is a multiple of k. If $p^k = 3$ there are exceptional $G^{(C)}$ of order 60, $2\cdot 60$, $2\cdot 4\cdot 3$, $2\cdot 4\cdot 12$, $2\cdot 4\cdot 24$. That of order $2\cdot 4\cdot 3$ may be generated by two skew elations whose axes intersect and contains no $G^{(R)}$.

It is perhaps worth while here to discuss briefly the groups which have an invariant congruence or an invariant regulus. If the congruence is parabolic, or if it is hyperbolic with respect to the $GF(p^n)$, such groups are subgroups of subgroups which contain central elations. If the congruence is elliptic with respect to the $GF(p^n)$, there are no central elations in $A_1(p^n)$ which leave it invariant. The order of the largest subgroup of $A_1(p^n)$ which leaves one of these congruences invariant is $p^{2n}(p^{4n} - 1)$. The totality of all such subgroups is a single conjugate set under $A_1(p^n)$.

There are two types of reguli, all the lines of which belong to the complex. In the one case there are two real lines of the conjugate regulus which belong to the complex and in the other these two lines are conjugate imaginary with respect to the $GF(p^n)$. The largest subgroup of $A_1(p^n)$ which leaves a regulus of the former type invariant is $(p^n + 1)p^n(p^n - 1)^2$. In the other case the largest subgroup is of order $(p^n + 1)^2 p^n(p^n - 1)$. The groups of each sort form a single conjugate set under $A_1(p^n)$. Neither of them is a maximal subgroup for $p^n = 3$. In that case the former leaves invariant both a hyperbolic and an elliptic congruence and the latter is a subgroup of a group of order 960 to be discussed later.

THEOREM 7. *If $p = 3$ every subgroup of $A_1(p^n)$ which contains skew elations but no central elations must leave invariant a point and plane, a congruence, or a regulus with the exception of two groups of order $16\cdot 60$ and $16\cdot 120$. The latter is a subgroup of $A_1(3^n)$ only if n is even.*

We first consider those subgroups which contain $G^{(C)}$ of order $2\cdot 4\cdot 12$ or $2\cdot 4\cdot 24$. Each of these contains C_4 which are the identity on one axis of the congruence and are of period 2 on the other. We will show that any reflection which is conjugate with the invariant reflection of this subgroup must be commutative with it, i. e., must interchange its axes.

Suppose first that there are two such reflections whose axes intersect. Their product will then be a skew elation. Consider a C_4 of the sort described above which is commutative with one of these reflections. It will either

transform the skew elation into another one having the same axis or will transform it into another one whose axis is left fixed by the first. In the first case there would be an additive group of skew elations present of higher order than 3. The second case is impossible by a previous theorem.

Suppose now that there are two such reflections whose axes do not intersect. If they do not interchange each other's axes their product cannot be of period less than 4. They must leave invariant in common all the lines of a regulus, since their axes are axes of congruences contained by the complex. A C_4 having one of them for its square must generate with the other a group which leaves two of the lines of this regulus invariant. If no additive group of higher order than 3 is present the group on each of these lines must be of order 24. But there must then be present reflections of the type considered whose products are skew elations.

Hence in any case two reflections which are squares of such C_4 must interchange each other's axes. The only groups which can contain $G^{(C)}$ of order $2\cdot4\cdot12$ or $2\cdot4\cdot24$ may then be shown* to be two groups of order $16\cdot60$ and $16\cdot120$ having an invariant G_{16}.

We suppose finally that the only $G^{(C)}$ which can be present are of order 60 or $2\cdot60$. We may then prove much as in Transactions I (under Theorem 13) that there must be commutative C_3. The proof that the R, A, and B of that discussion must leave invariant two lines in common is different, but may be made easily geometrically. But we have considered here the case where commutative C_3 are present.

5. Groups which Contain no Central Elations and no Skew Elations, but which Contain Skew Perspectivities of Higher Period than 2

The determination of the groups which contain no central elations or skew elations may be made much as in Transactions I, pp. 125–134. This is especially the case when the groups contain skew perspectivities of higher period than 2. Most of the general properties of the groups as stated there, p. 125, still hold if transformations of period p with a single fixed point are present. There are however the exceptions that if $p = 5$ two skew perspectivities of period 3 which generate a group of order 60, in which the operators of period 5 have each a single fixed point, leave invariant but one line in common. Also two reflections whose product is of period p can have but one fixed line in common. Much of the discussion is simplified on account of the limitation of the present discussion to those groups which have an invariant complex. Aside from this the differences are very slight. The results may be summarized as follows:

Theorem 8. *Any subgroup of $A_1(p^n)$ which does not contain central*

* Cf. Transactions I, p. 128.

elations or skew elations, but which contains skew perspectivities of higher period than 2, *has either an invariant regulus or congruence or else is a group of one of the following orders*: $16\cdot120$, $16\cdot60$, 360, 720, 2520, 5040. *Those of order* $16\cdot60$ *and* 360 *exist in every* $A_1(p^n)$, *that of order* $16\cdot120$ *only for* $p^n = 8h \pm 1$, *that of order* 720 *only for* $p^n = 12f \pm 1$, *that of order* 2520 *only for* $p = 7$, *and that of order* 5040 *only for* $p = 7$ *and* n *even.*

The groups occurring here which have invariant reguli or congruences are subgroups of those previously discussed. In the case of the groups of order $16\cdot120$ and $16\cdot60$, the axes of the five reflections contained by the invariant G_{16} which are axes of congruences must have coördinates in the $GF(p^n)$. The axes of the other ten are lines of the complex and must be real or conjugate imaginary with respect to the $GF(p^n)$ according as p^n has the form $4l + 1$ or $4l - 1$. These ten reflections are in the $G_{16\cdot120}$ the squares of skew perspectivities of period 4, which exist in $A_1(p^n)$ only if $p^n = 8h \pm 1$.

A $G_{16\cdot120}$ is generated by

$$\begin{bmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & -1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} a & 0 & 0 & b \\ 0 & a & b & 0 \\ 0 & b & d & 0 \\ b & 0 & 0 & d \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 \\ 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{bmatrix},$$

where $a + d = 2$, $a^2 + 2b^2 + d^2 = 0$. These groups always exist in $A_\nu(p^n)$ and form a single conjugate set under that group, and (if they exist) two conjugate sets under $A_1(p^n)$. The subgroups of order $16\cdot60$ always exist in A_1, and if $p^n = 8h \pm 3$, they form a single conjugate set under A_1.

To determine when the other groups are subgroups of A_1 we distinguish two cases according as the axes of the skew perspectivities of period 3 are real or conjugate imaginary with respect to the $GF(p^n)$, i. e., according as $p^n = 3k + 1$ or $3k - 1$. The G_{360} may be generated by three such C_3 of which two are commutative and the third generates a G_{12} with one and a G_{60} with the other. If their axes are real we find that (if we consider conjugacy under A_ν) they may be taken to be

$$(1\,0\,0\,0)(0\,1\,0\,0), \qquad (0\,0\,1\,0)(0\,0\,0\,1);$$

$$(1\,0\,0\,0)(0\,0\,1\,0), \qquad (0\,1\,0\,0)(0\,0\,0\,1);$$

$$(0\,1\,1\,1)(1\,0\,1\,-1), \qquad (0\,-2\,1\,1)(-2\,0\,1\,-1).$$

A G_{720} containing this G_{360} must also contain the reflection whose axes are $(1\,i\,0\,0)(0\,0\,1\,i)$, $(1\,-i\,0\,0)(0\,0\,1\,-i)$, where $i^2 + 1 = 0$. These are axes of a congruence and hence the G_{720} are subgroups of A_1 only if they are real, i. e., if $p^n = 4l + 1$, and hence $p^n = 12f + 1$.

If the axes of the C_3 are conjugate imaginary with respect to the field, i. e.,

if $p^n = 3k - 1$, we may take the G_{360} to be generated by the three C_3, C_3', C_3'', C_3''' where one axis of C_3' is

$$(1\ 0\ 0\ \omega)(0\ 1\ \omega\ 0),$$

one axis of C_3'' is

$$(0\ 1\ \omega\ 0)(1\ 0\ 0\ \omega^2)$$

and one axis of C_3''' is

$$(1 - \lambda\alpha, -\alpha, -\alpha\omega^2, \omega^2 - \lambda\alpha\omega)(1, \alpha + \lambda, \alpha\omega^2 + \lambda\omega, \omega^2)$$

where $\omega^2 + \omega + 1 = 0$, $\alpha\alpha' = 1$, $\lambda\lambda' = -1$, α' and λ' being the conjugates of α and λ. The G_{720} must also contain the reflection whose axes are

$$(i\alpha, 1, \omega, i\alpha\omega)(1, i\alpha, i\alpha\omega^2, \omega^2)$$

and

$$(-i\alpha, 1, \omega, -i\alpha\omega)(1, -i\alpha, -i\alpha\omega^2, \omega^2).$$

These must be real and this is the case if i does not exist in the field, i. e., if $p^n = 4l - 1$ and hence also $p^n = 12f - 1$.

Hence A_1 has primitive subgroups of order 360 in all cases ($p > 3$), whereas it has primitive subgroups of order 720 only if $p^n = 12f \pm 1$. These groups form each a single conjugate set under A_ν, whereas the G_{720} (if they exist) form two conjugate sets under A_1, and the G_{360} (if the G_{720} do not exist) form a single conjugate set under A_1.

The G_{2520} has an invariant complex only if $p = 7$ and the G_{5040} exists only in this case. The axes of the C_3 are then real and we may take the first choice of coörd nates for a subgroup of order 360. The G_{2520} must also contain the C_3 whose axes are $(1\ 2\ 0\ 0)(0\ 0\ 3\ 1)$ and $(1\ 3\ 0\ 0)(0\ 0\ 2\ 1)$. The G_{5040} is generated by the G_{720} and this C_3. It appears in A_1 only if n is even. In this case A_1 contains two conjugate sets of G_{5040}, whereas if n is odd it contains a single conjugate set of G_{2520}.

6. Groups which Contain no Central Elations, no Skew Elations, and no Skew Perspectivities of Higher Period than 2

The results to be obtained in this section may be summarized in the following theorem.

Theorem 9. *The only subgroups of $A_1(p^n)$ which contain no central elations, no skew elations, and no skew perspectivities of higher period than 2, are subgroups either of groups previously considered or of a group of order $1/2p^n(p^{2n} - 1)$ having an invariant twisted cubic.*

The groups of this type whose orders are prime to p and which do not have an invariant congruence or regulus are of order $16\cdot5$, $16\cdot10$, $16\cdot20$, 60, 120. These are subgroups respectively of groups of order $16\cdot60$, $16\cdot60$, $16\cdot120$, 360, 720. It is only necessary to consider the groups which contain trans-

formations of period p. We may also in consequence of the discussion in Transactions I, p. 132, assume that these groups do not contain reflections whose axes are axes of congruences. We may also suppose that no transformation other than the identity can leave fixed the axes of more than one reflection. It may also easily be shown that two cyclic groups can have no transformations (other than the identity) in common unless both are contained by a larger cyclic group.

We consider an additive group of order p^m and suppose a transformation in this additive group to be

$$S : [x_1 + ax_2 + bx_3 + cx_4, x_2 + dx_3 + ex_4, x_3 + fx_4, x_4],$$

where $a \neq 0$, $d \neq 0$, $f \neq 0$. If $p_{14} + p_{23} = 0$ is invariant we must have $a + f = 0$, $b - e + df = 0$. If the additive group is invariant under a metacyclic group there must be present transformations such as

$$T : [\alpha x_1, \beta x_2, \beta^{-1} x_3, \alpha^{-1} x_4],$$

the period of which is a divisor of $p^m - 1$. The transformation $T^{-1}ST$ must be commutative with S. For otherwise if we denote $T^{-1}ST$ by S_1, then $S^{-1}S_1^{-1}SS_1$ would be either a central elation or a skew elation. This leads to the conditions $\alpha = \beta^3$, $b + e = 0$.

We inquire next under what conditions the cyclic group of order d_1 generated by T can be invariant under a group of order $4d_1$ which contains transformations making a cyclic permutation of period 4 on the vertices of its invariant tetrahedron. This leads to $\beta^{10} = 1$ and hence $d_1 = 5$.

If now we denote the order of the whole group by Ω, it is clear that there must be in the group $(p^m - 1)\Omega/d_1 p^m$ additive transformations. If $d_1 > 3$ any maximal cyclic group of order d_1 can be invariant only under groups of order d_1, $2d_1$, or $4d_1$, and in the last case we must have $d_1 = 5$. In the same way any other maximal cyclic group of order d_i can be invariant only under groups of order d_i, $2d_i$, or $4d_i$, and in the last case it may easily be shown that d_i can be divisible only by primes of the form $4l + 1$. There must then be $(d_i - 1)\Omega/f_i d_i$ transformations in each conjugate set of cyclic groups, where $f_i = 1, 2, 4$.

If we attempt to enumerate the transformations which the group must contain we are led to the diophantine equation

$$\Omega = 1 + (p^m - 1)\Omega/d_1 p^m + \sum_{i=1}^{r} (d_i - 1)\Omega/f_i d_i.$$

This equation is slightly different if the metacyclic group is of order $2p^m$ or $3p^m$, for transformations of period 2 or 3 which leave the additive group invariant may be contained by cyclic groups of higher order which do not

leave it invariant. Hence if the first denominator were $2p^m$ or $3p^m$ we could conclude only that d_1 is divisible by 2 or 3 respectively. The first would give an equation of essentially the same type as that considered in Transactions I under Theorem 14 and no solutions exist which correspond to groups. The second leads to either $r = 2, f_1 = f_2 = 2$ or $r = 2, f_1 = 2, f_2 = 4$.

Since p^m must have the form $6f + 1$, and since d_1 and d_2 can have no odd factor in common, it follows that in the first of these two cases $d_2 = 2$. If $d_1 = 6$, we obtain $\Omega = 3p^m$, which is impossible. Hence $d_1 \geqq 9$. This leads to $p^m < 12$ and hence $p^m = 7$. We then have $d_1 < 14$ and consequently $d_1 = 9, 12$. For $d_1 = 9$ there is no solution, whereas for $d_1 = 12$ we obtain $\Omega = 168$. This solution however can correspond to no group, since there would be seven cyclic groups of order 12 and hence the invariant reflection in any one of these groups wou'd have to interchange the axes of each of the other six reflections of the same sort. This is easily seen to be impossible.

In the second case, since $f_2 = 4$, it follows that d_1 must be divisible by 12. Since Ω must be the least common multiple of $3p^m$, $2d_1$, and $4d_2$, we have $\Omega = 2p^m d_1 d_2$. This leads to

$$4d_1 d_2 + 6p^m d_2 + 3p^m d_1 = 6 + p^m d_1 d_2.$$

If $4d_1 d_2$ is the largest term on the left, it follows that $p^m < 12$ and hence $p^m = 7$. We then conclude that either $d_1 < 28$ or $d_2 < 14$, and hence that $d_1 = 12, 24$ or $d_2 = 5, 13$. None of these leads to a solution. The same result is obtained if $6p^m d_2$ or $3p^m d_1$ is supposed the largest term on the left.

We now take up the discussion of the general case. If no f_i has the value 4, the equation may be solved exactly as in a previous paper by the author.* The only solutions which need concern us here are:

$$r = 2, \quad f_1 = f_2 = 2, \quad d_1 = \tfrac{1}{2}(p^m - 1), \quad d_2 = \tfrac{1}{2}(p^m + 1),$$
$$\Omega = \tfrac{1}{2}p^m(p^{2m} - 1);$$
$$r = 2, \quad f_1 = f_2 = 2, \quad d_1 = p^m - 1, \quad d_2 = p^m + 1,$$
$$\Omega = p^m(p^{2m} - 1).$$

It will be shown later that there are groups which correspond to these two solutions.

We now suppose that at least one f_i has the value 4. If $f_1 = 4$, then (as shown above) $d_1 = 5$. Then one of the d's, say d_2, must be divisible by 4 and hence $f_2 = 1, 2$. It is evident from the equation that $f_2 = 2$ is the only possibility, since otherwise the sum of the coefficients of Ω on the right would exceed unity. It may then be seen from the equation that $r = 3$,

* These Transactions, vol. 12 (1911), p. 210.

$f_3 = 4$. Hence d_3 can be divisible only by primes of the form $4l + 1$, and since $d_1 = 5$, it follows that $d_3 \not< 13$. Since $p^m \not< 11$, we find that $d_2 = 4$. The order, Ω, of the group must be the least common multiple of the denominators, $5p^m$, 20, 8, $4d_3$, and hence must be $40d_3\, p^m$. This leads to

$$10p^m + 8d_3 = 1 + d_3\, p^m,$$

which may readily be shown to be impossible.

We now suppose that $f_1 = 1, 2$. If now any other d_i, say d_2, is even, we must have $f_2 = 1, 2$. This leads to $r = 2$, so that no f_i can be 4. Hence d_1 must be divisible by 4 and we then find $r = 3, f_1 = 2, f_2 = f_3 = 4$.

We observe that in this case the order of the group must be given by each of the two expressions, $\Omega = d_1\, p^m(1 + kp^m) = 2d_1\, d_2\, d_3\, p^m$. We may also obtain another expression for Ω by multiplying the number of reflections by the order of the group leaving a particular reflection invariant. There are d_1 reflections commutative with a particular reflection and $d_1 - 2$ other reflections commutative with each of these. The given reflection must be contained by two metacyclic groups of order $d_1\, p^m$, each of which contains $p^m - 1$ other reflections. It must also be contained by $d_1/2$ groups of order $4d_2$ and $d_1/2$ groups of order $4d_3$ which contain respectively $d_2 - 1$ and $d_3 - 1$ other reflections. Hence we must have

$$\Omega = 2d_1[1 + d_1(d_1 - 1) + 2(p^m - 1) + \tfrac{1}{2}d_1(d_2 - 1) + \tfrac{1}{2}d_1(d_3 - 1)].$$

Comparing this with one of the orders given above we find

$$2d_1(d_1 - 2) + (4p^m - 2) + d_1\, d_2 + d_1\, d_3 = p^m(1 + kp^m).$$

Also $2d_2\, d_3 = 1 + kp^m$. Since $d_1 < p^m$ and since we may suppose that $d_2 \not< 5$, $d_3 \not< 13$, it follows that

$$(4p^m - 2) + d_1\, d_2 + d_1\, d_3 < \tfrac{2\,2}{1\,3\,0}\, p^m(1 + kp^m).$$

Hence

$$2d_1(d_1 - 2) > \tfrac{1\,0\,8}{1\,3\,0}\, p^m(1 + kp^m).$$

This leads to $k = 1, 2$; $d_1 = p^m - 1$. We then find from the equation given above that $d_2 + d_3 - 4$ must be divisible by p^m. Hence we may suppose that $d_3 > p^m/2$. But this is impossible since $2d_2\, d_3 \not> 1 + 2p^m$. Hence no solution exists if any f_i has the value 4.

We proceed to construct the groups of order $1/2p^m(p^{2m} - 1)$ and $p^m(p^{2m} - 1)$. We may suppose that the former contains the transformations S and T written above, where $a + f = 0$, $b - e + df = 0$, $b + e = 0$, $\alpha = \beta^3$. We then obtain, by transforming S by the powers of T, the transformations

$$[x_1 + a\gamma x_2 + b\gamma^2 x_3 + c\gamma^3 x_4,\ x_2 + d\gamma x_3 + e\gamma^2 x_4,\ x_3 + f\gamma x_4,\ x_4],$$

where γ denotes any power of β^2. There are $1/2(p^m - 1)$ such transformations and they must generate the group of order p^m. There must be among these transformations some whose product is also in the set unless $p = 5$, $m = 1$. This leads to the condition, $3c = -ab$. [This may also be proved in the special case by a consideration of the other additive group left invariant by T.]

If for the present we consider conjugacy only under $A_\nu(p^n)$, we may choose a and d to be arbitrary marks in the $GF(p^n)$ different from 0. We suppose therefore that $a = d = 1$. The additive group then contains the transformations:

$$\left[x_1 + tx_2 + \frac{t^2}{2}x_3 - \frac{t^3}{6}x_4,\ x_2 + tx_3 - \frac{t^2}{2}x_4,\ x_3 - tx_4,\ x_4\right],$$

where t takes all values in the $GF(p^m)$.

The cyclic group generated by T must also leave another additive group invariant. Since the fixed points of the $p^m + 1$ additive groups must be $(1\,0\,0\,0)$, $(0\,0\,0\,1)$, and the $p^m - 1$ points $(-t^3/6, -t^2/2, -t, 1)$, we find this additive group to be

$$[x_1,\ 3tx_1 + x_2,\ 6t^2x_1 + 4tx_2 + x_3,\ -6t^3x_1 - 6t^2x_2 - 3tx_3 + x_4].$$

The largest group of this type which belongs to $A_1(p^n)$ is that of order $1/2p^n(p^{2n} - 1)$ obtained for $m = n$. They form a single conjugate set under $A_1(p^n)$ and may be said to correspond to the ordinary three-parameter continuous groups which have invariant twisted cubics.

7. Summary

We are now in a position to summarize our results. In the statement which follows we have, in a few places, denoted the order of $A_1(p^n)$ by $\Omega(p^n)$.

Theorem 10. *The maximal subgroups of $A_1(p^n)$ are as follows:*

(1) *groups of index $\Omega(p^n)/\Omega(p^k)$, each of which is conjugate under $A_1(p^n)$ with $A_1(p^k)$, where n/k is an odd prime;*

(2) *groups of index $\Omega(p^n)/2\Omega(p^k)$, each of which is conjugate under $A_\nu(p^n)$ with $A_\nu(p^k)$, where n is even and $n/k = 2$;*

(3) *a single conjugate set of groups of index $p^{3n} + p^{2n} + p^n + 1$, each of which has an invariant point and plane;*

(4) *a single conjugate set of groups of index $p^{3n} + p^{2n} + p^n + 1$, each of which has an invariant parabolic congruence;*

(5) *a single conjugate set of groups of index $p^{2n}(p^{2n} + 1)/2$, each of which has an invariant hyperbolic congruence;*

(6) *a single conjugate set of groups of index $p^{2n}(p^{2n} - 1)/2$, each of which has an invariant elliptic congruence;*

(7) *a single conjugate set of groups of index* $p^{3n}(p^{2n}+1)(p^n+1)/2$ $[p^n>3]$, *each of which has an invariant quadric such that all the lines of one regulus and two real lines of the other belong to the complex*;

(8) *a single conjugate set of groups of index* $p^{3n}(p^{2n}+1)(p^n-1)/2$ $[p^n>3]$, *each of which has an invariant quadric such that all the lines of one regulus and two imaginary lines of the other belong to the complex*;

(9) *a single conjugate set of groups of index* $p^{3n}(p^{4n}-1)$ $[p>3,\ p^n>7]$, *each of which has an invariant twisted cubic*;

(10) *two conjugate sets of groups of index* $\Omega(p^n)/16\cdot 120$ *if* $n=1, p=8h\pm 1$, *and a single conjugate set of groups of index* $\Omega(p^n)/16\cdot 60$ *if* $n=1$, $p=3$ *or* $8h\pm 3$.

(11) *two conjugate sets of groups of index* $\Omega(p^n)/720$ *if* $n=1, p=12f\pm 1$, *a single conjugate set of groups of index* $\Omega(p^n)/360$ *if* $n=1, p=5$ *or* $12f\pm 5$, $p\neq 7$, *and a single conjugate set of groups of index* $\Omega(p^n)/2520$ *if* $n=1$, $p=7$.

The G_{5040} is not a maximal subgroup of $A_1(7^n)$ for any n, but is a maximal subgroup of $A_\nu(7)$. Similarly for $p=12f\pm 5$, $p\neq 7$, the G_{720} is a maximal subgroup of $A_\nu(p)$, and if $p=3$ or $8h\pm 3$ the $G_{16\cdot 120}$ is a maximal subgroup of $A_\nu(p)$. For $p^n=5, 7$ the groups of index $p^{3n}(p^{4n}-1)$ are subgroups respectively of the G_{360} and the G_{2520}.

We observe that for $p^n=3$ the maximal subgroups are of index 40, 40, 45, 36, 27, which agrees with Dickson's result (loc. cit.). Also we find that the smallest index of any subgroup is $p^{3n}+p^{2n}+p^n+1$ except for $p^n=3$, in which case it is 27. Hence we have

THEOREM 11. *The smallest number of letters on which* $A_1(p^n)$ $[p$ *odd*$]$ *may be represented as a permutation group is* $p^{3n}+p^{2n}+p^n+1$ *except for* $p^n=3$, *in which case it is* 27.

This result is due to Jordan for $n=1$, $p=3$ and to Dickson* for $n=1$, $p>3$.

UNIVERSITY OF PENNSYLVANIA.

* Loc. cit.