COMPOSITIO MATHEMATICA

W. PEREMANS

Finite binary projective groups

Compositio Mathematica, tome 9 (1951), p. 97-129

<http://www.numdam.org/item?id=CM_1951__9__97_0>

Finite binary projective groups

by

W. Peremans

Amsterdam

§ 1. Introduction.

The problem of the finite binary projective groups arose from that of the finite groups of rotations on a fixed point in ordinary space. The group of the real rotations on a fixed point is isomorphic to the unitary binary projective group over the field of complex numbers. It has been shown by F. Klein [2] that the only possible finite subgroups of this group are the following: 1. cyclic groups, 2. dihedral groups, 3. the tetrahedral group, 4. the octahedral group, 5. the icosahedral group. The restriction to the unitary group may be dropped: there are no other finite subgroups of the binary projective group than those mentioned and their transforms $A\mathfrak{G}A^{-1}$.

We consider the generalisation to binary projective groups over an arbitrary commutative field. Asking first, which finite subgroups are possible, we meet with the following circumstance, which does not occur in the case of the complex field. A binary transformation has two fixed points (poles), which may coincide or not. We call a transformation with coinciding poles a parabolic transformation. Such a parabolic transformation has finite order if and only if the characteristic of the basic field is different from zero. Therefore also parabolic transformations must be taken into account. It is convenient to treat separately the finite groups in which parabolic transformations occur or do not occur. It appears that the possible groups without parabolic transformations are exactly the same as in the classical case, while in groups with parabolic transformations other types of groups may occur. This is proved by a discussion of the structure of all possible finite subgroups of the projective group.

In the case of rotation groups two finite groups, which are isomorphic, may be transformed into one another by a rotation of the space. Similarly, two isomorphic binary projective finite groups may be transformed into one another by a projective

transformation in the complex domain. The question arises whether this fact also holds in the general case. The method by which this is investigated consists in transforming a set of generators of a group of a certain type by a projective transformation into some canonical form; the coefficients of the transformation are allowed to belong to an algebraic extension of the basic field. In this paper we assume all extensions of the basic field we need to be performed. They are always finite. In the case of non-parabolic groups the attempt succeeds (just as in the classical case), but in the presence of parabolic transformations there may exist isomorphic groups, which are not conjugate in the projective group, even after algebraic closure of the field.

Finally the existence of the groups is discussed. For this the above-mentioned canonical forms are used and it turns out that the existence of the groups requires only some obvious restrictions concerning the characteristic of the basic field.

The problem of the existence of the groups without field extension, will be treated in another paper. There also the question which isomorphic groups are conjugate in the projective group over the basic field without extension, will be discussed.

§ 2. General remarks concerning the binary projective group over an arbitrary basic field.

The binary projective group is the group of all fractional linear transformations of one variable z:

$$z' = \frac{az + b}{cz + d}. \tag{2.1}$$

Any such transformation is determined by a matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}. \tag{2.2}$$

We call two matrices *congruent* ($A \equiv B$) or *projectively equivalent* if one arises from the other by multiplication with a factor $\lambda \neq 0$ of the basic field: $A = \lambda B$. In this case A and B define the same fractional linear transformation.

If we form the projective line by adding one element ∞ to the elements of the field, (2.1) defines a one-to-one transformation of the projective line into itself. By such a transformation three given distinct points may always be transformed into three arbitrarily given distinct points.

A pole of the transformation with matrix (2.2) (in the following

also called pole of the matrix) is found as a solution of the equation:

$$cz^2 + (d - a)z - b = 0.$$

So the poles belong either to the underlying field or to a quadratic extension. In this paper we tacitly assume this extension to be performed for all elements (in finite number) of the group, which amounts to a finite extension of the basic field. The poles may be different or coincident. In the latter case we call the transformation *parabolic*. If we bring the pole of a parabolic transformation P to ∞, we have $c = 0$ and $d = a$, so the matrix of P reduces to

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}.$$

Now is

$$P^n = \begin{pmatrix} 1 & nb \\ 0 & 1 \end{pmatrix},$$

so the order of P is infinite, if the characteristic is zero, and p, if the characteristic is p. This gives us:

THEOREM 2.1. In finite groups of binary projective transformations parabolic transformations may occur only if the characteristic of the basic field is $\neq 0$ and if they occur, their order is equal to the characteristic.

Now we consider the poles of the elements of a finite group.

THEOREM 2.2. The non-parabolic transformations, which have two fixed poles in common, form a cyclic group. Conversely the elements of a cyclic group with merely non-parabolic elements have their poles in common.

PROOF: Clearly the transformations having two given poles constitute a group. We bring the poles to 0 and ∞; the transformations then get the form

$$\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}.$$

If the order of the group is denoted by n, a must be a n^{th} root of the unity. For the n different transformations exactly n such n^{th} roots are available, and they form a cyclic group.

The converse is trivial, because the powers of a transformation have the same poles as the transformation itself.

THEOREM 2.3. When two non-parabolic transformations have one pole in common and not the other, the group must contain a parabolic transformation having the common pole of the given transformations as its pole.

Remark. From this theorem it follows that, if a certain pole is not a pole of any parabolic transformation, all transformations, which have this pole, have the other pole in common as well. Still more specially it follows that in a group without parabolic elements all poles occur in pairs, and a transformation having one pole of a pair, has the other as a pole too.

PROOF: We bring the common pole to ∞. According to the preceding theorem there are two cyclic groups of orders d_1 and d_2 with ∞ as a pole, but with different finite poles; let their primitive elements have the forms respectively

$$\begin{pmatrix} \eta_1 & b_1 \\ 0 & 1 \end{pmatrix} \text{ with } \eta_1^{d_1} = 1$$

and

$$\begin{pmatrix} \eta_2 & b_2 \\ 0 & 1 \end{pmatrix} \text{ with } \eta_2^{d_2} = 1.$$

We put $(d_1, d_2) = d$. We distinguish two cases:

1. $d \neq 1$. Let η be a primitive d^{th} root of the unity; the first group then contains a transformation

$$\begin{pmatrix} \eta & c_1 \\ 0 & 1 \end{pmatrix}$$

and the second

$$\begin{pmatrix} \eta^{d-1} & c_2 \\ 0 & 1 \end{pmatrix}.$$

Their product is:

$$\begin{pmatrix} \eta & c_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \eta^{d-1} & c_2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \eta c_2 + c_1 \\ 0 & 1 \end{pmatrix}.$$

Now $\eta c_2 + c_1 \neq 0$, because the two transformations belong to different cyclic groups. Their product therefore is a parabolic transformation with ∞ as its pole.

2. $(d_1, d_2) = 1$. We reduce this case to the preceding one. There are two such integers k_1 and k_2, that $k_1 d_1 + k_2 d_2 = 1$. Let η_3 be a primitive $d_1 d_2^{\text{th}}$ root of the unity, then $\eta_3^{k_2 d_2}$ is a d_1^{th} and $\eta_3^{k_1 d_1}$ a d_2^{th} root of the unity. The first group contains a transformation of the form

$$\begin{pmatrix} \eta_3^{k_2 d_2} & b_3 \\ 0 & 1 \end{pmatrix}$$

and the second

$$\begin{pmatrix} \eta_3^{k_1 d_1} & b_4 \\ 0 & 1 \end{pmatrix}.$$

Their product is

$$\begin{pmatrix} \eta_3^{k_2 d_2} & b_3 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \eta_3^{k_1 d_1} & b_4 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \eta_3 & \eta_3^{k_2 d_2} b_4 + b_3 \\ 0 & 1 \end{pmatrix}$$

and belongs to a cyclic group with an order, which is a multiple of $d_1 d_2$. By combining this group with one of the two given groups we return to case 1. With this the proof is completed.

In the following we treat the groups *with* and *without* parabolic elements separately, as the most efficient treatment is different for each of the two cases.

§ 3. The possible finite subgroups without parabolic elements.

We consider a finite subgroup $\mathfrak{G}$ of the binary projective group without parabolic elements. All elements of $\mathfrak{G}$, which have a pole of one element of $\mathfrak{G}$ as a pole, form a subgroup $\mathfrak{H}$. (We agree, that the identical transformation E has every pole of the group as its pole.) A left coset $A\mathfrak{H}$ transforms the pole into another point, which is a pole of the group $A\mathfrak{H}A^{-1}$ conjugate to $\mathfrak{H}$. We therefore call the poles conjugate and attach to each pole an order equal to the order of the subgroup belonging to this pole. The number of the poles conjugate to one pole is equal to the index of the subgroup belonging to that pole. If we add together the orders n_i minus 1 (omission of the identity) of all poles, all transformations except the identity are counted twice, namely at both their poles. If we call the order of the group N (by assuming $N \geqq 2$ we eliminate in advance the trivial case of the group consisting of the identity) we get the following fundamental Diophantine equation:

$$\sum_{i=1}^{r} (n_i - 1) \frac{N}{n_i} = 2(N-1). \tag{3.1}$$

The solutions of (3.1) in positive integers give us the possible finite groups without parabolic elements. We write (3.1) in two other forms, namely

$$\sum_{i=1}^{r} \frac{1}{n_i} = \frac{2}{N} + (r-2), \tag{3.2}$$

$$\sum_{i=1}^{r} (n_i - 1) \frac{1}{2n_i} = \frac{N-1}{N}. \tag{3.3}$$

The terms on the left-hand side of (3.3) are all $\geqq \frac{1}{4}$ and $< \frac{1}{2}$,

so $r = 2$ or $r = 3$. For $r = 2$ it follows from (3.2) and $n_1 \leqq N$ and $n_2 \leqq N$, that $n_1 = n_2 = N$. We call this case A.

For $r = 3$ the right-hand side of (3.2) is > 1, so one of the n_i, say n_1, must be 2. We get

$$\frac{1}{n_2} + \frac{1}{n_3} = \frac{2}{N} + \frac{1}{2}. \tag{3.4}$$

The right-hand side of (3.4) is $> \frac{1}{2}$, so the smallest of n_2 and n_3, say n_2, must be 2 or 3. For $n_2 = 2$ we get $n_3 = \frac{N}{2}$. Case **B**.

For $n_2 = 3$ we get for n_3 the possibilities 3, 4 or 5.

$n_3 = 3$ gives $N = 12$. Case **C**.

$n_3 = 4$ gives $N = 24$. Case **D**.

$n_3 = 5$ gives $N = 60$. Case **E**.

These 5 types evidently correspond to the 5 types of rotation groups. We therefore give them the same names and we shall prove later on that the groups of one type and the same order are isomorphic.

§ 4. List of the numbers of conjugate poles and group elements.

The numbers of conjugate poles may be derived immediately from the results of the preceding section.

A. N arbitrary, $n_1 = N$, $n_2 = N$.

1 pole of order N
1 pole of order N
} cyclic groups.

B. $N = 2n$, $n_1 = 2$, $n_2 = 2$, $n_3 = n$.

n conjugate poles of order 2
n conjugate poles of order 2
2 conjugate poles of order n
} dihedral groups.

C. $N = 12$, $n_1 = 2$, $n_2 = 3$, $n_3 = 3$.

6 conjugate poles of order 2
4 conjugate poles of order 3
4 conjugate poles of order 3
} tetrahedral group.

D. $N = 24$, $n_1 = 2$, $n_2 = 3$, $n_3 = 4$.

12 conjugate poles of order 2
8 conjugate poles of order 3
6 conjugate poles of order 4
} octahedral group.

E. $N = 60,\ n_1 = 2,\ n_2 = 3,\ n_3 = 5.$

30 conjugate poles of order 2
20 conjugate poles of order 3 } icosahedral group.
12 conjugate poles of order 5

Now we derive a list of conjugate group elements for the tetrahedal, the octahedral and the icosahedral groups, as we need it later on for the structure proof. To obtain it, we first prove a theorem, preceded by a

LEMMA. If the element S interchanges the poles of an element A, then $SAS^{-1} = A^{-1}$, and $S^2 = E$.

Proof: Bring the poles of A to 0 and ∞, then

$$\begin{pmatrix} 0 & s_{12} \\ s_{21} & 0 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & -s_{12} \\ -s_{21} & 0 \end{pmatrix} = \begin{pmatrix} -s_{12}s_{21} & 0 \\ 0 & -s_{12}s_{21}a \end{pmatrix} \equiv \begin{pmatrix} a^{-1} & 0 \\ 0 & 1 \end{pmatrix} = A^{-1}.$$

$$\begin{pmatrix} 0 & s_{12} \\ s_{21} & 0 \end{pmatrix}^2 = \begin{pmatrix} s_{12}s_{21} & 0 \\ 0 & s_{12}s_{21} \end{pmatrix} \equiv E.$$

THEOREM 4.1. The number of elements conjugate to an element A is equal to the number of the poles conjugate to a pole of A, except if A has order 2 and its poles are mutually conjugate; in the latter case the number of elements conjugate to A is equal to half the number of the poles conjugate to a pole of A.

PROOF: Let the element S transform a pole P of A into P'. Then SAS^{-1} has P' as a pole. The elements which transform P into P', form a left coset of the group $\mathfrak{H}$, belonging to the pole P. As $\mathfrak{H}$ is cyclic and contains A, $\mathfrak{H}$ is contained in the normalizer of A, so two elements of the same left coset of $\mathfrak{H}$ give the same transformed element of A. So we get exactly one transformed element of A having P' as a pole. Thus we find to each pole P_i conjugate with P exactly one transformed element SAS^{-1} with P_i as a pole. But it may happen, that two different poles P_i and P_k give the same transformed element:

$$S_iAS_i^{-1} = S_kAS_k^{-1}.$$

In this case $S = S_i^{-1}S_k$ gives $SAS^{-1} = A$. But S does not leave invariant the pole P, because $P_i \neq P_k$, so S must interchange the poles of A. Now from the lemma and $SAS^{-1} = A$ it follows that $A^{-1} = A$, or $A^2 = E$. In this exceptional case to each S_i belongs such a $S_k = S_iS$, that S_i and S_k give the same transformed element $S_iAS_i^{-1}$. The number of transformed elements is then half the number of conjugate poles P_i.

In the cases C, D and E the poles of an even order (to which

belongs an element of order 2) are always conjugate, and so for the elements of order 2 the exceptional case occurs always.

With use of theorem 4.1 and the numbers given at the beginning of this section the following list of conjugate group elements is obtained by simple counting.

order	1	2	3	4	5	total
tetrahedral group	1	3	4 4			12
octahedral group	1	6 3	8	6		24
icosahedral group	1	15	20		12 12	60

§ 5. The structure of the groups without parabolic elements.

A. There are only two poles, which all group elements must therefore have in common. We have already seen in § 2, that such a group is cyclic.

B. As there are only two poles of order n, the elements belonging to them form a cyclic group $\mathfrak{C}_n$ of order n and of index 2. All other n elements have order 2. It is known that such a group must be the dihedral group $\mathfrak{D}_n$. The argument does not hold for $n = 2$, as we do not know a priori how to combine the poles. However it is clear that a group of order 4 whose elements $\neq E$ all have order 2 can only be isomorphic to Klein's four-group, i.e. to the dihedral group $\mathfrak{D}_2$.

C. In this case we consider a set of four conjugate poles of order 3. These are permuted by the elements of the group. The mapping of the group upon these permutations is evidently a homomorphism. But a projectivity leaving 4 points invariant is the identity, so the homomorphism is an isomorphism. So the group is isomorphic to a permutation group of degree 4 and order 12. This must be the alternating group $\mathfrak{A}_4$, which is isomorphic to the tetrahedral group in the usual sense.

D. Here we take four conjugate subgroups of order 3. Each

group element transforms one of the subgroups into a conjugate one and so induces a permutation of the four subgroups. The mapping between the group and the permutation group is a homomorphism. The permutation group is transitive and so has an order which is a multiple of 4; so the normal subgroup belonging to the homomorphism must have an order which is a divisor of $24 : 4 = 6$. From the scheme at the end of § 4 it follows, that normal subgroups of order 2, 3 or 6 do not exist. So the homomorphism is an isomorphism, and the group is isomorphic to the symmetrical group $\mathfrak{S}_4$, which is isomorphic to the octahedral group in the usual sense.

E. First of all we take an element A of order 2. As the poles of A are conjugate, there exists an element, which interchanges the poles of A and which, according to the lemma of § 4, is of order 2. So $BAB = A$, $AB = BA$. The elements, A, B, AB and E constitute a four-group $\mathfrak{F}$. The number of elements conjugate to A is 15, which is just the index of the normalizer of A. Hence the latter has the order $60 : 15 = 4$, so it is the four-group $\mathfrak{F}$. This means that no other element than B is interchangeable with A. Thus all elements of order 2 are brought into 5 four-groups, which are disjoint. Each element of the group induces a permutation of these four-groups and the mapping of the group upon the permutationgroup is a homomorphism. However from the scheme at the end of § 4 it follows easily, that the group is simple, because from the numbers given there no proper divisor of 60 can be composed. Moreover not all elements are mapped upon the identical permutation (the permutationgroup is even transitive), and so the homomorphism must be an isomorphism upon the alternating group $\mathfrak{A}_5$, since this is the only permutationgroup of degree 5 and order 60. $\mathfrak{A}_5$ is isomorphic to the icosahedral group in the usual sense.

Thus the structure of the single types has been found. The reader will have noticed, that the permutationgroups are essentially the same as those which appear in the well-known geometrical treatment of the rotation groups.

§ 6. Equivalence of the groups of a type for the groups without parabolic elements.

THEOREM 6.1. Two groups without parabolic elements of the same type and of the same order may be transformed into one another by linear transformation.

PROOF: We prove this by transforming by linear transformation an arbitrary group of a type into an unambiguously determined form.

A. We bring the poles of a cyclic group to 0 and ∞. This gives

$$\begin{pmatrix}\zeta & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}\zeta^2 & 0\\ 0 & 1\end{pmatrix}, \cdots \begin{pmatrix}\zeta^{N-1} & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \tag{6.1}$$

in which ζ is an arbitrary primitive N^{th} root of the unity. Another root gives the same matrices, as ζ^k runs through all N^{th} roots of the unity and so do the powers of another primitive root of the unity.

B. We bring the poles of order n of a dihedral group to 0 and ∞. The transformations of the cyclic subgroup of order n having these poles are

$$\begin{pmatrix}\zeta & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}\zeta^2 & 0\\ 0 & 1\end{pmatrix}, \cdots \begin{pmatrix}\zeta^{n-1} & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},$$

ζ being a primitive n^{th} root of the unity. We now take an arbitrary transformation T not belonging to the cyclic subgroup. Since T has order 2, we may write

$$T = \begin{pmatrix}a & b\\ c & -a\end{pmatrix}.$$

T generates a coset of the cyclic group consisting exclusively of the elements

$$\begin{pmatrix}a & b\\ c & -a\end{pmatrix}\begin{pmatrix}\zeta^k & 0\\ 0 & 1\end{pmatrix} = \begin{pmatrix}a\zeta^k & b\\ c\zeta^k & -a\end{pmatrix}.$$

Since these elements are all of order 2, we must have $a\zeta^k = a$. As $\zeta^k \neq 1$ is possible, $a = 0$. Now we may choose $b = 1$. Finally we bring one of the poles of T to 1, then we have $c = 1$:

$$T = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}.$$

The group now consists of the following elements:

$$\left.\begin{array}{l}\begin{pmatrix}\zeta & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}\zeta^2 & 0\\ 0 & 1\end{pmatrix}, \cdots \begin{pmatrix}\zeta^{n-1} & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\\ \begin{pmatrix}0 & 1\\ \zeta & 0\end{pmatrix}, \begin{pmatrix}0 & 1\\ \zeta^2 & 0\end{pmatrix}, \cdots \begin{pmatrix}0 & 1\\ \zeta^{n-1} & 0\end{pmatrix}, \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\end{array}\right\}. \tag{6.2}$$

Evidently this form is unambiguously determined.

C D E. For the tetrahedral, the octahedral and the icosahedral groups we use an analogous method, which consists in choosing two generators and transforming them into an unambiguously determined form by bringing poles to **0**, **1** and ∞. By this the proof is finished, as the form of the generators determines that of all group elements.

We start with some remarks concerning generators of $\mathfrak{A}_4$, $\mathfrak{S}_4$ and $\mathfrak{A}_5$, which we shall need repeatedly.

THEOREM 6.2. The groups $\mathfrak{A}_4$, $\mathfrak{S}_4$ and $\mathfrak{A}_5$ are isomorphic to groups defined by two generators A and B and the relations:

for $\mathfrak{A}_4$: $A^3 = B^2 = (AB)^3 = E$,
for $\mathfrak{S}_4$: $A^3 = B^2 = (AB)^4 = E$,
for $\mathfrak{A}_5$: $A^5 = B^2 = (AB)^3 = E$.

PROOF: For $\mathfrak{A}_4$ and $\mathfrak{A}_5$ the generators are well-known. (cf. Dickson [1], § 265 and § 267.) For $\mathfrak{S}_4$ Dickson ([1], § 264) gives three generators B_1, B_2, B_3 satisfying the relations

$$B_1^2 = B_2^2 = B_3^2 = (B_1B_3)^2 = (B_1B_2)^3 = (B_2B_3)^3 = E.$$

Now if we introduce $A = B_1B_2$ and $B = B_3$, we can express B_1, B_2, B_3 as follows:

$$\left.\begin{aligned} B_1 &= ABA^2BAB \\ B_2 &= BA^2BAB \\ B_3 &= B \end{aligned}\right\},$$

and we get the relations mentioned before.

We now prove that in this theorem the orders of the generators and their product may be permuted arbitrarily, in the following sense:

THEOREM 6.3. In $\mathfrak{A}_4$ there are two generators A and B, so that A, B, AB have order 2 ,3 ,3 in an arbitrarily given order. In $\mathfrak{S}_4$ there are two generators A and B, so that A, B, AB have order 2, 3, 4 in an arbitrarily given order. In $\mathfrak{A}_5$ there are two generators A and B, so that A, B, AB have order 2, 3, 5 in an arbitrarily given order.

PROOF: That we may interchange the orders of the generators themselves, follows from the well-known group theorem: If $A^k = B^h = (AB)^m = E$, then $(BA)^m = E$.

The following cases remain:

for $\mathfrak{A}_4$: (3, 3, 2) $\left.\begin{aligned} P &= A^2 \\ Q &= AB \\ PQ &= B \end{aligned}\right\}$ $\left.\begin{aligned} A &= P^2 \\ B &= PQ \\ AB &= Q \end{aligned}\right\}$

$$\text{for } \mathfrak{S}_4\text{: } (3,4,2)\quad \left.\begin{matrix} P = A^2 \\ Q = AB \\ PQ = B \end{matrix}\right| \left.\begin{matrix} A = P^2 \\ B = PQ \\ AB = Q \end{matrix}\right|$$

$$(4,2,3)\quad \left.\begin{matrix} P = AB \\ Q = B \\ PQ = A \end{matrix}\right| \left.\begin{matrix} A = PQ \\ B = Q \\ AB = P \end{matrix}\right|$$

$$\text{for } \mathfrak{A}_5\text{: } (3,2,5)\quad \left.\begin{matrix} P = AB \\ Q = B \\ PQ = A \end{matrix}\right| \left.\begin{matrix} A = PQ \\ B = Q \\ AB = P \end{matrix}\right|$$

$$(5,3,2)\quad \left.\begin{matrix} P = A^4 \\ Q = AB \\ PQ = B \end{matrix}\right| \left.\begin{matrix} A = P^4 \\ B = PQ \\ AB = Q \end{matrix}\right|$$

Clearly P and Q satisfy the required relations. This completes the proof.

We use for each of the three groups two generators A and B, of which A has order 3 for the tetrahedral, 4 for the octahedral and 5 for the icosahedral group, B order 2 in the three cases and AB order 3 in the three cases. Here A may be chosen arbitrarily out of the elements of the given order, because the alternating group is a normal subgroup of the symmetric group and because in $\mathfrak{S}_4$, $\mathfrak{S}_4$ and $\mathfrak{S}_5$ the elements of order 3, 4 and 5 respectively are conjugate. The poles of A may be brought to 0 and ∞, a pole of B to 1. Then A becomes:

$$A = \begin{pmatrix} \varepsilon & 0 \\ 0 & 1 \end{pmatrix},$$

in which ε is respectively a third, fourth or fifth root of unity. B has order 2 and has 1 as a pole:

$$B = \begin{pmatrix} a & b \\ 2a + b & -a \end{pmatrix}.$$

As the point 0 is certainly not a pole of B we have $b \neq 0$, hence b may be chosen $= 1$. So we get

$$B = \begin{pmatrix} a & 1 \\ 2a + 1 & -a \end{pmatrix}.$$

LEMMA. A non-singular matrix

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix}$$

has order 3 if and only if

$$p^2 + ps + s^2 + qr = 0.$$

PROOF: By computing the third power of the matrix, equating the elements of the main diagonal and putting zero the other elements, we immediately find the condition.

Now

$$\begin{pmatrix} \varepsilon & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 1 \\ 2a+1 & -a \end{pmatrix} = \begin{pmatrix} \varepsilon a & \varepsilon \\ 2a+1 & -a \end{pmatrix}.$$

The condition of order 3 for this product takes the form:

$$(\varepsilon^2 - \varepsilon + 1)a^2 + \varepsilon(2a+1) = 0.$$

We transform the roots of this equation (called a_1 and a_2) into one another by means of a transformation, which interchanges 0 and ∞ but leaves invariant 1, i.e. with

$$S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

This gives in the general case

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} s & r \\ q & p \end{pmatrix}.$$

If $\varepsilon^2 - \varepsilon + 1 = 0$ were true, only one solution would exist, and we should have nothing to prove. (This case does not occur, which however does not interest us now.) Otherwise we put

$$\frac{\varepsilon}{\varepsilon^2 - \varepsilon + 1} = k,$$

and the equation becomes $a^2 + 2ka + k = 0$. So we have, since $k \neq 0$: $a_1 a_2 = k$, $2a_1 + 1 = -\frac{a_1^2}{k}$ and $2a_2 + 1 = -\frac{a_2^2}{k}$. Now

$$\begin{pmatrix} a_1 & 1 \\ 2a_1+1 & -a_1 \end{pmatrix} = \begin{pmatrix} a_1 & 1 \\ -\frac{a_1^2}{k} & -a_1 \end{pmatrix}$$

becomes by transformation with S:

$$\begin{pmatrix} -a_1 & -\frac{a_1^2}{k} \\ 1 & a_1 \end{pmatrix} \equiv \begin{pmatrix} \frac{k}{a_1} & 1 \\ -\frac{k}{a_1^2} & -\frac{k}{a_1} \end{pmatrix} = \begin{pmatrix} a_2 & 1 \\ -\frac{a_2^2}{k} & -a_2 \end{pmatrix} = \begin{pmatrix} a_2 & 1 \\ 2a_2+1 & -a \end{pmatrix}.$$

By the transformation ε in A has changed into ε^{-1}. Therefore we replace A by A^{-1}, A^{-1} and B being admissible generators too.

Now the unambiguous determination of the form of the generators has been obtained, viz.

$$A = \begin{pmatrix} \varepsilon & 0 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} a_1 & 1 \\ 2a_1+1 & -a_1 \end{pmatrix},$$

as the multivalence of ε has no influence, because the powers of

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

give the other values of the roots of the unity and ε by the choice of A indeed may be made equal to a certain given primitive root of the unity.

§ 7. Existence of the groups without parabolic elements.

By means of the result of the preceding section we are able to decide whether the groups without parabolic elements exist after properly chosen extension of the basic field.

The cyclic group of order N, being isomorphic to the multiplicative group of the N^{th} roots of unity (cf. § 2), can only exist if the characteristic of the field is not a divisor of N, as otherwise no N different N^{th} roots of the unity are possible.

For the various types of groups this condition imposes restrictions on the characteristic, because of the cyclic subgroups occuring in those groups. These restrictions appear to be the only ones. This fact is expressed in the following theorem:

THEOREM 7.1. The necessary and sufficient condition for the existence of a group of given type in a properly chosen extension of the basic field is, that the characteristic of the field suffices the following conditions:

for the cyclic group of order N: no divisor of N,
for the dihedral group of order $2n$: $\neq 2$ and no divisor of n,
for the tetrahedral group: $\neq 2$ and $\neq 3$,
for the octahedral group: $\neq 2$ and $\neq 3$,
for the icosahedral group: $\neq 2$, $\neq 3$ and $\neq 5$.

PROOF: We have already proved the necessity of these conditions. Now suppose that they are fulfilled.

The existence of the cyclic and dihedral groups then is established because of the schemes (6.1) and (6.2) in which the occuring matrices are regular and different.

In the final forms of the generators of the tetrahedral, octahedral and icosahedral groups in § 6 only roots of the unity and the element a_1 occured, a_1 being quadratic over the prime field extended with a root of the unity.

Let R be the prime field. The generating matrices A and B, determined in § 6, contained only elements of the field $R(\varepsilon, a_1)$. We adjoin to an arbitrary basic field ε and a_1 if necessary; it then

contains $R(\varepsilon, a_1)$ as a subfield, and therefore also the matrix-elements of A and B. According to a wellknown theorem of group theory, if a group has a set of generating elements, which suffice certain relations, the group is a homomorphic image of the abstract group $\mathfrak{G}$ generated by corresponding generators with the same relations. In our case A, B and AB have the prescribed orders and no lower ones. To show this, we need only prove, that they cannot be singular. For A this is clear; the determinant of B is $-a_1^2 - 2a_1 - 1 = -(a_1 + 1)^2$. This would be zero, if $a_1 = 0$, but then the condition which a_1 fulfills becomes: $\varepsilon^2 - 2\varepsilon + 1 = (\varepsilon - 1)^2 = 0$, $\varepsilon = 1$, which is not the case. So A and B generate a group $\mathfrak{G}'$, which is a homomorphic image of $\mathfrak{G}$: $\mathfrak{G}' \simeq \mathfrak{G}/\mathfrak{N}$.

For the tetrahedral group the orders of A and B are 3 and 2, hence the order of $\mathfrak{G}'$ is a multiple of 6. If $\mathfrak{G}'$ were not isomorphic to $\mathfrak{G}$, $\mathfrak{N}$ would have order 2. Since $\mathfrak{A}_4$ has no normal subgroup of order 2, we have $\mathfrak{G}' \simeq \mathfrak{A}_4$.

For the octahedral group the orders of A and AB are 4 and 3, hence the order of $\mathfrak{G}'$ is a multiple of 12. If $\mathfrak{G}'$ were not isomorphic to $\mathfrak{G}$, $\mathfrak{N}$ would have order 2. Since $\mathfrak{S}_4$ has no normal subgroup of order 2, we have $\mathfrak{G}' \simeq \mathfrak{S}_4$.

For the icosahedral group the order of $\mathfrak{G}'$ is certainly > 1. Since $\mathfrak{A}_5$ is simple, it follows that $\mathfrak{G}' \simeq \mathfrak{A}_5$.

This completes the proof of existence.

§ 8. Finite additive groups in a field.

In this section we collect some well-known facts about finite additive groups in a field. (cf Dickson [1], § 68 and § 70.)

In a field of characteristic zero every element $\neq 0$ has order ∞ (additively!); hence only the trivial finite additive group, consisting of the zero only, exists. Now let the characteristic of the field be p, so that every element $\neq 0$ has order p. A finite additive group, being an abelian group, has a base $\lambda_1, \ldots, \lambda_m$, such that all elements of the group may be written as $c_1\lambda_1 + \ldots + c_m\lambda_m$ ($c_i = 0, 1, \ldots, p-1$); we call this the additive group $[\lambda_1, \lambda_2, \ldots, \lambda_m]$ of rank m with respect to $GF(p)$. The elements $\gamma_1\lambda_1 + \gamma_2\lambda_2 + \ldots + \gamma_m\lambda_m$ (γ_i arbitrary in a $GF(p^r)$ and $\lambda_k \neq \gamma_1\lambda_1 + \ldots + \gamma_{k-1}\lambda_{k-1}$) form an additive group of order p^{mr}; we call this the additive group $[\lambda_1, \ldots, \lambda_m]$ of rank m with respect to $GF(p^r)$.

If we multiply all elements of an additive group $[\lambda_1, \ldots, \lambda_m]$ with respect to $GF(p)$ by $\mu \neq 0$, we get an additive group

$[\mu\lambda_1, \ldots, \mu\lambda_m]$ of the same rank, because

$$\sum_{i=1}^{m} \gamma_i \mu\lambda_i = \mu \sum_{i=1}^{m} \gamma_i\lambda_i = 0 \text{ and } \mu \neq 0$$

implies

$$\sum_{i=1}^{m} \gamma_i\lambda_i = 0.$$

If this group is identical with the original group we call μ a multiplier of the group. The number of the multipliers is finite ($\leqq p^m - 1$), because a certain element $\neq 0$ of the group must be transformed into another definite element of the group, which in each case is only possible with one multiplier. There are at most as much multipliers as group elements $\neq 0$. If μ_1 and μ_2 are multipliers, so are $\mu_1 + \mu_2$ (if $\neq 0$) and $\mu_1\mu_2$; therefore the multipliers together with zero constitute a Galois field $GF(p^k)$, called the multiplicative Galois field of the additive group. Now it is easy to see, that the additive group is also an additive group with respect to its multiplicative Galois field and therefore $k \mid m$. Finally an arbitrary multiplicative group of order d of multipliers is a subgroup of the multiplicative group of the multiplicative Galois field $GF(p^k)$, so $d \mid p^k - 1$, further $p^k - 1 \mid p^m - 1$ (because $k \mid m$), and $d \mid p^m - 1$.

§ 9. The normalizers of the additive and cyclic binary projective groups.

The parabolic elements of a subgroup of the binary projective group having a given pole form a group, which is isomorphic to an additive group in the basic field. For if we bring the pole to ∞, the parabolic element becomes

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \tag{9.1}$$

and the product of two such elements is

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b + c \\ 0 & 1 \end{pmatrix}.$$

We therefore call a group of parabolic transformations having the same pole an additive group. Sometimes it is necessary to distinguish between the additive field group and the additive transformation group; but when no confusion is to be feared we simply speak of the additive group.

We now consider in a finite subgroup of the binary projective

group an arbitrary transformation, which has a pole at the common pole of an additive group. The transformation may have the form

$$\begin{pmatrix} \eta & c \\ 0 & 1 \end{pmatrix}.$$

Now let (9.1) be an arbitrary transformation of the additive group. Then

$$\begin{pmatrix} \eta & c \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \eta & c \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & \eta b \\ 0 & 1 \end{pmatrix}.$$

This must be a transformation of the additive group for every b of the additive group, i.e. η must be multiplier of the additive group, and the order d of the corresponding transformation suffices $d \mid p^m - 1$, if p^m denotes the order of the additive group.

We now consider the normalizer of an additive group. In general, if an element S transforms an element A into A' with the same poles (or pole) as A, then S transforms a pole P of A (or A') into a pole of A (or A'), because $SA = A'S$ implies $S(P) = A'S(P)$. If A is parabolic, an element S of the normalizer must have the pole of A as a pole. The converse is also true:

$$\begin{pmatrix} p & q \\ 0 & s \end{pmatrix}\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} s & -q \\ 0 & p \end{pmatrix} = \begin{pmatrix} ps & p^2 b \\ 0 & ps \end{pmatrix} \equiv \begin{pmatrix} 1 & \mu b \\ 0 & 1 \end{pmatrix};\ \mu = \frac{p}{s}.$$

If S is in the group, μ must be a multiplier. So we obtain

THEOREM 9.1. The normalizer of an additive transformation group consists of those and only those elements, which have the pole of the additive group as a pole. If d is the order of a non-parabolic element of the normalizer, the d^{th} roots of the unity are multipliers of the additive field group corresponding to the additive transformation group.

We consider the multipliers which occur in the normalizer somewhat more in detail. If

$$\begin{pmatrix} \eta_1 & c_1 \\ 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} \eta_2 & c_2 \\ 0 & 1 \end{pmatrix}$$

are elements of the normalizer, their product

$$\begin{pmatrix} \eta_1 & c_1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \eta_2 & c_2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \eta_1\eta_2 & \eta_1 c_2 + c_1 \\ 0 & 1 \end{pmatrix}$$

obviously is an element of the normalizer too. From this it follows that the multipliers occurring in the normalizer form a multiplicative group, which is certainly cyclic for being a subgroup

of the multiplicative group of a Galois field. So the multipliers occurring in the normalizer are powers of one of them: η.

THEOREM 9.2. An additive transformation group of order p^m and an element of its normalizer of order $d \mid p^m - 1$ generate a metacyclic group of order dp^m.

PROOF: We bring the pole of the additive group to ∞, the other pole of the given element of the normalizer to 0. Let (9.1) be a transformation of the additive group and

$$\begin{pmatrix} \vartheta & 0 \\ 0 & 1 \end{pmatrix}, \quad \vartheta^d = 1$$

the element of the normalizer. The dp^m elements:

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \vartheta^k & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \vartheta^k & b \\ 0 & 1 \end{pmatrix}, \quad (k = 0, 1, \ldots, d-1),$$

form a group, because the product of two of them:

$$\begin{pmatrix} \vartheta^k & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \vartheta^l & c \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \vartheta^{k+l} & \vartheta^k c + b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \vartheta^h & a \\ 0 & 1 \end{pmatrix}$$

(ϑ is a multiplier!) is also such an element. This group is metacyclic, because it is homomorphic to the cyclic group of the ϑ^k, the kernel of the homomorphism being the abelian group of the b.

On account of the preceding the proof of the theorem we aimed at is simple.

THEOREM 9.3. The normalizer of an additive group is either the group itself or a metacyclic group as in theorem 9.2.

PROOF: We bring the pole of the additive group to ∞. If there exists an element of the normalizer not belonging to the group, the multipliers form a cyclic group of order d, of which we choose a primitive element η and take a corresponding element T of the normalizer. If we bring the other pole of T to 0, the element η remains unchanged and T takes the form

$$T = \begin{pmatrix} \eta & 0 \\ 0 & 1 \end{pmatrix}.$$

Now we may form with T, as in theorem 9.2., a metacyclic group, and we assert that this group is already the whole normalizer. To prove this it suffices to show that in an arbitrary element of the normalizer, which obviously has the form

$$\begin{pmatrix} \eta^k & c \\ 0 & 1 \end{pmatrix},$$

c is an element of the additive field group corresponding to the

additive transformation group. We multiply the element by T^{d-k} and obtain

$$\begin{pmatrix} \eta^k & c \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \eta^{d-k} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}.$$

This is an element of the additive transformation group, which completes the proof.

Next we consider the normalizer of a finite cyclic group $\mathfrak{G}$ with two different poles. An element S of the normalizer of $\mathfrak{G}$ must leave the poles of $\mathfrak{G}$ invariant or interchange them. Conversely a transformation which leaves invariant the poles of $\mathfrak{G}$ belongs itself to $\mathfrak{G}$ and a fortiori to the normalizer of $\mathfrak{G}$; a transformation which interchanges the poles of $\mathfrak{G}$ transforms the elements of $\mathfrak{G}$ (lemma of § 4) into their inverses and therefore also belongs to the normalizer of $\mathfrak{G}$. Now it is easy to show:

THEOREM 9.4. The normalizer in a finite group of a non-parabolic cyclic group is a dihedral group or the cyclic group itself.

PROOF: A product of two transformation interchanging the poles, leaves invariant the poles and hence belongs to $\mathfrak{G}$. So $V_1V_2 = G$, $V_2 = V_1G$ (for $V_1^2 = E$, lemma in § 4), and the elements V_1G_i and G_i form the normalizer. Of course it may happen, that there are no transformations interchanging the poles; then the cyclic group is its own normalizer.

§ 10. The possible finite groups with parabolic elements.

Now we may pass on to the discussion of the possible finite groups with parabolic elements. The method of treating it will consist, once more, in solving a Diophantine equation, which holds in this case not for the orders of the poles but for those of the additive and cyclic subgroups.

The parabolic transformation with a certain pole constitute, according to the preceding section, an additive group of order p^m.

THEOREM 10.1. All additive groups are conjugate.

PROOF: We take an additive group of order p^m. Every point except the pole of this group is transformed by the p^m transformations of the group into p^m different points, and a pole into conjugate poles. So there are $1 + fp^m$ (f a non-negative integer) additive groups conjugate with this group. If there would be still another parabolic additive group of order p^n, not conjugate to this, the transformations of the latter group would transform the poles of the former groups into p^n poles, from which it would

follow, that there would be gp^n (g a positive integer) groups conjugate to the first mentioned additive group. But $1 + fp^m = gp^n$ is impossible; so all additive groups are conjugate.

For the rest of this section see also Mitchell [3]. The results of the preceding section on normalizers, and the fact, that the additive groups of order p^m and also the corresponding cyclic groups of order d_1 are conjugate, give us immediately the following Diophantine equation (in which N is the order of the whole group, and d_i the orders of the occuring cyclic subgroups):

$$(10.1) \qquad N = 1 + (p^m - 1)\frac{N}{d_1 p^m} + \sum_{i=1}^{r} (d_i - 1)\frac{N}{f_i d_i}, \quad (f_i = 1 \text{ or } 2),$$

or in other forms:

$$(10.2) \qquad N = 1 + \frac{(f_1 + d_1 - 1)p^m - f_1}{f_1 d_1 p^m} N + \sum_{i=2}^{r} (d_i - 1)\frac{N}{f_i d_i},$$

$$(10.3) \qquad \frac{1}{N} = \frac{(f_1 - 1)(d_1 - 1)p^m + f_1}{f_1 d_1 p^m} - \sum_{i=2}^{r} \frac{d_i - 1}{f_i d_i}.$$

We remark, that d_i as orders of cyclic groups with different poles are not divisible by p.

We first put $d_1 = 1$, then (10.3) becomes:

$$\frac{1}{N} = \frac{1}{p^m} - \sum_{i=2}^{r} \frac{d_i - 1}{f_i d_i}.$$

Now $\frac{1}{p^m} \leqq \frac{1}{2}$ gives us

$$\sum_{i=2}^{r} \frac{d_i - 1}{f_i d_i} < \frac{1}{2}.$$

Each term, which is not zero, is $\geqq \frac{1}{4}$. So there is at most one term $\neq 0$ and then only with $f_2 = 2$. So $r = 1$ or $r = 2$. For $r = 1$ we obtain:

$N = p^m$, $d_1 = 1$, $r = 1$, case **I.**
If $r = 2$, $f_2 = 2$, p^m can be only $= 2$ or $= 3$. $p^m = 2$ gives $N = 2d_2$, $p = 2$, $m = 1$, $d_1 = 1$, $r = 2$, d_2 odd, $f_2 = 2$, case **II.**
If $p^m = 3$, the only possibility is $d_2 = 2$ and $N = 12$:
$N = 12$, $p = 3$, $m = 1$, $d_1 = 1$, $r = 2$, $d_2 = 2$, $f_2 = 2$, case **III.**

Now we put $d_1 > 1$, and we treat first the case $f_1 = 1$. Then

$$\frac{1}{N} = \frac{1}{d_1 p^m} - \sum_{i=2}^{r} \frac{d_i - 1}{f_i d_i}.$$

Now $p^m \geqq 3$ ($p^m = 2$ gives $d_1 = 1$) and so $\frac{1}{d_1 p^m} \leqq \frac{1}{6}$:

$$\sum_{i=2}^{r} \frac{d_i - 1}{f_i d_i} < \frac{1}{6},$$

which is only possible if the sum is void, so $r = 1$ and:

$$N = d_1 p^m,\ d_1 \mid p^m - 1,\ f_1 = 1,\ r = 1,\ \text{case IV.}$$

Finally the case $d_1 > 1$, $f_1 = 2$. Then:

$$\frac{1}{N} = \frac{(d_1 - 1)p^m + 2}{2 d_1 p^m} - \sum_{i=2}^{r} \frac{d_i - 1}{f_i d_i}.$$

Now

$$\frac{(d_1 - 1)p^m + 2}{2 d_1 p^m} = \frac{1}{2} - \frac{p^m - 2}{2 d_1 p^m} < \frac{1}{2}$$

and so:

$$\sum_{i=2}^{r} \frac{d_i - 1}{f_i d_i} < \frac{1}{2}.$$

The sum has at most one term, and f_2 must be 2. A void sum ($r = 1$) is impossible; for in that case

$$N = \frac{2 d_1 p^m}{(d_1 - 1)p^m + 2}$$

and $N \geqq d_1 p^m$ give $(d_1 - 1)p^m \leqq 0$, which contradicts the assumption $d_1 > 1$. The only remaining case is $d_1 > 1$, $f_1 = 2$, $d_2 > 1$, $f_2 = 2$. For the discussion of this case the following consideration will be useful.

We shall count the number of conjugate cyclic groups of order d_2 in two different ways. First we take a special group $\mathfrak{C}$ of this type. A point, which is not a pole of $\mathfrak{C}$ is transformed by the transformations of $\mathfrak{C}$ into d_2 different points. A pole is transformed into d_2 different conjugate poles. If two poles of a cyclic group are interchanged by an element A of $\mathfrak{C}$, there exists for another group, the poles of which are obtained from the first by the transformation B of $\mathfrak{C}$, a transformation BAB^{-1} of $\mathfrak{C}$, which interchanges its poles. So the transformation with $\mathfrak{C}$ gives d_2 or $\frac{1}{2}d_2$ conjugate groups. If there remain groups which are not yet treated, we treat the remaining groups in the same way, and so on, until all groups are treated. Hence the number of conjugate groups is $1 + \frac{1}{2}d_2 g_1$, where g_1 is an integer. By transforming in an analogous way with a group of order d_1 we find, that the same number is $\frac{1}{2}d_1 g_2$. So we obtain $2 = g_2 d_1 - g_1 d_2$, hence $(d_1, d_2) = 1$ or 2.

Let M be the least common multiple of p^m, $2d_1$, $2d_2$. Now N is divisible by M, because the group contains subgroups of those orders. Further (10.1) and $(d_1, p) = 1$ imply $N = 1 + \frac{g}{M}N$ (g a positive integer) or

$$N = \frac{M}{M - g} \leqq M,$$

hence $N = M$.

If p is odd, two cases are possible:

$(d_1, d_2) = 2$ and $N = d_1 d_2 p^m$,

or $(d_1, d_2) = 1$ and $N = 2d_1 d_2 p^m$.

If $p = 2$, d_1 and d_2 are odd, so we have only one case:

$(d_1, d_2) = 1$ and $N = d_1 d_2 2^m$.

Now we substitute $r = f_1 = f_2 = 2$ in (10.2):

$$N = 1 + \frac{(d_1 + 1)p^m - 2}{2d_1 p^m} N + \frac{d_2 - 1}{2d_2} N. \tag{10.4}$$

Consider first the case $N = d_1 d_2 p^m$. In this case (10.4) becomes

$$(d_2 - d_1)p^m - 2(d_2 - 1) = 0. \tag{10.5}$$

If $p = 2$, d_1 and d_2 are odd, $d_2 - d_1$ even; if p is odd, $(d_1, d_2) = 2$, d_1 and d_2 are even, $d_2 - d_1$ also even. In both cases $\frac{1}{2}(d_2 - d_1)$ is an integer, and by (10.5) a positive integer. If we put $\frac{1}{2}(d_2 - d_1) = h$, then $d_2 = hp^m + 1$ and $d_1 = h(p^m - 2) + 1$, but $d_1 \leqq p^m - 1$, so $h = 1$ and $d_1 = p^m - 1$ and $d_2 = p^m + 1$:

$N = (p^m - 1)p^m(p^m + 1)$, $p^m \neq 2$, $d_1 = p^m - 1$, $f_1 = 2$, $r = 2$, $d_2 = p^m + 1$, $f_2 = 2$, case **V.**

Next consider the case $N = 2d_1 d_2 p^m$. Then (10.4) becomes:

$$(d_2 - d_1)p^m - (2d_2 - 1) = 0. \tag{10.6}$$

$(d_2 - d_1)$ is an integer, and according to (10.6) a positive integer. We put $d_2 - d_1 = k$, then $d_2 = \frac{1}{2}(kp^m + 1)$, $d_1 = \frac{1}{2}(kp^m + 1) - k$. Because d_2 is an integer, k must be odd. Further $d_1 \leqq p^m - 1$, hence $(k - 2)p^m \leqq 2k - 3$. If $k \neq 1$, we have

$$3 \leqq p^m \leqq \frac{2k - 3}{k - 2},$$

hence $k \leqq 3$. Therefore either $k = 1$, or $k = 3$ and $p^m = 3$.

If $k = 1$, we have $d_1 = \frac{1}{2}(p^m - 1)$, $d_2 = \frac{1}{2}(p^m + 1)$:

$N = \frac{1}{2}(p^m - 1)p^m(p^m + 1)$, $p \neq 2$, $p^m \neq 3$, $d_1 = \frac{1}{2}(p^m - 1)$, $f_1 = 2$, $r = 2$, $d_2 = \frac{1}{2}(p^m + 1)$, $f_2 = 2$, case **VI.**

If $k = 3$, we have $p^m = 3$, $d_1 = 2$, $d_2 = 5$:

$N = 60$, $p = 3$, $m = 1$, $d_1 = 2$, $f_1 = 2$, $r = 2$, $d_2 = 5$, $f_2 = 2$, case **VII.**

Thus all types of groups with parabolic elements are enumerated.

§ 11. The structure of the groups with parabolic elements.

We discuss the group-theoretical structure of the types of groups deduced in the preceding section.

I. This group is isomorphic to an *additive group* of order p^m in a field of characteristic p, or, expressed in terms of group theory, to the direct product of m cyclic groups of order p.

II. This group obviously is a *dihedral group*: it contains a cyclic group of order d_2, which lies, because of $f_2 = 2$, in a dihedral group of order $2d_2$, which constitutes already the whole group.

III. This group is the *tetrahedral group*: we may use for the $12 : 3 = 4$ poles of parabolic elements the same argument as for the 4 poles in § 5, case C, leading to the isomorphism to $\mathfrak{A}_4$.

IV. This group is a *metacyclic group*, as we have seen already in § 9. As explained in § 9, the additive group, contained in the group, is isomorphic to an additive field group, and there exists a field element η of order d_1 (primitive d_1^{th} root of the unity), which is multiplier of the additive group. The multiplicative Galois field $GF(p^k)$ of the additive group therefore contains the field of the d_1^{th} roots of the unity over the prime field $GF(p)$, i.e. the field $GF(p^r)$ with the smallest r, for which $d_1 \mid p^r - 1$. As the additive group may be considered as an additive group with respect to $GF(p^k)$, it is certainly an additive group with respect to $GF(p^r)$. The elements are of the form

$$a = \sum_{i=1}^{s} \gamma_i a_i \quad \left(s = \frac{m}{r},\ \gamma_i \text{ arbitrary in } GF(p^r)\right).$$

We now form the group of the elements:

$$x = \sum_{i=1}^{s} \gamma_i y_i,$$

here y_i being variables. The two groups are operatorisomorphic with respect to the elements of $GF(p^r)$ as operators, because

$$\eta x = \sum_{i=1}^{s} \eta\gamma_i y_i \text{ implies } \sum_{i=1}^{s} \eta\gamma_i a_i = \eta a.$$

This also gives an isomorphism between the given metacyclic

group and the metacyclic group having the group

$$\sum_{i=1}^{s} \gamma_i y_i$$

as its additive group. For if

$$A = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$$

are the elements of the additive group and

$$T = \begin{pmatrix} \eta & 0 \\ 0 & 1 \end{pmatrix}$$

a primitive element of order d_1, then AT^h form the metacyclic group. The calculation table for these elements may be deduced from

$$T^h A = \begin{pmatrix} \eta^h & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \eta^h & \eta^h a \\ 0 & 1 \end{pmatrix}.$$

Now let be $x \to a$ in the isomorphism, and $\eta^h x = x_1$, $x_1 \to a_1 = \eta^h a$ and

$$A_1 = \begin{pmatrix} 1 & a_1 \\ 0 & 1 \end{pmatrix},$$

then obviously $T^h A = A_1 T^h$ and so the multiplication of elements of the group is unambiguously determined.

V. The excluded case $p^m = 2$ is exactly case II, already treated, with $d_2 = 3$. The group contains $p^m + 1$ additive groups of order p^m, and so there are $p^m + 1$ poles of parabolic transformations. In the corresponding metacyclic group both poles of a cyclic group are conjugate ($f_1 = 2$), and therefore both are poles of parabolic transformations. As $\frac{1}{2}p^m(p^m + 1) = \binom{p^m + 1}{2}$ such cyclic groups exist, to each pair of points chosen from the $p^m + 1$ points there corresponds a cyclic group of order $p^m - 1$ having that pair of points as its pair of poles. The group is at any rate homomorphic to a permutation group of these $p^m + 1$ points. A transformation however, which leaves $p^m + 1 > 3$ points invariant, is certainly the identity, and therefore the homomorphism is an isomorphism. We may bring three of those points to 0, 1 and ∞. The group then contains the transformation

$$T = \begin{pmatrix} \eta & 0 \\ 0 & 1 \end{pmatrix}, \quad \eta^{p^m - 1} - 1 = 0, \text{ i.e. } \eta \text{ in } GF(p^m).$$

T transforms the point 1 into the point η, the powers of T transform 1 into the powers of η, i.e. into all elements $\neq 0$ of $GF(p^m)$. The $p^m + 1$ points are exactly the points of the binary projective space over $GF(p^m)$. Since the group is a permutation group of

the $p^m + 1$ points and since to each transformation of the group we may find a matrix in $GF(p^m)$ by considering three points of the $p^m + 1$ points and their images, the group is a subgroup of $PGL(2, p^m)$ in the notation of Van der Waerden [4]. The group is $PGL(2, p^m)$ itself, its order being $(p^m - 1)p^m(p^m + 1)$. This result holds also in the excluded case $p^m = 2$, because we get a permutation group of degree 3 and of order 6, whose objects may brought to 0, 1 and ∞.

VI. The excluded case $p^m = 3$ is exactly the case III, already treated. There are, as in the preceding case V, $p^m + 1$ poles of parabolic transformations of order p^m and $\frac{1}{2}p^m(p^m + 1) = \binom{p^m + 1}{2}$ cyclic groups with pairs of poles chosen from these $p^m + 1$ points, this time of order $\frac{1}{2}(p^m - 1)$. Here too the group is a permutation group of the $p^m + 1$ points, and three of those points may be brought to 0, 1 and ∞. The group contains the transformation

$$T^2 = \begin{pmatrix} \eta^2 & 0 \\ 0 & 1 \end{pmatrix}$$

with η^2 instead of η. To each of the $p^m + 1$ points corresponds a parabolic transformation having this point as its pole, which transforms another arbitrary point into a third arbitrary point, because the p^m parabolic transformations having the first point as their pole transform a certain point, which does not coincide with that pole, into p^m different points, and therefore all points except the first of the $p^m + 1$ points get their turn. So there exists in the group a parabolic element

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

which transforms ∞ into ∞ and 0 into 1. Now

$$\begin{pmatrix} \eta^{2d} & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \eta^{-2d} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \eta^{2d} \\ 0 & 1 \end{pmatrix}.$$

So the additive group contains the additive group, which lies in $GF(p^m)$, generated by the η^{2d} and of order p^k $(k \leqq m)$. This group contains η^{2d} and 0, so $\frac{1}{2}(p^m - 1) + 1 \leqq p^k$, $\frac{1}{2}p^m \leqq p^k$, $m \leqq k$, and therefore $m = k$. The additive group is $GF(p^m)$. Now

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

with b arbitrary in $GF(p^m)$ transforms 0 into b; the $p^m + 1$ points therefore are again the points of the binary projective space over $GF(p^m)$ and again the group is a subgroup of $PGL(2, p^m)$. To

show that it is $PSL(2, p^m)$, we observe, that the elements of $PSL(2, p^m)$ have a transformation determinant, which is a square in $GF(p^m)$. Now T^2 and therefore all transformations of the cyclic groups of order $\frac{1}{2}(p^m - 1)$ fulfill this requirement, just as all parabolic transformations. For T^2 this is obvious (η lies in $GF(p^m)$) and a transformation

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix}$$

is parabolic if $rx^2 + (s - p)x - q = 0$ has a double root, i.e. (characteristic $\neq 2$ is assumed in advance) if $(s - p)^2 + 4rq = 0$, i.e. $(s + p)^2 = 4(ps - rq)$. The transformation determinant is a square. If we count all transformations of the group of which we know already that they belong to $PSL(2, p^m)$, we find:

$$1 + (p^m + 1)(p^m - 1) + \tfrac{1}{2}p^m(p^m + 1)[\tfrac{1}{2}(p^m - 1) - 1] = \\ = \tfrac{1}{4}(p^m - 1)p^m(p^m + 3) > \tfrac{1}{4}(p^m - 1)p^m(p^m + 1).$$

The group has in common with $PSL(2, p^m)$ more than half of the elements, and so the group is $PSL(2, p^m)$. We could have shortened the last part of the proof, if we had used the theorem, that $PSL(2, p^m)$ is simple for $p^m \neq 2$ and $\neq 3$ (cf Dickson [1], § 104 and § 105). Finally the isomorphism to $PSL(2, p^m)$ also holds in the excluded case $p^m = 3$, because $PSL(2, 3)$, being a permutation group of degree 4 and order 12, is isomorphic to $\mathfrak{A}_4$.

VII. This group is the *icosahedral group*. The proof of § 5, case **E**, may be repeated literally, because the validity of the scheme at the end of § 4 may be deduced easily from what is said about normalizers of additive and cyclic groups in § 9. That the parabolic transformations are all conjugate follows from the fact, that -1, being a square root of unity, is a multiplier belonging to an element of the normalizer, and so

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix}$$

are conjugate.

§ 12. List of the groups and their conjugate subgroups.

On account of the preceding sections the contents of table I are clear. The table contains a complete list of all possible finite binary projective groups with their conjugate additive and cyclic subgroups. For the groups without parabolic elements we now have followed a choice of letters according to that of the groups with parabolic component.

TABLE I.

A. $N = d_1,\ r = 1,\ f_1 = 1.$ *cyclic*

1	normal	group	order	d_1	*groups.*

B. $N = 2d_2,\ r = 2,\ d_1 = 2,\ f_1 = 1,\ f_2 = 2.$

d_2 odd: d_2	conjugate	groups	order	2	
d_2 odd: 1	normal	group	order	d_2	
d_2 even, $d_2 \neq 2$: $\frac{1}{2}d_2$	conjugate	groups	order	2	
d_2 even, $d_2 \neq 2$: $\frac{1}{2}d_2$	conjugate	groups	order	2	*dihedral*
d_2 even, $d_2 \neq 2$: 1	normal	group	order	d_2	*groups.*
$d_2 = 2$: 1	normal	group	order	2	
$d_2 = 2$: 1	normal	group	order	2	
$d_2 = 2$: 1	normal	group	order	2	

C. $N = 12,\ r = 2,\ d_1 = 2,\ f_1 = 2,\ d_2 = 3,\ f_2 = 1.$

3	conjugate	groups	order	2	*tetrahedral*
4	conjugate	groups	order	3	*group.*

D. $N = 24,\ r = 3,\ d_1 = 2,\ f_1 = 2,\ d_2 = 3,\ f_2 = 2,\ d_3 = 4,\ f_3 = 2.$

6	conjugate	groups	order	2	*octa-*
4	conjugate	groups	order	3	*hedral*
3	conjugate	groups	order	4	*group.*

E. $N = 60,\ r = 3,\ d_1 = 2,\ f_1 = 2,\ d_2 = 3,\ f_2 = 2,\ d_3 = 5,\ f_3 = 2.$

15	conjugate	groups	order	2	*icosa-*
10	conjugate	groups	order	3	*hedral*
6	conjugate	groups	order	5	*group.*

I. $N = p^m,\ d_1 = 1,\ r = 1.$ *additive*

1 parabolic	normal	group	order	p^m	*groups.*

II. $N = 2d_2,\ p = 2,\ m = 1,\ d_1 = 1,\ r = 2,\ d_2$ odd, $f_2 = 2.$

d_2 conjugate parabolic		groups	order	2	*dihedral*
1	normal	group	order	d_2	*groups.*

III. $N = 12,\ p = 3,\ m = 1,\ d_1 = 1,\ r = 2,\ d_2 = 2,\ f_2 = 2.$

4 conjugate parabolic		groups	order	3	*tetrahedral*
3 conjugate		groups	order	2	*group.*

IV. $N = d_1 p^m,\ d_1 \mid p^m - 1,\ r = 1,\ f_1 = 1.$ *meta-*

1 parabolic	normal	group	order	p^m	*cyclic*
p^m conjugate		groups	order	d_1	*groups.*

V. $N = (p^m-1)p^m(p^m+1),\ p^m \neq 2,\ d_1 = p^m-1,\ r=2,\ f_1=2,\ d_2=p^m+1,\ f_2=2.$

$p^m + 1$ conjugate parabolic	groups	order	p^m	
$\frac{1}{2}p^m(p^m + 1)$ conjugate	groups	order	$p^m - 1$	$PGL(2, p^m)$.
$\frac{1}{2}(p^m - 1)p^m$ conjugate	groups	order	$p^m + 1$	

VI. $N=\frac{1}{2}(p^m-1)p^m(p^m+1),\ p\neq 2,\ p^m\neq 3,\ d_1=\frac{1}{2}(p^m-1),\ r=2,\ f_1=2,\ d_2=\frac{1}{2}(p^m+1),\ f_2 = 2.$

$p^m + 1$ conjugate parabolic	groups	order	p^m	
$\frac{1}{2}p^m(p^m + 1)$ conjugate	groups	order	$\frac{1}{2}(p^m-1)$	$PSL(2, p^m)$.
$\frac{1}{2}(p^m - 1)p^m$ conjugate	groups	order	$\frac{1}{2}(p^m+1)$	

VII. $N = 60,\ p = 3,\ m = 1,\ d_1 = 2,\ r = 2,\ f_1 = 2,\ d_2 = 5,\ f_2 = 2.$

10 conjugate parabolic		groups	order	3	*icosa-*
15 conjugate		groups	order	2	*hedral*
6 conjugate		groups	order	5	*group.*

§ 13. Equivalence of the groups of a type for groups with parabolic elements.

We now ask, whether the groups of one type are unambiguously determined except for linear transformation.

For additive groups this is not true. If we bring the pole to ∞, the transformations get the well-known form

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}. \tag{13.1}$$

b runs through an additive group of rank m over the prime field $GF(p)$. We may choose for b the elements of $GF(p^m)$. But we may also extend $GF(p)$ by adjoining m variables $y_1, \ldots, y_m$ and choose the additive group generated by $y_1, \ldots, y_m$. Now we try to transform by linear transformation the latter group into the former. We transform

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}.$$

As we know, the transformation matrix S must leave the pole invariant. In § 9 we have seen that the transformed element has the form

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

in which μ depends only on S, i.e. all elements of the field group are multiplied by the same factor. The field, generated by the quotients of the group elements remains the same. But the quotients y_i/y_j do not belong to $GF(p^m)$, except in the trivial case $m = 1$. For $m > 1$ the transformation therefore is impossible.

In the case $m = 1$ (cyclic group) a primitive element may be written in the form

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}. \tag{13.2}$$

We have left the possibility of transformation with

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

and we may just bring a point a into a point b with it:

$$a + q = b, \quad q = b - a.$$

We apply this in the case of the dihedral group. An element of order 2 may be brought into the form (13.2). By the remark just made we may bring a pole of a primitive element of order

d_2 to 0; it takes the form

$$\begin{pmatrix} \eta & 0 \\ c & 1 \end{pmatrix}, \text{ with } \eta^{d_2} = 1.$$

Now

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \eta & 0 \\ c & 1 \end{pmatrix} = \begin{pmatrix} \eta + c & 1 \\ c & 1 \end{pmatrix}$$

must have order 2, i.e. (remember $p = 2$) $\eta + c = 1$, $c = 1 + \eta$. So the elements

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} \eta & 0 \\ \eta + 1 & 1 \end{pmatrix}$$

are fixed, and as they generate the dihedral group, the group is also fixed.

For the tetrahedral group (characteristic 3) we bring a pole of an additive group to ∞; the transformations of this group take the form (13.1). The poles of an element of order 2 are brought to 0 and 1; the matrix of that element then is

$$\begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Now the product of these elements has again order 3, i.e. it is parabolic. It reads like this:

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} b-1 & b \\ 1 & 1 \end{pmatrix}$$

The poles are roots of the equation $x^2 - (1 + b)x - b = 0$. The transformation is parabolic, if $(1 + b)^2 + b = 1 + b^2 = 0$, i.e. $b = \pm i$ ($i = \sqrt{-1}$). The two elements are generators of the group. The bivalence of b may be eliminated by interchanging 0 and 1 and leaving ∞ invariant, i.e. by transforming with

$$\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}.$$

This gives

$$\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -i \\ 0 & 1 \end{pmatrix},$$

$$\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix} \equiv \begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix}.$$

We now consider the metacyclic group of order $d_1 p^m$. We know already that the additive group, contained in it, may be brought into the form (13.1), where b runs through an additive group $[\lambda_1, \ldots, \lambda_m]$ of rank m. This additive group may be changed only

into one which arises by multiplying all elements by a fixed factor μ. Let T be a primitive element of order d_1. We may bring the other pole of T to 0; T then becomes

$$T = \begin{pmatrix} \eta & 0 \\ 0 & 1 \end{pmatrix}.$$

η is a primitive d_1^{th} root of the unity. By replacing T by a power of T we may replace η by every other primitive d_1^{th} root of the unity. η must be a multiplier of the additive group. The multiplicative field $GF(p^k)$ of the additive group must contain the field $GF(p^r)$ of the d_1^{th} roots of the unity. For the rest the additive field group is perfectly arbitrary: we may choose $s = \frac{m}{r}$ elements $\gamma_1, \ldots, \gamma_s$ arbitrarily in a field which contains $GF(p^r)$ and then choose for $[\lambda_1, \ldots, \lambda_m]$ the additive group of all elements

$$a = \sum_{i=1}^{s} a_i \gamma_i \quad (a_i \text{ in } GF(p^r)).$$

We may take e.g. $\gamma_1, \ldots, \gamma_s$ as basic elements of $GF(p^m)$ or as variables $y_1, \ldots, y_s$. The two groups obtained in this way are certainly not equivalent. Only in the case $r = m$, $s = 1$ we may change the variable y_1 by multiplication with a factor μ into the constant $\gamma_1 = 1$. Therefore:

The metacyclic group of order $d_1 p^m$, $d_1 \mid p^m - 1$ is unambiguously determined except for linear transformation if and only if the field of the d_1^{th} roots of the unity over $GF(p)$ is identical with $GF(p^m)$, or in other words if m is the smallest divisor k of m for which $d_1 \mid p^k - 1$.

The groups $PGL(2, p^m)$ and $PSL(2, p^m)$ are already brought into an unambiguously determined form by bringing three points to 0, 1 and ∞ in the structure proof of § 11.

Finally the icosahedral group (characteristic 3). For an arbitrary element of order 5 we may find an element of order 3 such that the product has order 2. The two elements then generate the group. We bring the poles of an element of order 5 to 0 and 1. It reads like this:

$$\begin{pmatrix} \varepsilon & 0 \\ \varepsilon - 1 & 1 \end{pmatrix}.$$

By taking a power of this element we may make ε equal to a certain given root of the equation $x^4 + x^3 + x^2 + x + 1 = 0$. We bring the pole of the element of order 3 to ∞. It then takes the

form (13.1). Now

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \varepsilon & 0 \\ \varepsilon - 1 & 1 \end{pmatrix} = \begin{pmatrix} \varepsilon + b(\varepsilon - 1) & b \\ \varepsilon - 1 & 1 \end{pmatrix}.$$

This must have order 2, and so $\varepsilon + b(\varepsilon - 1) + 1 = 0$, $b = \dfrac{1+\varepsilon}{1-\varepsilon}$.

By this the unambiguously determined form has been obtained.

The results of this section may be summarized in the following theorem:

THEOREM 13.1. Two groups with parabolic elements of the same type and with the same value of the constants p, m and d_i may be transformed into one another by linear transformation, except in the following cases:

case I: additive group of order p^m, if $m > 1$,
case IV: metacyclic group of order $d_1 p^m$, if $d_1 \mid p^k - 1$ with $k < m$.

§ 14. Existence of the groups with parabolic elements.

From the results on the form into which the transformations of the groups may be brought we infer, just as for groups without parabolic elements, the existence of the groups of the different types after properly chosen extension of the basic field.

It is clear in advance that the prime order corresponding to the parabolic elements must be the same as the characteristic of the field (in this section always denoted by p). This natural restriction is always made in what follows. We may adjoin the $(p^m - 1)^{\text{th}}$ roots of the unity to the basic field and so make $GF(p^m)$ to a subfield of the basic field. Then from the results of the preceding section the existence of the additive and metacyclic groups follows immediately. For the dihedral group we adjoin the d_2^{th} roots of the unity and then find in (6.2) an always existing representation. (The elements of order 2 there may be parabolic). The groups $PGL(2, p^m)$ and $PSL(2, p^m)$ exist over $GF(p^m)$, the tetrahedral group exists as $PSL(2, 3)$. Finally for the icosahedral group we may literally repeat the proof of existence of § 7: nowhere the fact is used that the poles of the element of order 3 should be different. This completes the proof of existence and gives us:

THEOREM 14.1. The necessary and sufficient condition for the existence of the groups with parabolic elements after properly chosen extension of the basic field is that the prime order occuring in the additive subgroups be equal to the characteristic p of the field.

Interesting is also the question whether the restrictions on the characteristic for the types of groups without parabolic elements may be dropped if we admit for those types groups with parabolic elements. First of all cyclic groups exist only if the order is prime to p or equal to p. For if the order is prime to p, there exist cyclic groups with different poles, and if it is equal to p, there exists an additive cyclic group of order p. This turns out to be the only restriction we have to make for the types of groups with respect to the cyclic subgroups occuring in it. This is expressed in the following theorem.

THEOREM 14.2. The types of groups without parabolic elements exist after properly chosen extension of the basic field, possibly as groups with parabolic elements, if and only if the following requirements concerning the characteristic of the basic field are fulfilled:

for the cyclic group of order d_1: no divisor of d_1 or $= d_1$,
for the dihedral group of order $2d_2$: no divisor of d_2 or $= d_2$,
for the tetrahedral group: no restriction,
for the octahedral group: $\neq 2$,
for the icosahedral group: no restriction.

PROOF: The necessity of these requirements has been shown already. Now we assume that they are fulfilled. We may restrict us to the cases in which the conditions of the corresponding theorem about groups without parabolic elements in § 7 (theorem 7.1) are not fulfilled, because in the other cases that theorem gives the required proof of existence.

The cyclic group has been treated already. For the dihedral group we get first the case $p = 2$; d_2 then is also 2 or odd. If d_2 is odd we get case II; $d_2 = 2$ gives a four-group, which occurs as an additive group with $p^m = 4$. Finally the case $p = d_2 \neq 2$; this dihedral group occurs as a metacyclic group with $p \neq 2$ and $d_1 = 2$, $m = 1$. For the tetrahedral group we have $p = 2$ or $p = 3$. Now $p = 3$ gives case III, for $p = 2$, the group occurs as a metacyclic group with $p^m = 4$ and $d_1 = 3$. For the octahedral group we have $p = 3$ and then $PGL(2, 3)$ meets the requirements. Finally for the icosahedral group we have $p = 2$, $p = 3$ and $p = 5$. Now $p = 3$ gives case VII, $p = 2$ is fulfilled by $PGL(2, 4)$ and for $p = 5$ we have $PSL(2, 5)$, because the isomorphism of $PSL(2, 5)$ and $\mathfrak{A}_5$ may be shown literally in the same way as in § 5, case **E**.

This completes the proof.

REFERENCES.

L. E. DICKSON

[1] Linear groups, with an exposition of the Galois field theory, Leipzig 1901.

F. KLEIN

[2] Über binäre Formen mit linearen Transformationen in sich selbst, Math. Ann. 9 (1876), 183—208.

H. H. MITCHELL

[3] Determination of the ordinary and modular ternary linear groups, Trans. Amer. Math. Soc. 12 (1911), 207—242.

B. L. VAN DER WAERDEN

[4] Gruppen von linearen Transformationen, Erg. d. Math. IV 2, Berlin 1935.

(Oblatum 19-5-50).

Mathematisch Centrum,
Amsterdam.