STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZW 1951- 33 c

Existence and equivalence of finite binary projective groups

W. Peremans

Reprinted from
Compositio Mathematica, 9(1951), p 169-192

1951

W. PEREMANS

COMPOSITIO MATHEMATICA

VOLUMEN 9

FASCICULUS 2

W. PEREMANS

Existence and equivalence of finite binary projective groups

In Aedibus
P. NOORDHOFF - GRONINGEN
1951

Existence and equivalence of finite binary projective groups[1])

by

W. Peremans

§ 1. Introduction.

In another paper [2]) the author has treated the finite binary projective groups over an arbitrary commutative basic field. There, however, extensions of the basic field, if they were necessary for an easy treatment, were assumed to be performed. In this paper we discuss some problems concerning these groups without this assumption.

First of all we discuss the existence of different types of groups. In B.P. we have set up a list of all possible finite subgroups of the binary projective group [3]). Moreover we have proved there, that, besides some obvious restrictions concerning the characteristic of the basic field, the existence of all those possible groups can be established by a suitable extension of the basic field. We shall investigate now, which groups exist over a given commutative field without extension. This discussion constitutes part I of this paper. The problem causes difficulties only in the case of the tetrahedral, octahedral and icosahedral groups. Apart from the lowest values (2, 3 and 5) of the field characteristic, the condition for the existence of these 3 groups is, that the field must be a splitting field of the quaternions, which means that the equation $x^2 + y^2 + z^2 = 0$ must have a non-trivial solution in the field. (Moreover, in the case of the icosahedral group, 5 must be a square.) This condition will be considered somewhat more in detail, especially in the case, when the basic field is an algebraic number field.

Another question, which may be posed is, whether two groups of the same type may be transformed into one another by linear

---

[1]) Part I of this paper contains results of the last section of the author's thesis, part II is new.

[2]) Finite binary projective groups, Comp. Math. 9, 97—129; in the following we shall refer to this paper with B.P.

[3]) This list will be reproduced in § 2 of this paper.

transformation. We may express this question also by asking whether two such groups are conjugate in the whole projective group, or whether they are equivalent in the sense of representation theory. In B.P. the method, by which this problem was treated, consisted in transforming generators of the group under discussion into some canonical form. This canonical form and the transformations which leaded to it, were permitted to belong to the projective group over an extension of the basic field. In part II of this paper this extension will not be allowed. The results about the existence show us already, that a fixed canonical form, independent of the choice of the basic field, cannot be expected in all cases, because there exist splitting fields of the quaternions, which have only the field of rational numbers in common, which is not a splitting field of the quaternions. So we must try to transform directly one group into another. The resulting conditions, under which all groups are conjugate, are simple in most of the cases. Only for the dihedral groups they are rather involved.

§ 2. Some results of B.P.

Throughout the whole paper K denotes the basic field and p its characteristic. The following finite binary projective groups are possible:

Groups without parabolic elements:

A. Cyclic groups of order N.
B. Dihedral groups of order $2n$.
C. Tetrahedral group (order 12).
D. Octahedral group (order 24).
E. Icosahedral group (order 60).

Groups with parabolic elements in fields of characteristic p:

I. Additive groups of order p^m (m arbitrary).
II. Dihedral groups of order $2d_2$ ($p = 2$, d_2 odd).
III. Tetrahedral group ($p = 3$).
IV. Metacyclic groups of order $d_1 p^m$ (m arbitrary, $d_1 | p^m - 1$).
V. The general projective group $PGL(2, p^m)$, $p^m \neq 2$.
VI. The special projective group $PSL(2, p^m)$, $p \neq 2$, $p^m \neq 3$.
VII. Icosahedral group ($p = 3$).

The groups without parabolic elements exist in a suitable extension of K, if p is no divisor of the order of the group. Similarly the groups with parabolic elements exist if p has the prescribed value. In the following we tacitly assume that these conditions are fulfilled.

If the conditions for the existence of the groups without parabolic elements are not fulfilled, these groups may nevertheless exist as a group with parabolic elements in the following cases:
Cyclic groups: if $p = N$, as additive groups with $m = 1$ (case I).
Dihedral groups: if $p = 2$, n odd, as case II.
if $p = n = 2$, as an additive group with $p = 2$, $m = 2$ (case I).
if $p = n \neq 2$, as metacyclic groups with $m = 1$, $d_1 = 2$ (case IV).
Tetrahedral group: if $p = 2$, as a metacyclic group with $p = 2$, $m = 2$, $d_1 = 3$ (case IV).
if $p = 3$, as case III.
Octahedral group: if $p = 3$, as $PGL(2,3)$ (case V).
Icosahedral group: if $p = 2$, as $PGL(2,4)$ (case V).
if $p = 3$, as case VII.
if $p = 5$, as $PSL(2,5)$ (case VI).

Two isomorphic groups are always conjugate in the projective group over an extended basic field, except for additive groups if $m > 1$, and for metacyclic groups if $d_1 \mid p^k - 1$ with $k < m$.

Part I.

Existence.

§ 3. Cyclic and dihedral groups without parabolic elements.

A fixed point (pole) of a binary projective transformation is a root of a quadratic equation, and so needs not belong to K. Since we are not allowed to extend K we cannot always make use of the poles. This constitutes the main difference with the treatment in B.P. More general forms than the diagonal form of the matrix of the transformation must be considered.

We first consider non-parabolic cyclic groups of order N. Since a matrix of order 2 always exists, we may assume $N \neq 2$. Every two-rowed matrix, which is not a multiple of identity, may be reduced to the canonical form:

$$\begin{pmatrix} y & 1 \\ z & 0 \end{pmatrix}.$$

$N \neq 2$ gives $y \neq 0$. By transforming with

$$\begin{pmatrix} z & 0 \\ 0 & -y \end{pmatrix}$$

the matrix takes the form

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

with $a = -y^2/z$.
The characteristic polynomial of this matrix is

$$f(x) = x^2 - ax + a.$$

In a field which contains the poles of A (K or a quadratic extension of K), the poles may be brought to 0 and ∞ and the matrix assumes the form

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

If A has order N, r must be a primitive N^{th} root of unity ζ. As the quotient of the characteristic roots is invariant under linear transformation the roots x_1, x_2 of $f(x) = 0$ satisfy

$$\frac{x_1}{x_2} = \zeta.$$

We now have

$$\zeta + \zeta^{-1} = \frac{x_1}{x_2} + \frac{x_2}{x_1} = \frac{x_1^2 + x_2^2}{x_1 x_2} = \frac{(x_1 + x_2)^2 - 2x_1 x_2}{x_1 x_2} = \frac{a^2 - 2a}{a} = a - 2,$$

so our matrix becomes

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

with $k = \zeta + \zeta^{-1} + 2$. Conversely if A has this form, it has order N. So we get

THEOREM 3.1. Necessary and sufficient in order that in a field K a non-parabolic matrix of order N exists is that
1° N is not divisible by the characteristic.
2° $\zeta + \zeta^{-1}$ lies in K, if ζ denotes a primitive N^{th} root of unity [4]).
It is clear that the theorem also holds in the originally excluded case $N = 2$. From this theorem it follows, that ζ must lie in K or in a quadratic extension of K. In the latter case it must be conjugate to ζ^{-1} with respect to K.

Because the cyclotomic polynomials of orders 2, 3, 4 and 6 are of the first or second degree, matrices of those orders exist in every field, e.g.

---

[4]) I owe this proof, which is much simpler than that given in my thesis, to Prof. B. L. VAN DER WAERDEN.

$N = 2;\ A = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$

$N = 3;\ k = 1;\ A = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}.$

$N = 4;\ k = 2;\ A = \begin{pmatrix} 2 & 1 \\ -2 & 0 \end{pmatrix}.$

$N = 6;\ k = 3;\ A = \begin{pmatrix} 3 & 1 \\ -3 & 0 \end{pmatrix}.$

For $N = 5$ our condition 2° requires that $\alpha = \zeta + \zeta^{-1}$, a root of the quadratic equation

$$\alpha^2 + \alpha - 1 = 0,$$

lies in the field K. If $p = 2$, α is a third root of unity; in all other cases we have

$$\alpha = -\tfrac{1}{2} + \tfrac{1}{2}\sqrt{5}.$$

We must remember, that $k = \zeta + \zeta^{-1} + 2$ depends on the choice of the primitive root of unity, ζ.

From now on we suppose that we know, whether a cyclic group of any given order exists in K or not. In considering any type of non-cyclic group, we shall assume that for all orders of non-parabolic cyclic subgroups the conditions of Theorem 3.1 are satisfied. If not, the group cannot exist.

To prove the existence of the dihedral group of order $2n$ without parabolic elements ($n \neq 2$) we bring an element of order n into the form

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

An element of order 2 must have the form

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

Now

$$AB = \begin{pmatrix} k & 1 \\ -k & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & -a \end{pmatrix} = \begin{pmatrix} ak + c & bk - a \\ -ak & -bk \end{pmatrix}$$

must have order 2. This gives $ak + c - bk = 0$, $c = bk - ak$,

$$B = \begin{pmatrix} a & b \\ bk - ak & -a \end{pmatrix}.$$

Here a and b may be chosen at will, provided the matrix is not singular, e.g. $a = 0$, $b = 1$ (we know $k \neq 0$). From $(AB)^2 = E$ and $B^2 = E$ follows by induction $(A^kB)^2 = E$. A^k and A^kB form

a dihedral group. So the dihedral group exists as soon as the cyclic group of order n exists.

For $p = 2$ and n odd, the same reasoning holds and yields the existence of the dihedral group of case II with parabolic elements, provided the cyclic group of order n exists in the field under consideration.

If $n = 2$, the dihedral group always exists:

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

So we have

THEOREM 3.2. Dihedral groups of order $2n$ without parabolic elements exist if and only if $p \neq 2$ and a non-parabolic group of order n exists (cf. theorem 3.1).

The tetrahedral, octahedral and icosahedral groups without parabolic elements being the most difficult to treat, they will be put off to the last.

§ 4. Parabolic groups.

For groups with parabolic elements the treatment is simpler because, apart from the case $p = 2$, the pole of an additive transformation always lies in K. For such a pole is a double root of a quadratic equation with coefficients in K and therefore must belong itself to K. This conclusion does not hold if $p = 2$. Until further notice we assume $p \neq 2$.

For the additive group of order p^m the common pole can be brought to ∞; the transformations then get the form

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

where b runs through an additive group in K. Such an additive group only exists if the order of K is p^m at least. In the case of the metacyclic group we have the same condition for the additive subgroup. In B.P. § 11 we have found that the d_1^{th} roots of unity must lie in K. If this is the case we may form an additive group of order p^m with respect to the field $GF(p^r)$ of the d_1^{th} roots of the unity over $GF(p)$, and then also the metacyclic group. Necessary and sufficient for the existence of the metacyclic group is, that K contains the d_1^{th} roots of unity and has an order not smaller than p^m.

The $p^m + 1$ poles of parabolic transformations of $PGL(2, p^m)$ and $PSL(2, p^m)$ certainly lie in K. Hence they may as exposed

in B.P. § 11 be transformed into the points of the space over $GF(p^m)$ by bringing three of them to 0, 1 and ∞. Necessary for the existence of these groups is, that K contains $GF(p^m)$ as a subfield. Obviously this is also sufficient.

The tetrahedral group (case III) always exists as $PSL(2,3)$ for $p = 3$.

For the existence of the icosahedral group for $p = 3$ (case VII) all non-parabolic cyclic subgroups, i.e. those of orders 2 and 5, must exist. Cyclic groups of order 2 always exist; for those of order 5 we have deduced the condition, that the roots of the equation

$$x^2 + x - 1 = 0$$

are in K. This is an irreducible, separable equation in $GF(3)$, having its roots in the quadratic extension $GF(9)$. Necessary and sufficient for the existence of a matrix of order 5 is that K contains $GF(9)$. If we call ε a fifth root of unity in $GF(81)$, we have $\varepsilon + \varepsilon^{-1} = \alpha$, where α is a root of $x^2 + x - 1 = 0$.
We put

$$A = \begin{pmatrix} \alpha + 2 & 1 \\ -\alpha - 2 & 0 \end{pmatrix}.$$

The existence of the icosahedral group then follows from the existence of a matrix B of order 3 such that AB has order 2 (cf. B.P. § 6).
Put

$$B = \begin{pmatrix} q & r \\ s & t \end{pmatrix},$$

then

$$AB = \begin{pmatrix} \alpha + 2 & 1 \\ -\alpha - 2 & 0 \end{pmatrix}\begin{pmatrix} q & r \\ s & t \end{pmatrix} = \begin{pmatrix} \alpha q - q + s & \alpha r - r + t \\ -\alpha q + q & -\alpha r + r \end{pmatrix}.$$

Condition for order 2 is $\alpha q - q + s - \alpha r + r = 0$, $s = (r-q)(\alpha-1)$.
Then

$$B = \begin{pmatrix} q & r \\ (r-q)(\alpha-1) & t \end{pmatrix}.$$

B has order 3 means B is parabolic. We may obtain this by putting e.g. $r = 0$, $q = t = 1$ (both poles in 0); then the transformation is certainly not singular. This proves the existence of the icosahedral group in a field K of characteristic 3 if and only if K contains $GF(9)$.

Finally we must consider the case $p = 2$. If the poles of the parabolic transformations lie in K all remains the same and so

we need only investigate whether the conditions for existence mentioned above can be weakened by using parabolic elements with poles not lying in K. Such a parabolic element has the form

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

The equation for the poles of this matrix reads

$$cx^2 + 1 = 0$$

and is irreducible if c is not a square. Thus a transformation of order 2 with its pole not in K (of characteristic 2) exists if and only if K is not perfect („vollkommen" in the sense of Steinitz).

If the group contains a non-parabolic cyclic group such that one of the pair of poles coincides with the pole of an arbitrary parabolic transformation of the group, the latter must lie in K.

We therefore may restrict ourselves to the cases in which p can be 2, and in which no non-parabolic cyclic groups with poles in the poles of additive groups occur, viz. cases I and II (cf. B.P. § 12; the condition there reads $d_1 = 1$). But the condition of case I that the order of K is $\geqq 2^m$, is certainly necessary, all finite fields being perfect. The condition of case II, that the cyclic group of order d_2 exists, obviously is necessary too.
So we get

THEOREM 4.1. For the existence without extension of the basic field K of the groups with parabolic elements we must add to the requirement that p has the prescribed value the following necessary and sufficient conditions:

case I: additive group of order p^m: order of K is $\geqq p^m$,

case II: dihedral group of order $2d_2$: cyclic group of order d_2 exists (cf. theorem 3.1),

case III: tetrahedral group for $p = 3$: no condition,

case IV: metacyclic group of order $d_1 p^m$: order of $K \geqq p^m$ and K contains the d_1^{th} roots of unity,

case V: $PGL(2, p^m)$: K contains $GF(p^m)$,

case VI: $PSL(2, p^m)$: K contains $GF(p^m)$,

case VII: icosahedral group for $p = 3$: K contains $GF(9)$.

We are left with the tetrahedral, octahedral and icosahedral groups without parabolic elements. They will be treated in the next section.

§ 5. The tetrahedral, octahedral and icosahedral groups without parabolic elements.

Necessary and sufficient for the existence of these groups is, that there is an element A of order resp. 3, 4 and 5 and an element B of order 3, whose product has order 2 (cf. B.P. § 6).

If ε denotes respectively a third, fourth or fifth root of unity, we may bring A into the form

$$A = \begin{pmatrix} k & 1 \\ -k & 0 \end{pmatrix}, \qquad k = \varepsilon + \varepsilon^{-1} + 2.$$

Let B be

$$B = \begin{pmatrix} x & y \\ z & u \end{pmatrix} \text{ with } x^2 + xu + u^2 + yz = 0.$$

Their product is

$$\begin{pmatrix} k & 1 \\ -k & 0 \end{pmatrix}\begin{pmatrix} x & y \\ z & u \end{pmatrix} = \begin{pmatrix} kx + z & ky + u \\ -kx & -ky \end{pmatrix}.$$

This must have order 2, so $kx + z - ky = 0$, or $z = k(y - x)$. The first condition now becomes

$$x^2 + xu + u^2 + k(y - x)y = 0. \tag{5.1}$$

We must add to this the condition of non-singularity for the matrix of order 3:

$$xu - yz \neq 0.$$

Since

$$-yz = x^2 + xu + u^2,$$

this condition may be written as

$$x + u \neq 0.$$

The equation (5.1) may be brought into a simpler form by a non-singular homogeneous linear transformation in the basic field. We do this for the three groups separately.

1. Tetrahedral group. $k = 1$. We may write the equation

$$\tfrac{1}{2}(x^2 + xu + u^2 + y^2 - xy) = 0.$$

By the transformation

$$\left.\begin{aligned} x &= 2x' \\ u &= -x' + u' + y' \\ y &= x' - u' + y' \end{aligned}\right\} \text{determinant } = 4 \neq 0,$$

this becomes if we omit the accents

$$x^2 + u^2 + y^2 = 0.$$

2. Octahedral group. $k = 2$. We may write the equation.

$$\tfrac{1}{2}x^2 + \tfrac{1}{2}xu + \tfrac{1}{2}u^2 + y^2 - xy = 0.$$

By the transformation

$$\left.\begin{aligned} x &= 2x' - 2u' \\ u &= \quad 2u' \\ y &= x' - u' + y' \end{aligned}\right\} \text{determinant} = 4 \neq 0,$$

this becomes

$$x^2 + u^2 + y^2 = 0.$$

3. Icosahedral group. Here k fulfills $k^2 - 3k + 1 = 0$. By the transformation

$$\left.\begin{aligned} x &= 2(k-1)x' \\ u &= -(k-1)x' + u' \\ y &= (k-1)x' + (k-2)y' \end{aligned}\right\} \text{determinant} = 2(k^2 - 3k + 2) = 2 \neq 0$$

(5.1) becomes

$$x^2 + u^2 + y^2 = 0.$$

In the three cases the form of the equation now is the same. The conditions for non-singularity now read as follows in the three cases:

1° $x + y + u \neq 0$,
2° $x \neq 0$,
3° $(k-1)x + u \neq 0$.

These conditions may be replaced by the condition, that x, u and y are not all $= 0$ (i.e. that the solution is non-trivial).

If in case 1° a non-trivial solution exists, for which $x+y+u=0$, we replace the value of one variable, which is $\neq 0$, by its opposite. In case 2° by permutation of the values of the variables x may be made $\neq 0$. In the same way in case 3° u may be made $\neq 0$; if then $(k-1)x + u = 0$, we replace u by $-u$.

It is well known that in a field in which

$$x^2 + y^2 + u^2 + z^2 = 0 \tag{5.2}$$

has a non-trivial solution, also

$$x^2 + y^2 + u^2 = 0 \tag{5.3}$$

has a non-trivial solution. For if $\xi_1^2 + \xi_2^2 + \xi_3^2 + \xi_4^2 = 0$, $\xi_4 \neq 0$, we need only take [5]) $(\xi_1\xi_3 - \xi_2\xi_4,\ \xi_1\xi_4 + \xi_2\xi_3,\ \xi_3^2 + \xi_4^2)$ if -1 is not a square in K and $(\sqrt{-1}, 1, 0)$ if -1 is a square in K.

---

[5]) This expression may be found with use of the famous identity of EULER.

Now the fields in which (5.2) has non-trivial solutions are exactly the splitting fields of the ordinary quaternions (cf. Van der Waerden [6], Kap. 16).

We remark that fields, which contain the third, fourth or fifth roots of unity, are splitting fields of the quaternions; for the third and fourth this follows immediately from their defining equation: $0 = \varepsilon^2 + \varepsilon + 1 = \varepsilon^2 + (\varepsilon^2)^2 + 1^2$, respectively $0 = \varepsilon^2 + 1 = \varepsilon^2 + 1^2$, for the fifth we shall show it later on.

Finally we remember that the condition that the fifth roots of unity are at most quadratic over K is the same as the condition that 5 is a square in K. Collecting our results, we obtain the following theorem:

THEOREM 5.1. The tetrahedral, octahedral and icosahedral groups are realisable as groups of binary projective transformations without parabolic elements in those and only those fields K, which fulfill the following conditions:

1° the characteristic of K is $\neq 2$ and $\neq 3$ and for the icosahedral group also $\neq 5$,

2° only for the icosahedral group: 5 is a square in K,

3° K is a splitting field of the ordinary quaternion system.

Finally we write down the conditions for existence of the types of groups discussed before in the cases in which they occur as groups with parabolic elements. These conditions are found immediately by means of the list in § 2 and theorem 4.1:

cyclic groups;	if $p = N$, no condition.
dihedral groups;	if $p = 2$, n odd, same condition as in case B.
	if $p = n = 2$, order of K is $\geqq 4$.
	if $p = n \neq 2$, no condition.
tetrahedral group;	if $p = 2$, K contains the third roots of unity (i.e. K contains $GF(4)$).
	if $p = 3$, no condition.
octahedral group;	if $p = 3$, no condition.
icosahedral group;	if $p = 2$, K contains $GF(4)$.
	if $p = 3$, K contains $GF(9)$.
	if $p = 5$, no condition.

The conditions for the icosahedral group correspond to the condition that the fifth roots of unity are quadratic over K. New conditions, which do not appear for the groups without parabolic elements, occur only in the cases of the dihedral group for $p = n = 2$ (four-group for $p = 2$), $GF(2)$ being excluded, and the tetrahedral group for $p = 2$, because K must contain the third roots of unity.

§ 6. Which fields are splitting fields of the quaternions?

To this question we may apply the results of the theory of algebras.

The case that the characteristic of the field is $\neq 0$ is immediately solved as follows

THEOREM 6.1. All fields of characteristic p are splitting fields of the quaternion system.

PROOF: It is sufficient to consider the prime fields. These however are finite and the quaternion system with such a field as basic field also, but finite non-commutative fields do not exist, so they must be splitted. The proof does not hold if $p = 2$, the quaternion system then being commutative. A commutative field is impossible, because $x^2 + 1 = 0$ has more than two solutions in the quaternion system and this proves the theorem for $p = 2$.

If K is an algebraic number field it is possible to apply arithmetical methods to characterize the splitting fields. We consider this case somewhat more in detail. For the results from the arithmetic theory of hypercomplex systems, which are used in the following, cf. e.g. DEURING [1], Kap. 6 and 7.

If R is the field of the rational numbers and K an algebraic numberfield, the necessary and sufficient condition for K to be a splitting field of an algebra A over R, is that all $\mathfrak{p}$-adic extensions $K_\mathfrak{p}$ of K, belonging to a prime ideal $\mathfrak{p}$ in K are splitting fields of the p-adic extended algebra A_p, in which p is the prime number, which is multiple of $\mathfrak{p}$, and the same for the (real or complex) extensions belonging to the infinite prime places. Cf. for this Hasse [3] and Köthe [4].

Now for a simple algebra over a p-adic numberfield the splitting fields are those whose degrees are multiples of the index of the algebra.

The p-index of an algebra however is $\neq 1$ only if p is divisor of the discriminant of the algebra. So a condition arises only from the prime divisors of the discriminant, and from the infinite places.

The discriminant of the quaternion system is -16.

We therefore need only consider ∞ and the prime divisors of 2. Now ∞ gives the condition that K is not formally real: the rank of the perfect extension of K must be > 1 over the real closed field contained in it. This condition is obvious, for in a real field a sum of squares never may be zero non-trivially.

The prime divisors of 2 give raise to $\mathfrak{p}$-adic extensions of K, which are found as follows (cf. Van der Waerden [5] § 76): resolve the defining equation of K into 2-adic irreducible factors. Let those factors have degrees $g_1, \ldots, g_r$. Then the $\mathfrak{p}$-adic extensions of K, which belong to prime divisors of 2 have also degrees $g_1, \ldots, g_r$.

We may also resolve 2 in K into powers of prime ideals

$$2 = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2} \ldots \mathfrak{p}_r^{e_r}.$$

Let $\mathfrak{p}_i$ have degree f_i. Then

$$g_i = e_i f_i.$$

The $\mathfrak{p}$-adic extensions of degrees $g_1, \ldots, g_r$ are on account of the theorem just mentioned splitting fields of the quaternion algebra only if their degrees $g_1, \ldots, g_r$ are all even. We thus get the following criterion:

THEOREM 6.2. Necessary and sufficient for a number field K to be a splitting field of the quaternions is:

1° that K is not formally real, i.e. has no real conjugate,

2° that in the resolution of 2 into powers of prime ideals the products $e_i f_i$ of exponents and degrees are all even.

We may also formulate this criterion by using the defining equation of K:

THEOREM 6.3. Necessary and sufficient for a number field K to be a splitting field of the quaternions is, that the defining equation of K has only even prime factors both over the fields of real and of 2-adic numbers.

We shall illustrate this by some examples. First of all we show that every field of characteristic $\neq 5$ which contains the fifth roots of unity, is a splitting field of the quaternions. It will be sufficient to do this for the fields of the fifth roots of unity over the prime fields. The finite prime fields are splitting fields themselves; only the case of R, the field of rational numbers, remains. This is treated with the above-mentioned arithmetic conditions as follows. The equation

$$x^4 + x^3 + x^2 + x + 1 = 0$$

has no real roots, and therefore it resolves into two quadratic factors in the field of real numbers; further it is unsolvable as a congruence mod 2 and therefore cannot be resolved into 2-adic factors of odd degree. The field therefore is a splitting field. The result may also be obtained easily with use of the following well-known theorem of number theory (cf. Hecke [2], Satz 92): If

the prime number p is no divisor of m and f denotes the smallest exponent for which $p^+ \equiv 1(m)$, then p is in the field of the m^{th} roots of unity the product of exactly $\varphi(m)/f$ different prime ideals of degree f. In our case is $m = 5$, $p = 2$, so $f = 4$ and 2 is prime in the field of the fifth roots of unity. Since 4 is even, the field is a splitting field.

We now treat the case of the quadratic number fields $R(\sqrt{D})$, in which D is a square-free rational integer. The defining equation reads

$$x^2 - D = 0. \tag{6.1}$$

This must be resolved in the real and the 2-adic field. The field will be splitting field if (6.1) remains irreducible in both cases. For real numbers this is the case if and only if $D < 0$. For the 2-adic case we first consider:

$$x^2 - D \equiv 0(8). \tag{6.2}$$

This congruence is solvable only if $D \equiv 0$ (4) or $D \equiv 1$ (8). The case $D \equiv 0$ (4) is excluded, because D has been assumed to be square-free. If $D \not\equiv 1$ (8), (6.2) is unsolvable, so (6.1) is unsolvable, and hence irreducible in the field of 2-adic numbers.

If $D \equiv 1$ (8) we put $1 - D = 8h$ and transform x by $x = 2y + 1$; the equation becomes:

$$4(y^2 + y + 2h) = 0.$$

Now the polynomial

$$y^2 + y + 2h$$

is a product of 2 relatively prime factors y and $y + 1$ modulo 2.

It follows that this is also the case in the field of 2-adic numbers (cf. Van der Waerden [9], § 76 Reduzibilitätskriterium) and from this the same thing follows for the original equation (6.1). In this case K is no splitting field. So we find:

THEOREM 6.4. The quadratic number fields $R(\sqrt{D})$, D square-free, are splitting fields of the quaternions if and only if $D < 0$ and $D \not\equiv 1(8)$.

The field of the m^{th} roots of unity $R(\zeta)$, $\zeta^m = 1$ is also easily treated. For $m = 4$: $R(i)$, $i^2 = -1$, the field naturally is a splitting field, and the same holds if m is a quadruple. For $m = 2h$, h odd, the field is identical with that of the h^{th} roots of unity. We may therefore restrict ourselves to m odd. But this case is treated with use of the above-mentioned number theoretic theorem as follows. Let f be the smallest positive integer for which $2^f \equiv 1(m)$,

then the field of the m^{th} roots of unity is splitting field of the quaternions if and only if f is even.

Applying this criterion, we obtain the following theorem:

THEOREM 6.5. The field of the m^{th} roots of unity over R is splitting field of the quaternions if m is divisible by 4 or by an odd prime factor p such that the smallest exponent f, for which $2^f \equiv 1(p)$, is even, and only in these cases.

Part II.

EQUIVALENCE.

§ 7. Groups without parabolic elements.

We now consider the question whether two groups of the same type and the same value of the constants N, n, p, m, d_i may be transformed into one another by linear transformation (i.e. are conjugate in the whole projective group).

A *Cyclic group of order* N. We know that a non-parabolic matrix of order N ($N \neq 2$) may be brought into the form

$$A = \begin{pmatrix} k & 1 \\ -k & 0 \end{pmatrix} \quad \text{with } k = \zeta + \zeta^{-1} + 2,$$

where ζ is a primitive N^{th} root of unity.

The element $k = \zeta + \zeta^{-1} + 2$ is not uniquely determined by N, because ζ may be replaced by any other primitive N^{th} root of unity ζ^b. However, ζ is the quotient of the characteristic roots of the matrix A. Hence, if we replace A by A^b, ζ will be replaced by ζ^b.

So if $N \neq 2$, an arbitrary matrix of order N is conjugate to a power of another arbitrary matrix of order N, hence all cyclic groups of order N are conjugate.

Now the case $N = 2$. A matrix of order 2 may be brought into the form

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

Two such matrices (with c_1 and c_2) are conjugate if and only if $c_1 c_2^{-1}$ is a square. So e.g. in the field of rational numbers the square free integers give rise to infinitely many matrices of order 2 which are not mutually conjugate.

THEOREM 7.1. Non-parabolic cyclic groups of order N are always conjugate except if $N = 2$ and the basic field contains an element which is not a square.

We now consider, which transformations let invariant the above

mentioned canonical form of the matrices of order N ($N \neq 2$), viz.

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

One finds by easy calculation that this is the matrix

$$\begin{pmatrix} kr + t & r \\ -kr & -t \end{pmatrix}. \tag{7.1}$$

B *Dihedral group of order* $2n$. We first assume $n \neq 2$. We get

$$\begin{pmatrix} k & 1 \\ -k & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & -a \end{pmatrix} = \begin{pmatrix} ka + c & kb - a \\ -ka & -kb \end{pmatrix}.$$

So $ka + c - kb = 0$, and therefore we get

$$\begin{pmatrix} k & 1 \\ -k & 0 \end{pmatrix} \begin{pmatrix} a & b \\ kb - ka & -a \end{pmatrix} = \begin{pmatrix} kb & kb - a \\ -ka & -kb \end{pmatrix}.$$

We try to bring the second element into the canonical form ($a = 1$, $b = 0$):

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

by transformation with (7.1). This gives the following equation for r and t:

$$(k^2b - kb - ka)r^2 + 2(kb - a)rt + bt^2 = 0,$$

which is solvable if $kb^2 - kab + a^2$ is a square. When this is not the case we may not yet conclude that not all groups are conjugate, for it would be possible that another element of order 2 might be transformed into the canonical form. Although there exists an automorphism between two sets of generators, this automorphism needs not be a linear transformation. However, we need not distinguish between elements of order 2 which belong to the same class of conjugates in the dihedral group, as they are transformable into one another by linear transformation (that the transformation incidentally belongs to the dihedral group does not matter; moreover the transformation can be chosen in this way that the elements of order n are invariant). If n is odd, all elements of order 2 are conjugate; if n is even but $\neq 2$, there are two classes of elements of order 2; if $n = 2$ there are three classes (each of one element).

So for n odd we are ready and the groups are always conjugate if $a^2 - kab + kb^2$ is a square for all choices of a and b. If such a quadratic form can be splitted into two different linear factors, which is the case if K contains the n^{th} roots of unity:

$$a^2 - kab + kb^2 = [a - (\zeta + 1)b][a - (\zeta^{-1} + 1)b],$$

it may take all values of K and the condition is equivalent to the condition that all elements of K are squares. If K does not contain the n^{th} roots of unity the quadratic form is the norm of an element $c + d\zeta$ of $K(\zeta)$ ($a = c - d$, $b = -d$), and the condition is equivalent to the condition that all norms of elements of $K(\zeta)$ are squares in K.

If n is even we must also consider an element of order 2, which belongs to the other class of conjugates. If A denotes an element of order n and B an element of order 2, the two classes of elements of order 2, viz. A^hB, are those with h odd, resp. even. So we may choose for the element of the other class the product AB.

This comes into the canonical form if B gets the form

$$\begin{pmatrix} k & 1 \\ k - k^2 & -k \end{pmatrix}.$$

This gives the following equation for r and t:

$$(k^3b + 2k^2b + k^2a - ka)r^2 + 2(kb + ka - k^2b)\,rt + (a - kb)t^2 = 0,$$

which is solvable if $k(kb^2 - kab + a^2)$ is a square.

So the dihedral groups are all conjugate if for all choices of a and b either $a^2 - kab + kb^2$ or $k(a^2 - kab + kb^2)$ is a square. If K contains the n^{th} roots of unity this condition may be replaced by the condition that for all choices of c either c or kc is a square and this may be replaced by the condition that either c or ζc is a square, because $k\zeta = (\zeta + 1)^2$ is a square. If K does not contain the n^{th} roots of unity the condition is that for every element of $K(\zeta)$ either the norm N or kN is a square.

To show that the second condition is not superfluous if n is even and K contains the n^{th} roots of unity we give an example of a field in which not all elements are squares, but in which c or ζc is always a square. To do this we choose a prime p, such that $n \mid p - 1$ and $\frac{p-1}{n}$ is odd. This is possible, because the arithmetic progression with first term $n + 1$ and difference $2n$ contains an infinity of primes. If ε denotes a primitive element of $GF(p)$, ζ is an odd power of ε, viz. $\frac{p-1}{n}$. The elements of $GF(p)$ which are not squares are also odd powers of ε and their products with ζ are even powers of ε and therefore squares.

To show that the second condition is not superfluous if n is even and K does not contain the n^{th} roots of unity, it suffices to give an example of a field in which k is not a square, but in

which c or kc is always a square. We choose a prime p, such that $n \mid p+1$ and $\frac{p+1}{n}$ is odd. This is possible, because $(n-1, 2n) = 1$. We have $n \neq 2$. Now $GF(p)$ does not contain the n^{th} roots of unity but $GF(p^2)$ does, because $p \equiv -1(n)$, $p^2 \equiv 1(n)$. In $GF(p^2)$ each element is conjugate with its p^{th} power with respect to $GF(p)$. So the n^{th} root of unity is conjugate with its inverse (because $p \equiv -1(n)$) and k belongs to $GF(p)$. To show that k is not a square in $GF(p)$ we remark that $GF(p^2)$ contains also the $2n^{th}$ roots of unity, because $p \equiv -1(n)$ and n even imply $p^2 \equiv 1(2n)$, but a $2n^{th}$ root of unity is not conjugate with its inverse with respect to $GF(p)$, because $\frac{p+1}{n}$ odd implies $p \not\equiv -1(2n)$. So the sum of a $2n^{th}$ root of unity and its inverse does not belong to $GF(p)$, but this is just a square root of k. Now k is an odd power of a primitive element ε of $GF(p)$ and the elements of $GF(p)$ which are not squares too, and their products with k are even powers of ε and therefore squares.

We are left with the case $n = 2$ (four-group). We distinguish three cases.

(i) At least two elements of the four-group have their poles in K. If we bring the poles of one of them to 0 and ∞, and a pole of the other to 1 we get the canonical form

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

(ii) Only one element of the four-group has its poles in K. We get:

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

with neither c, nor $-c$ a square.

(iii) No element of the four-group has its poles in K. We get:

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

with $c + \lambda b = 0$, and so:

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

with λ no square, $(a^2 - \lambda b^2)$ no square, and $\lambda(\lambda b^2 - a^2)$ no square.

Case (i) is always possible. Some examples for the possibility of the other cases: in the field of rational numbers all three cases are possible; in $GF(3)$ only (i) and (iii) are possible; in $GF(5)$

only (i) and (ii) are possible and in the field of real numbers only (i) is possible.

Two four-groups belonging to different cases obviously are not conjugate. So all four-groups are conjugate if and only if cases (ii) and (iii) are impossible. Case (ii) gives that for every c at least one of c and $-c$ must be a square. If this is the case and λ and $(a^2 - \lambda b^2)$ are not squares, $(\lambda b^2 - a^2)$ is a square and $\lambda(\lambda b^2 - a^2)$ is not a square. So if λ is not a square $a^2 - \lambda b^2$ always must be a square, but $-\lambda$ is also a square and a and b arbitrary. So if there is an element λ which is not a square every sum of (two) squares must be a square. If all elements are squares this is also the case. So the four-groups are all conjugate in those and only those fields in which a sum of squares is a square and for every c at least one of c and $-c$ is a square.

THEOREM 7.2. The dihedral groups of order $2n$ without parabolic elements are conjugate in those and only those fields K which meet the following requirements:

(ζ denotes a primitive n^{th} root of unity, $k = \zeta + \zeta^{-1} + 2$)

if n is odd and the field contains the n^{th} roots of unity:
all elements of K are squares,
if n is odd and K does not contain the n^{th} roots of unity:
the norms of all elements of $K(\varsigma)$ are squares in K,
if n is even and $\neq 2$, and K contains the n^{th} roots of unity:
x or ζx is a square for all x,
if n is even and $\neq 2$ and K does not contain the n^{th} roots of unity:
for every element of $K(\zeta)$ the norm N or kN is a square in K,
if $n = 2$: every sum of squares is a square and x or $-x$ is a square for all x.

C, D, E. *Tetrahedral, octahedral and icosahedral groups.* We take a product of an element of order 3, 4 or 5 with one of order 3 such that the product has order 2. We get

$$\begin{pmatrix} k & 1 \\ -k & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ka + c & kb + d \\ -ka & -kb \end{pmatrix}$$

with $ka + c - kb = 0$, so

$$\begin{pmatrix} k & 1 \\ -k & 0 \end{pmatrix}\begin{pmatrix} a & b \\ kb - ka & d \end{pmatrix} = \begin{pmatrix} kb & kb + d \\ -ka & -kb \end{pmatrix}$$

with $a^2 + ad + d^2 - kab + kb^2 = 0$.

For the tetrahedral group we have $k = 1$, for the octahedral group $k = 2$, for the icosahedral group k is a root of $k^2 - 3k + 1 = 0$.

We transform the second matrix with (7.1) and try to determine r and t such that the transformed matrix becomes

$$\begin{pmatrix} a_1 & b_1 \\ kb_1 - ka_1 & d_1 \end{pmatrix}$$

with $a_1^2 + a_1 d_1 + d_1^2 - k a_1 b_1 + k b_1^2 = 0$ [6]).
This turns out to be possible with:

$$\frac{t}{r} = \frac{ad_1 + da_1 + dd_1 + kba_1 - kbb_1}{ab_1 - ba_1} =$$

$$= k\frac{aa_1 - ab_1 + da_1 - db_1 - ba_1 - bd_1}{ad_1 - da_1} =$$

$$= \frac{-kbd_1 + ad_1 - kbb_1 + aa_1 + da_1}{bd_1 - db_1}.$$

These fractions are not all indefinite. (It is remarkable that this holds whatever the value of k is, except $k = 0$ and $k = 3$). So we have

THEOREM 7.3. The tetrahedral, octahedral and icosahedral groups without parabolic elements are always conjugate.

§ 8. Groups with parabolic elements.

I. *Additive group of order* p^m. If $p \neq 2$, the pole of the group is in K and may be brought to ∞. The matrices of the group then read

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

and the only remaining possibility is a multiplication of all b with the same factor μ. So we may bring one of the elements in the form

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

but this is possible in $p^m - 1$ ways, but at most $\frac{p^m - 1}{p - 1}$ give rise to different additive groups, because $\mu, 2\mu, \ldots, (p-1)\mu$ give the same group. If $m = 1$, the additive group is the additive group of $GF(p)$ and so determined, and all groups are conjugate. We now assume $m > 1$.

If the field K is infinite there are infinitely many additive groups of order p^m, which contain 1, and so not all additive groups

[6]) Obviously a fixed canonical form is not obtainable in this case.

are conjugate. In $GF(p^n)$ $(n \geqq m)$ the number of different additive groups of order p^m, which contain 1, is

$$\frac{(p^n - p)(p^n - p^2) \dots (p^n - p^{m-1})}{(p^m - p)(p^m - p^2) \dots (p^m - p^{m-1})} = \frac{(p^{n-1} - 1)(p^{n-2} - 1) \dots (p^{n-m+1} - 1)}{(p^{m-1} - 1)(p^{m-2} - 1) \dots (p - 1)}.$$

If $2 \leqq m \leqq n-2$, this obviously is $> \frac{p^m - 1}{p - 1}$; the additive groups cannot all be conjugate. If $m = n$, only one additive group is possible. If $m = n - 1$ the number of possible additive groups is $\frac{p^{n-1} - 1}{p - 1}$. We show that the $\frac{p^{n-1} - 1}{p - 1}$ groups obtained by multiplication are all different. If two of them were identical, this group would have a multiplier not belonging to $GF(p)$. The multipliers however, form a field $GF(p^k)$ with $k \mid n - 1$, but, as $GF(p^k)$ is a subfield of $GF(p^n)$, also with $k \mid n$. This is only possible for $k = 1$ and this gives a contradiction. So we get the result that the additive groups of order p^m $(m > 1)$ are conjugate only in $GF(p^m)$ and $GF(p^{m+1})$. For $p = 2$ this result also holds; for $GF(2^m)$ and $GF(2^{m+1})$, because these fields are perfect and only groups with poles in the basic field are possible; for the other fields a fortiori. If $p = 2$ and $m = 1$, the groups are all conjugate if and only if all parabolic elements have their poles in the basic field, i.e. in perfect fields. Thus we get

THEOREM 8.1. Additive groups of order p^m are conjugate in those and only those fields K which meet the following requirements:

for $m = 1$, $p \neq 2$: no requirement,
for $m = 1$, $p = 2$: K is perfect,
for $m > 1$: K is $GF(p^m)$ or $GF(p^{m+1})$.

II. *Dihedral groups of order* $2d_2$ ($p = 2$, d_2 odd). The discussion is nearly the same as for case B (dihedral groups without parabolic elements). The equation for r and t now reads

$$(k^2b + kb + ka)r^2 + bt^2 = 0,$$

which is solvable if and only if $k^2b^2 + kb^2 + kab$ is a square.

This may be replaced by the condition that $kb^2 + kab$ is a square. Taking $a = 0$, $b = 1$, we obtain the necessary condition, that k is a square. If this is the case ab must be a square too. If K contains an element u which is not a square, for $a = 1$, $b = u$, ab is not a square. Thus all elements must be squares.

THEOREM 8.2. The dihedral groups of order $2d_2$ ($p = 2$, d_2 odd) are all conjugate if and only if the basic field is perfect.

III. *Tetrahedral group* ($p = 3$). An element of order 3 has its pole in K and may be brought into the form

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

So we get

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

and $a + c + d = 0$, so

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

with $a^2 + ad + d^2 - ab - bd = 0$.
By transformation with

$$\begin{pmatrix} a+d & -a+d \\ 0 & a+d \end{pmatrix}$$

the first matrix remains unchanged and the second turns into the canonical form:

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

THEOREM 8.3. Tetrahedral groups in fields of characteristic 3 are always conjugate.

IV. *Metacyclic groups of order* $d_1 p^m$. We bring the pole of the additive group to ∞, and transform one of the elements by multiplication into

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

A primitive element of order d_1 then reads

$$\begin{pmatrix} \eta & b \\ 0 & 1 \end{pmatrix}. \tag{8.1}$$

Transformation with

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

does not change all elements of the form

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

and transforms (8.1) into

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

We know that η is a multiplier of the additive group (B.P. § 9). If we denote by $GF(p^r)$ the field of the d_1^{th} roots of unity over $GF(p)$, the additive group must be an additive group with respect to $GF(p^r)$, but for the rest is arbitrary. The rest of the discussion runs along the same lines as in case I (additive groups). The multiplication which turns an element into the form

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

is possible in $p^m - 1$ ways, but at most $\dfrac{p^m - 1}{p^r - 1}$ give rise to different additive groups. If $m = r$, the additive group is the additive group of $GF(p^r)$ and so determined and the metacyclic groups are conjugate. We now assume $m > r$. If the order of K is infinite there are infinitely many additive groups of order p^m with respect to $GF(p^r)$ which contain 1, and not all metacyclic groups are conjugate. In $GF(p^n)$ $(n \geqq m)$ the number of different additive groups of order p^m with respect to $GF(p^r)$, which contain 1, is

$$\frac{(p^n - p^r)(p^n - p^{2r}) \dots \left(p^n - p^{(\frac{m}{r}-1)r}\right)}{(p^m - p^r)(p^m - p^{2r}) \dots \left(p^m - p^{(\frac{m}{r}-1)r}\right)} =$$

$$= \frac{(p^{n-r} - 1)(p^{n-2r} - 1) \dots (p^{n-m+r} - 1)}{(p^{m-r} - 1)(p^{m-2r} - 1) \dots (p^r - 1)}.$$

If $2r \leqq m \leqq n - 2r$, this obviously is $> \dfrac{p^m - 1}{p^r - 1}$. If $m = n$ only one additive group is possible. If $m = n - r$ the number of possible additive groups is $\dfrac{p^{n-r} - 1}{p^r - 1}$. We show that the $\dfrac{p^{n-r} - 1}{p^r - 1}$ groups obtained by multiplication are all different. If two of them were identical, this group would have a multiplier not belonging to $GF(p^r)$. The field of multipliers $GF(p^k)$ would satisfy $k \mid n - r$, $k \mid n$ and $k > r$. This is impossible.

THEOREM 8.4. Metacyclic groups of order $d_1 p^m$ are conjugate for $m = r$ always and for $m > r$ only in $GF(p^m)$ and $GF(p^{m+r})$, r denoting the least positive integer for which $d_1 \mid p^r - 1$.

V, VI. *$PGL(2, p^m)$ and $PSL(2, p^m)$.* The poles of the additive subgroups of these groups are always in K. By bringing three of them to 0, 1 and ∞ we get a canonical form of the group, as is already pointed out in BP § 11.

THEOREM 8.5. The groups $PGL(2, p^m)$ and $PSL(2, p^m)$ are always conjugate.

VII. *Icosahedral group* ($p = 3$). The treatment of case E (icosahedral group without parabolic elements) may be repeated literally. So we have

THEOREM 8.6. Icosahedral groups in fields of characteristic 3 are always conjugate.

Finally we state the conditions for equivalence for the types of groups without parabolic elements in the cases in which they occur as groups with parabolic elements. This gives:

Cyclic groups: if $p = N \neq 2$, no condition.
if $p = N = 2$, K is perfect, i.e. all elements of K are squares.

Dihedral groups: if $p = 2$, n odd, all elements of K are squares.
if $p = n = 2$, K is $GF(4)$ or $GF(8)$.
if $p = n \neq 2$, no condition.

Tetrahedral, octahedral and icosahedral groups: in all cases, no condition.

A new condition, which does not appear for the groups without parabolic elements, occurs only for the four-group if $p = 2$.

Finally I wish to express my sincere thanks to Prof. B. L. van der Waerden for his valuable advice on the subject of this paper.

REFERENCES.

M. DEURING,

[1] Algebren, Erg. d. Math. IV 1, Berlin 1935.

E. HECKE,

[2] Vorlesungen über die Theorie der algebraischen Zahlen, Leipzig 1923.

H. HASSE,

[3] Die Struktur der R. Brauerschen Algebrenklassengruppe über einem algebraischen Zahlkörper, Math. Ann. **107** (1933), 731—760.

G. KÖTHE,

[4] Erweiterung des Zentrums einfacher Algebren, Math. Ann. **107** (1933), 761—766.

B. L. v. d. WAERDEN,

[5] Moderne Algebra I, 2. Aufl., Berlin 1937.

[6] Moderne Algebra II, 2. Aufl., Berlin 1940.

(Oblatum 31-1-51)

Mathematisch Centrum
Amsterdam