FINITE SUBGROUPS OF $PGL_2(K)$ AND THEIR INVARIANTS

Ph. D. Thesis

E.M. GRUZA

Bedford College, University of London

A B S T R A C T

This thesis looks at finite subgroups of the pro= jective group of 2 x 2 matrices over a skew field and the invariants of these subgroups.

Chapter 0 recalls most of the preliminary results needed in subsequent chapters. In particular the con= struction of $K_k(x)$ is outlined briefly.

Chapter 1 establishes an isomorphism between the group of tame automorphisms in one variable over the skew field K and the projective group of 2 x 2 matrices over K, $PGL_2(K)$. It shows that if K is of suitable characteristic, then any element A of $PGL_2(K)$ of finite order has either two or else infinitely many fixed points in some extension of K. In particular this means that such A can be diagonalized.

Chapter 2 is divided into three sections. The first section deals with finite subgroups of $PGL_2(K)$ whose elements may have infinitely many fixed points. The second section analyses finite cyclic subgroups whose elements have only two fixed points. The third section finds the finite non-diagonal groups in $PGL_2(K)$ whose elements have exactly two fixed points. In particular a complete classification is given of the finite subgroups of $PGL_2(K)$ when the centre k of K is algebraically closed.

Chapter 3 shows that if the centre k of K is algebrai= cally closed, then any finite subgroup of $PGL_2(K)$ is in

fact conjugate to one in $PGL_2(k)$. It finds the fixed fields in $K_k(x)$ of the finite subgroups of $PGL_2(K)$ and shows that their respective generators are the same as in the commutative case.

TABLE OF CONTENTS

INTRODUCTION

Let k be a commutative field. There is a well known matrix representation of the automorphisms of k(x) over k, i.e. $\alpha : x \mapsto \frac{ax+b}{cx+d}$ is represented uniquely up to a scalar multiple by $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Moreover if A is of finite order n in $PGL_2(k)$ (and char $k \nmid n$), then it can be diagonalized over some extension of k. It is mainly these two facts which make possible a complete classifi= cation of the finite subgroups of $PGL_2(C)$, where C denotes the complex numbers (or indeed of any $PGL_2(k)$, where k is commutative and algebraically closed). It is possible to determine explicitly the fixed fields of these finite subgroups in their action on k(x) (this was done by Felix Klein over a hundred years ago in [6]).

The object of this thesis is to generalize these facts as far as possible to the case where k is not commutative.

Let K be a skew field with centre k. In the first chapter we shall find that all known automorphisms in one variable over K can be represented by a 2 x 2 matrix A (as above) which is unique up to a central scalar multiple. As in the commutative case we shall also see that any $A \in PGL_2(K)$ of finite order n can be diagonalized over some extension of K, provided char $K \nmid n$. One main differ= ence between the skew and the commutative case lies in the occurence of non-central scalar matrices. These, as well

as their conjugates in $PGL_2(K)$, we call quasiconjugations.

Chapter 2 deals with finite subgroups in $PGL_2(K)$. In particular a classification up to finite groups of diagonal matrices is given of those finite subgroups which do not contain any quasiconjugations. Indeed when the centre k of K is algebraically closed this will amount to a complete classification.

Chapter 3 proves that when k is algebraically closed, every finite group in $PGL_2(K)$ is conjugate to a group in $PGL_2(k)$. This allows the adaptation of some of the methods used in the commutative case to find the fixed fields of the finite subgroups of $PGL_2(K)$. It turns out that their generators are in fact the same as in the commutative case.

Detailed summaries of the content of the various chapters are given at the beginning of each chapter. Chapter 0 does not contain any original work and such results in the later chapters as are known not to be original will be credited to their sources.

The author wishes to record his gratitude to Prof. P.M. Cohn for his patient guidance and encouragement without which this work would not have been achieved.

A. Gruza

Bedford College
London
November 1978

0. PRELIMINARIES

In this chapter we assemble some of the facts and definitions which will be needed in the following chapters. Most of the theorems given here are due to P. M. Cohn and unless their proof is of special interest in our work later on we shall omit the latter but give appropriate references. Where the most general form of these results is not required we shall sometimes recall them in terms of the more specialized setting relevant to us. This will save us from making definitions which are not used afterwards.

Let K be a skew field with centre k. Denote by $K_k\langle x\rangle$ the ring obtained by adjoining to K the indeterminate x, with defining relations $xc = cx$ for all $c \in k$. The general element of $K_k\langle x\rangle$ has form

$$a + b_1xc_1 + \ldots + b_rxc_r + d_1xe_1xf_1 + \ldots + d_sxe_sxf_s + \ldots,$$

where $a, b_i, \ldots \in K$.

In the commutative case, i.e. when $K = k$, we have $K_k\langle x\rangle = k[x]$, the polynomial ring over k in one variable. Then $k[x]$ has field of fractions $k(x)$, the field of rational functions over k, which is fairly easy to construct from $k[x]$, mainly because the elements of $k(x)$ can all be written in the form fg^{-1}, where $f, g \in k[x]$, $g \neq 0$. In the non-commutative case even the existence of a field of fractions of $K_k\langle x\rangle$ is not obvious and its

construction requires very different methods. The following is a sketch of this construction; further details and proofs can be found in chapter 7 of [3].

Essentially we shall find that the elements of a field of fractions of $K_k\langle x\rangle$ are obtained as components of solutions of matrix equations. We shall also quote a criterion for the existence of a "universal" field of fractions of any general ring.

Let R,S be any rings and Σ a set of square matrices over R. A homomorphism $f: R \to S$ is said to be Σ - inverting if every matrix in Σ is mapped by f to an invertible matrix over S. Assume f is Σ - inverting, then the Σ - rational closure of R in S (under f) is defined as the set $R_\Sigma(S)$ of all entries of inverses of elements of $f(\Sigma)$ (the image of Σ under f). Σ is called multiplicative if $I \in \Sigma$ and if $A,B \in \Sigma$, then $\begin{pmatrix} A & C \\ 0 & B \end{pmatrix} \in \Sigma$, where C is any matrix of suitable size. The next result characterizes the Σ - rational closure in three ways. Denote by e_i the column vector with 1 in the i-th place and 0's elsewhere.

Theorem 0.1 (cf. thm.7.1.2 in [3]). Let R be a ring and Σ a multiplicative set of matrices over R. Given any Σ - inverting homomorphism $f: R \to S$, then the Σ - rational closure $R_\Sigma(S)$ is a subring of S containing im f, and for any $x \in S$ the following conditions are equivalent:

a) $x \in R_\Sigma(S)$;

b) x is a component of the solution u of a matrix equation

$$Au + a = 0 ,$$

where $A \in f(\sum)$ and a is a column vector with components in im f;

c) x is a component of the solution u of a matrix equation

$$Au - e_j = 0 ,$$

where $A \in f(\sum)$.

This theorem shows that every element of $R_\Sigma(S)$ can be obtained as some component u_i of a matrix equation $Au = a$. Here A is called the <u>denominator</u> of u_i, and A_i (the matrix obtained by replacing the i-th column of A by a) is called <u>numerator</u> of u_i. This definition has its justification in the next result which strongly resembles Cramer's Rule of the commutative case.

<u>Theorem 0.2</u> (cf. thm.7.1.3 in [3]). Let u_i be the i-th component of the solution of $Au = a$, where A is invertible. Then u_i is a $\left\{\begin{matrix}\text{left}\\\text{right}\end{matrix}\right\}\left\{\begin{matrix}\text{zero divisor}\\\text{unit}\end{matrix}\right\}$ if and only if the numerator of u_i has the same property in the matrix ring.

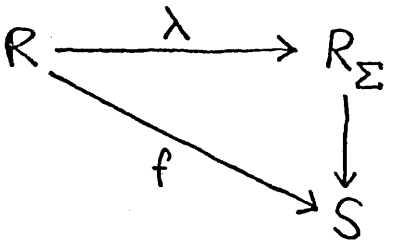
Next we recall the precise definition of the universal field of fractions of a ring R. Given a ring R, an <u>R - ring</u> refers to a ring L with a homomorphism from R to L. An <u>epic R - field</u> is an R - ring K which is a

skew field and such that K is the smallest field con= taining the image of R. We shall refer to epic R - fields simply as "R - fields" since no others occur in what follows. Note that R - fields need not exist for every ring R. If the canonical mapping $R \longrightarrow K$ is inject= ive, we call K a <u>field of fractions</u> of R. Given R - fields K,L, let f be an R - ring homomorphism from K_0 to L, where K_0 is an R - subring of K such that every element of K_0 not in ker f has an inverse in K_0. Such f is called a <u>specialization</u> between K and L. It follows that K_0 is a local ring with maximal ideal ker f; hence $K_0/\ker f$ is isomorphic to a subfield of L, namely im f. But since L is an R - field we find that im f = L. Hence any specialization of R - fields is surjective. Two specializations from K to L are considered equal if they agree on a subring K_0 of K and the common restriction to K_0 is again a specialization.

The R - fields and specializations are easily shown to form a category. An initial object in this category is called a <u>universal R - field</u>. Clearly if a universal R - field exists it will be unique up to isomorphism. Suppose R has a universal R - field U. Then R has a field of fractions if and only if U is a field of fractions; in that case U is called the <u>universal field of fractions</u> of R.

Let Σ be a set of square matrices over R as before. Let $\lambda : R \longrightarrow R_\Sigma$ be a ring homomorphism which is Σ - inverting and such that any Σ - inverting homomorphism

$f: R \longrightarrow S$ can be factored uniquely by λ (i.e. such that the diagram commutes). λ is called the <u>universal Σ - inverting homomorphism</u> and R is called the <u>universal Σ - inverting ring</u>.



<u>Theorem 0.3</u> (cf. thm.7.2.1 in [3]). Let R be any ring and Σ any set of square matrices over R. Then there is a universal Σ - inverting homomorphism $\lambda : R \longrightarrow R_\Sigma$, where R_Σ is unique up to isomorphism. λ is injective if and only if R can be embedded in a ring over which all the elements of Σ have inverses.

The next result shows that any R - field is deter= mined completely by the multiplicative set of matrices which become invertible.

<u>Theorem 0.4</u> (cf. thm.7.2.2 in [3]). Let R be any ring.

1. If Σ is a set of matrices such that the universal Σ - inverting ring R_Σ is a local ring, then the residue-class field of R_Σ is an R - field.
2. If K is an R - field and Σ is the set of all matrices over R whose images in K are invertible, then Σ is multiplicative and R_Σ is a local ring whose residue-class field is isomorphic to K.

Next we shall give the promised criterion for the existence of a universal field of fractions. To this

end we need some definitions. Let A,B be two matrices over a ring R. Then the diagonal sum of these matrices is defined to be

$$A \dot{+} B = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} .$$

Note that this sum is always defined. Given two n x n matrices $A = (a_{ij})$, $B = (b_{ij})$ such that $a_{ij} = b_{ij}$ for all $i = 2,3,\ldots,n$ and $j = 1,2,\ldots,n$, then the determinantal sum of A and B with respect to the first row exists; it is defined to be the matrix C whose first row is the sum of the first rows of A and B, and whose other rows agree with those of A and B. Similarly one defines the determinantal sum with respect to another row or column, if it exists. Let A,B be two matrices over R, not necessarily of the same size. A and B are said to be stably associated if there exist invertible matrices P,Q such that

$$\begin{pmatrix} A & 0 \\ 0 & I \end{pmatrix} = P \begin{pmatrix} B & 0 \\ 0 & I \end{pmatrix} Q$$

for unit matrices I of suitable size. An n x n matrix A over R is said to be full if it cannot be written as a product of matrices P,Q , where P is an n x r matrix and Q is r x n, and $r < n$. If this condition is not satis= fied, A is said to be non-full. If A is non-full, then its diagonal sum with any square matrix B is non-full, for if $A = PQ$, then $A + B = \begin{pmatrix} P & 0 \\ 0 & B \end{pmatrix}\begin{pmatrix} Q & 0 \\ 0 & I \end{pmatrix}$. However if A is full, then it does not follow that its diagonal sum

with another full matrix is again full. We are now in the position to state the key result referred to above.

Theorem 0.5 (cf. thm.7.6.4 in [3]). A ring R has a universal field of fractions over which every full matrix can be inverted if and only if

1. $1 \neq 0$ and the diagonal sum of any full matrices is full;
2. the determinantal sum of any non-full matrices, whenever defined, is non-full.

From this follows

Theorem 0.6 (cf. thms.7.6.5&6 in [3]). Let R be any ring in which the set Σ of all full matrices is multiplicative.

1. If $f: R \longrightarrow S$ is a Σ - inverting homomorphism (where $S \neq 0$), then f is injective and the Σ - rational closure is a field of fractions of R.
2. The universal Σ - inverting homomorphism $\lambda: R \longrightarrow R_\Sigma$ is an embedding of R into the universal field of fractions of R.

Thus we come to the result most relevant to us:

Theorem 0.7. $K_k\langle x\rangle$ has a universal field of fractions, obtained as the universal ring inverting all full matrices.

Without going into any further details we just mention that the proof of this theorem rests on the fact

that $K_k\langle x\rangle$ is a free ideal ring ("fir" for short).

We shall denote the universal field of fractions of $K_k\langle x\rangle$ by $K_k(x)$.

Early in chapter 1 we shall use the following

Theorem 0.8 (cf. p.152,202 in [4]). Let K be a skew field with centre k and let $A = A(x)$ be a square matrix over $K_k\langle x\rangle$. Then A is stably associated to $Bx + C$, where B,C are square matrices over K.

The proof is essentially the process of "linearization by enlargement". To elucidate this process we suppose that the (n,n) entry of an n x n matrix has the form $f + ab$. We enlarge the matrix by taking its diagonal sum with a 1 x 1 unit matrix and then apply a series of elementary operations, as follows:

$$f + ab \longrightarrow \begin{vmatrix} f + ab & 0 \\ 0 & 1 \end{vmatrix} \rightarrow \begin{vmatrix} f + ab & a \\ 0 & 1 \end{vmatrix} \rightarrow \begin{vmatrix} f & a \\ -b & 1 \end{vmatrix} .$$

It is clear that this amounts to stable association between the original matrix A and its enlarged form A'. By repeated application we can enlarge A to the form $A' = A_0 + A_1x$ as required.

The linear matrix $A_0 + A_1x$ thus obtained is called a companion matrix for A(x). Of course A_0 and A_1 are not unique. We note the following fairly obvious

Lemma 0.9. If a matrix A(x) over $K_k\langle x\rangle$ is invertible, or full, then any companion matrix of A(x) has the same property.

Let K be a skew field and let A be a square matrix over K. A singular eigenvalue of A is an element $a \in K$ such that $A - aI$ is singular. It is not known whether every square matrix has a singular eigenvalue (in some extension of K). However this question forms part of a general conjecture quoted at the beginning of chapter 1 and which entails a positive answer, as shown by Cohn in [4], p.204.

An element $a \in K$ is called a right eigenvalue of A if there is a non-zero column vector u, the eigenvector corresponding to a, such that

$$Au = ua \quad .$$

Similarly a left eigenvalue is an element $b \in K$ such that for a row vector v we have $vA = bv$. It is not difficult to see that left, right and singular eigenvalues in the centre of K coincide. Generally however there seems to be little connection between left and right eigenvalues on the one hand and singular eigenvalues on the other. It can be shown that a square matrix A over K always has a right (and left) eigenvalue in a suitable extension of K. One consequence of this fact is the following

Theorem 0.10 (cf. thm.8.4.1 in [4]). Let K be a skew field, then any equation

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0 \quad (a_i \in K) \qquad (1)$$

has a solution in some extension of K.

The proof rests on the fact that any companion matrix

of this equation (considered as 1 x 1 matrix over $K_k\langle x\rangle$) has a right eigenvalue c in some extension of K. This c is easily seen to satisfy (1).

There is one other result on a particular type of equation (over K) which we shall need:

Theorem 0.11 (cf. thm.8.4.4 in [4]). Let K be a skew field which is a k-algebra, and consider the equation

$$ax - xb = c \quad (a,b,c \in K). \qquad (2)$$

1. If a,b are both transcendental over k, (2) has infinitely many solutions in a suitable extension of K.
2. If one of a,b is transcendental over k and the other algebraic, then (2) has a unique solution in K or any extension of K.
3. If a,b are both algebraic over k but with different minimal equations over k, then (2) has a unique solution in K or indeed in any extension of K.
4. If a,b have the same minimal polynomial f over the centre k of K, then (2) has a solution in K (or in any extension of K) if and only if either $c = 0$, or $(t - cbc^{-1})(t - a)$ divides f in $K[t]$.

We shall in fact only make use of parts 3 and 4. The condition in part 4 becomes clearer with the next

Theorem 0.12 (cf. thm.8.5.2 in [4]). Let K be a skew field with centre k. Two algebraic elements $a,b \in K$ are conjugate

in K (i.e. $cac^{-1} = b$ for $c \in K$, $c \neq 0$) if and only if a and b satisfy the same minimal polynomial over k.

From this we can deduce another useful result, i.e.

Theorem 0.13 (cf. thm.8.5.4 in [4]). In a non - commutative field K, every element is contained in an infinite commutative subfield.

In particular this means that the centralizer of any element of K is infinite.

It will be necessary to have a non-commutative analogue to commutative algebraically closed fields. This is problematic since not all properties of commutative algebraically closed fields can be carried over into the skew case. For instance over a commutative field every equation has a solution in some extension and in the algebraic closure of that field in particular. As theorem 0.11, part 4, shows this need not be true in general. So what we shall define is a closure condition on a (skew) field K to the effect that if a system of equations over K has a solution in some extension of K, then it has already a solution in K itself. More formally,

Definition : Any sentence of the form

$$\exists\, a_1, \ldots, a_n \; P(a_1, \ldots, a_n) \quad ,$$

where P is an expression obtained from equations by

negation, conjunction and disjunction is called an existential sentence. By an existentially closed field, EC - field for short, we understand a field K such that any consistent existential sentence (i.e. one which holds in some field extension of K) already holds in K.

If K has centre k, then k is existentially closed if and only if k is algebraically closed. But if K is existentially closed it does not follow that k is algebraically closed. We have an embedding theorem as in the commutative case:

Theorem 0.14 (cf. thm.6.2.2 in [4]). Let K be any (skew) field, then there exists an EC - field L containing K, in which every finite consistent set of equations over K has a solution.

Note however that L in this theorem will not be unique in any way, even when assumed minimal over K. It is therefore not possible to speak of "the existential closure" of a skew field.

This concludes the preliminary chapter. Any other non-original results that we shall use will be recalled (with appropriate references) in the context of the work that follows.

1. TAME AUTOMORPHISMS; THEIR REPRESENTATIONS AND FIXED POINTS

Introduction

Throughout this chapter K will denote a skew field with centre k. Let G_0 be the set of all automorphisms of $K_k(x)$ over K (i.e. which keep K fixed). G_0 clearly forms a group.

In the commutative case, i.e. when K = k, each element of G_0 has the form of a linear fractional transformation

$$\alpha : x \mapsto \frac{ax + b}{cx + d} \quad , \qquad (1)$$

where $a,b,c,d \in k$ are unique up to a common factor and $ad - bc \neq 0$. Every such automorphism can be represented by a matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

which is unique up to a non-zero constant of k and which in turn determines α uniquely. Furthermore it is not difficult to see that every α of finite order n (such that the characteristic of k does not divide n) has exactly two fixed points in an appropriate extension of K(= k), for instance in the algebraic closure, and that with the help of these fixed points α can be put into the normal form $x \mapsto \omega x$, where ω is a primitive n-th

root of 1 (in terms of A this amounts to diagonalization).

The aim of this chapter is to generalize these results as far as possible to the non-commutative case, i.e. when $K \neq k$.

We encounter a major stumbling block virtually before the beginning because in the skew case it is not clear whether every element of G_0 is in fact a linear fractional transformation, i.e. of the form $\alpha : x \longmapsto (ax + b)(cx + d)^{-1}$ as in the commutative case. A distinction must therefore be made between wild and tame automorphisms (the latter being of form α), although the existence of the former is uncertain.

After a brief remark on wild automorphisms we shall turn to tame automorphisms exclusively. Benz showed in [2] that these form a group. Giving a new proof we show in addition that it is precisely the tame automorphisms which are representable as 2 x 2 matrices which are unique up to a central multiple - as in the commutative case. The main result of chapter 1 will tell us that every tame automorphism whose order is not divisible by the characteristic of K has either two or else infinitely many fixed points (in some extension of K, e.g. in some existentially closed field containg K). This will mean that all the normalization results mentioned above for the commutative case can be carried over to the non-commutative case.

a) On Wild and Tame Automorphisms of $K_k(x)$ over K

Let K be a skew field with centre k and let G_0 be the group of all automorphisms of $K_k(x)$ over K. Denote by G the subset of G_0 consisting of all transformations of the form

$$\alpha : x \longmapsto (ax + b)(cx + d)^{-1} \quad , \qquad (2)$$

where $a,b,c,d \in K$ are such that the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is invertible.

The elements of G are called tame automorphisms, all others correspondingly wild automorphisms. It is not known whether wild automorphisms exist at all, i.e. whether G is a proper subset of G_0.

In the special case where the centre k of K is algebraically closed we can describe the wild automorphisms (if any exist) more explicitly if the eigenvalue conjecture by P. M. Cohn ([4], p.204) has an affirmative solution.

The conjecture says the following: Let K be a field which is a k-algebra and assume that k is algebraically closed in K. Then every square matrix A over K has a non-zero singular eigenvalue in some extension of K unless A is conjugate over k to a triangular matrix.

If this were shown to be true, then if wild automorphisms exist at all of $K_k(x)$ over K, they will have to be conjugate to

$$x \longmapsto a + b_1 x b_2 + c_1 x c_2 + \cdots \qquad (a,b_i,c_i,\ldots \in K) \qquad (3)$$

To see this let α be an automorphism of $K_k(x)$ over K. Clearly $\alpha(x)$ will generate $K_k(x)$. We claim that $\alpha(x)$ is conjugate to some $u_1 \in K_k\langle x\rangle$ (necessarily also a generator of $K_k(x)$), and that $x \in K_k\langle u_1\rangle$. If this holds, then for polynomials $f, g \in K_k\langle x\rangle$ we have $f(u_1) = x$ and $g(x) = u_1$, i.e. $f(g(x)) = x$. But if $w = \deg f$, $v = \deg g$, then $vw = 1$, so $v = w = 1$. Hence f and g have form as indicated on the right hand side of (3) and α is as in (3). Note that if it turned out that there is only one summand of degree 1 in (3) we would have a tame automor= phism. The conjecture does not therefore entail the existence of wild automorphisms, it just limits the form they might take.

To prove the claim we note that u_1 (like any other element of $K_k(x)$) can be obtained as the first component of the solution to a matrix equation $Au = a$, where A (the denominator) is a full square matrix over $K_k\langle x\rangle$. Using theorem 4.4 ("On Universal Denominators") from a paper of P. M. Cohn ("The Universal Field of Fractions of a Semifir", to appear) we can say even more about A. The relevant part of the theorem may be restated as follows:

Given any $p \in K_k(x)$, there is a representation for p with a denominator which is non-singular over any $K_k\langle x\rangle$-field in which p is defined. (In fact the theorem holds for more general rings than $K_k\langle x\rangle$).

Clearly K is a $K_k\langle x\rangle$-field, with homomorphism e.g. $p(x) \longmapsto p(0)$ from $K_k\langle x\rangle$ to K.

Returning to u_1 we note that u_1 may not be defined at a certain value (the value being the image of the point "at infinity" under α). Without loss of generality we may take that value to be the point "at infinity" itself, for if the value is finite, say $x = d$, we change variables by putting $y = (x - d)^{-1}$.

So u_1 is defined at all finite values and according to the theorem above we may take A to be invertible for any finite value of x in K, and in particular for $x = 0$.

We want to show that A is in fact invertible in $K_k\langle x\rangle$ for then $u = A^{-1}a$, giving the claim. We know A is stably associated to $A_0 + xA_1$, where $A_0, A_1 \in K_n$ for some n by theorem 0.8. But A(0) is non-singular, therefore so is A_0, by putting $x = 0$ in $A_0 + xA_1$. Multiplying out by A_0^{-1} gives us A in the form $A = I - xA_1$ without loss of generality since multiplication by A_0^{-1} obviously does not affect the possible invertibility of A. By hypothesis $I - xA_1$ is non-singular for any finite $x \in K$. This is equivalent to saying $Ix - A_1$ is non-singular for any non-zero $x \in K$, i.e. A_1 does not have a singular eigenvalue in any extension of K. By the conjecture A_1 is triangularizable over k, say $P^{-1}A_1P = T$, where P has its entries in k. If T has a non-zero diagonal element t, then $I - Tt^{-1}$ is singular, contrary to the hypothesis. So the diagonal entries of T are all zero. Hence $P^{-1}(I - A_1x)P = I - Tx$ and A is (conjugate to) a triangular matrix with 1's on the main diagonal. Therefore A is invertible in $K_k\langle x\rangle$. Thus $u_1 \in K_k\langle x\rangle$ and

by symmetry $x \in K_k\langle u_1 \rangle$, giving the claim.

In what follows we shall consider tame automorphisms only. For the remainder of this chapter we shall not impose any conditions on K or on its centre k.

Let α be a tame automorphism as given in (2). Then we obtain a representation by mapping α to $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ or rather, by mapping α to the set of central multiples of this matrix:

To see this we take another automorphism $\beta : x \longmapsto (Ax + B)(Cx + D)^{-1}$, where $A,B,C,D \in K$, and we show that $\alpha\beta$ is represented by the matrix product $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} A & B \\ C & D \end{pmatrix}$:

$\alpha\beta$ maps x to

$$(a(Ax + B)(Cx + D)^{-1} + b)(c(Ax + B)(Cx + D)^{-1} + d)^{-1}$$
$$= ((aAx + aB) + (bCx + bD))((cAx + cB) + (dCx + dD))^{-1}$$
$$= ((aA + bC)x + (aB + bD))((cA + dC)x + (cB + dD))^{-1}$$

which is represented by $\begin{pmatrix} aA + bC & aB + bD \\ cA + dC & cB + dD \end{pmatrix}$ as desired.

We also need to show the uniqueness of this representation, i.e. the uniqueness up to a central factor. To this end we note the following

Lemma 1.1. Every tame automorphism α (as in (2)) can be written in one of the forms

$$\varphi : x \longmapsto a'xb' + c' \quad , \quad a',b' \neq 0$$
$$\psi : x \longmapsto a''(x - p)^{-1}b'' + q \quad , \quad a'',b'' \neq 0$$

according as $c = 0$ or $c \neq 0$.

Conversely any automrphism of the form φ or ψ is tame.

Proof : If $\alpha : x \longmapsto (ax + b)(cx + d)^{-1}$ and $c = 0$, then α is of form φ with $b' = d^{-1}$, $a' = a$ and $c' = bd^{-1}$. Conversely any φ is obviously always of form α with $c = 0$. If $c \neq 0$, then α is of form ψ with $a'' = b - ac^{-1}d$, $b'' = c^{-1}$, $p = -c^{-1}d$, $q = ac^{-1}$. We note that $a'' \neq 0$ since $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is non-singular. Conversely, given ψ, then this can be brought into the form of α by taking $a = qb''^{-1}$, $b = a'' - qb''^{-1}p$, $c = b''^{-1}$, $d = b''^{-1}p$.

Now we show the uniqueness of the representation by showing the uniqueness of the maps φ and ψ, i.e. by determining how far the constants of φ and ψ can be changed without altering the mappings themselves. We begin with ψ:

Let $\quad a(x - p)^{-1}b + q = A(x - P)^{-1}B + Q$,

where $a,b,A,B \neq 0$. Then

$(b^{-1}xa^{-1} - b^{-1}pa^{-1})^{-1} + q = (B^{-1}xA^{-1} - B^{-1}PA^{-1})^{-1} + Q$ so

$$(B^{-1}xA^{-1} - B^{-1}PA^{-1}) + (b^{-1}xa^{-1} - b^{-1}pa^{-1})q(B^{-1}xA^{-1} - B^{-1}PA^{-1})$$
$$= (b^{-1}xa^{-1} - b^{-1}pa^{-1}) + (b^{-1}xa^{-1} - b^{-1}pa^{-1})Q(B^{-1}xA^{-1} - B^{-1}PA^{-1}).$$

Compare the terms of degree 2 in this :

$$b^{-1}xa^{-1}qB^{-1}xA^{-1} = b^{-1}xa^{-1}QB^{-1}xA^{-1} .$$

This shows that $Q = q$, leaving us with

$$B^{-1}xA^{-1} - B^{-1}PA^{-1} = b^{-1}xa^{-1} - b^{-1}pa^{-1} .$$

Compare the terms of degree 1 in this :

$$B^{-1}xA^{-1} = b^{-1}xa^{-1} \quad .$$

Let $A^{-1} = a^{-1}\lambda$, $B^{-1} = \mu b^{-1}$ for some $\lambda, \mu \in K$. Then

$$a^{-1}(x - \lambda x \mu)b^{-1} = 0 \ ,$$

so $x = \lambda x \mu$ and hence $\lambda^{-1} = \mu \in k$. Substitute this in

$$B^{-1}PA^{-1} - b^{-1}pa^{-1} = 0$$

for A and B, then

$$b^{-1}\lambda \, P \, \lambda^{-1}a^{-1} - b^{-1}pa^{-1} = 0$$

hence $P = p$.

Similarly one shows for φ that the constants cannot be changed without affecting the transformation except where a',b' are simultaneously replaced by $a'\lambda$, $\lambda^{-1}b'$ respectively, where $\lambda \in k$.

The matrix for ψ: $x \mapsto a(x - p)^{-1}b + q$ is therefore

$$\begin{pmatrix} q(b\lambda^{-1})^{-1} & a - q(b\lambda^{-1})^{-1}p \\ (b\lambda^{-1})^{-1} & -(b\lambda^{-1})^{-1}p \end{pmatrix} = \lambda \begin{pmatrix} qb^{-1} & a - qb^{-1}p \\ b^{-1} & -b^{-1}p \end{pmatrix}$$

and the matrix for φ: $x \mapsto axb + c$ is similarly

$$\begin{pmatrix} a\lambda & q(b\lambda^{-1})^{-1} \\ 0 & (b\lambda^{-1})^{-1} \end{pmatrix} = \lambda \begin{pmatrix} a & qb^{-1} \\ 0 & b^{-1} \end{pmatrix}$$

This shows that the representing matrix of ψ and φ, and hence of α is unique up to a central scalar multiple.

Let $GL_2(K)$ be the group of invertible 2 x 2 matrices over K. Let Z be the centre of $GL_2(K)$. Z is in fact the group of central scalar matrices in $GL_2(K)$. Define $PGL_2(K)$, the projective group of invertible 2 x 2 matrices by

$$PGL_2(K) = GL_2(K)/Z \ .$$

Then we have proved

Theorem 1.2. Let G_0 be the group of all automorphisms of $K_k(x)$ over K and let G be the subset of all tame automorphisms. Then the bijection between G and $PGL_2(K)$ is a homomorphism from the latter into G_0.
Hence G is a group.

This last result can also be found in [2]; however the argument presented here seems both simpler and more illuminating.

Note: 1) Similarly the transformation $x \longmapsto (xa + b)(xc + d)^{-1}$ has a matrix representation $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. But here if α has matrix A and β has matrix B, then $\alpha\beta$ would have representing matrix BA. The isomorphism between $PGL_2(K)$ and G in theorem 1.2 would become an antiisomorphism. We shall therefore choose to write our transformations as before, x having its coefficients on the left.

2) Strictly speaking the transformations (2) are not represented by one matrix, but rather by an equivalence

class of matrices, namely those matrices differing by a central scalar factor. "matrix" shall therefore mean "class of matrices" as described.

b) Normal Forms

The object of what follows is to find out how many fixed points the automorphism

$$\alpha : x \longmapsto (ax + b)(cx + d)^{-1} \qquad (2)$$

has when it is of finite order.

α is said to have a fixed point (in K') if it has a fixed point in $K' \cup \{\infty\}$, where K' is some extension field of K. In other words, if x_0 lies on the projective line of some extension K' of K, and x_0 satisfies

$$x_0 = (ax_0 + b)(cx_0 + d)^{-1} \quad ;$$

then x_0 is called a fixed point of α (sometimes we shall add: in K'). More accurately, x_0 is a fixed point of the action of α on the projective line of K'.

Lemma 1.3. α has the same number of fixed points as any of its conjugates.

Proof : If $\alpha x_0 = x_0$ and $\tau \in PGL_2(K)$, then $\tau \alpha \tau^{-1} \tau x_0 = \tau x_0$. If $x_0 \neq x_1$, then $\tau x_0 \neq \tau x_1$ since τ is an automorphism.

It follows that in order to show the existence of a fixed point for α we only need to show the existence of

a fixed point for an appropriately chosen conjugate of α. We remark once more that the point "at infinity" will also be eligible as fixed point, since we can always change variables, e.g. $y = x^{-1}$, to transform it to a finite fixed point and vice versa.

Lemma 1.4. Let α be as in (2), not necessarily of finite order. Then α has at least one fixed point (in some extension K' of K).

Proof : We may assume that $c \neq 0$ in α for otherwise α is of form φ which has a fixed point at infinity. But if $c \neq 0$, then α is of form ψ: $x \longmapsto a(x - p)^{-1}b + q$. Put $\tau_1 x = x - q$ and $\tau_2 x = xb$ and $\tau = \tau_1 \tau_2$. Note that τ_1, τ_2 and therefore τ are tame automorphisms, hence in $PGL_2(K)$. Then $\tau^{-1}\psi\tau$ is a map of the form

$$\psi' : x \longmapsto A(x - P)^{-1} \quad ,$$

where $A = ab^{-1}$, $P = b^{-1}(q - p)$. But ψ' has a fixed point x_0 if and only if $x_0 = A(x_0 - P)^{-1}$. Such x_0 is known to exist since the equation $x^2 - xP - A = 0$ has a solution in some extension K' of K by theorem 0.10.

It will be useful to fix some terminology: When we mean the matrix (class) representing α we shall simply refer to "the matrix of α". Conversely if $A \in PGL_2(K)$ is given α will sometimes be called the "map of A". When a matrix is conjugate to a triangular matrix we shall say it is triangularizable. Similarly when it is

conjugate to a diagonal matrix we say it is diagonalizable.

The next theorem will show why we can use the terms "fixed point" (of α) and "eigenvector" (of A, the matrix of α) interchangeably. In this theorem we do not need α to be of finite order. However we shall see later (in theorem 1.13) that for α of finite order there will always be at least two fixed points (over a sufficiently large field of appropriate characteristic).

Theorem 1.5. Let α be as in (2) and let $A \in PGL_2(K)$ be the matrix of α.

1. Let $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ be an eigenvector of A, corresponding to a right eigenvalue. If $x_2 \neq 0$, then $x_1 x_2^{-1}$ is a fixed point of α, and if $x_2 = 0$, then α has a fixed point at infinity.
2. Conversely, if x_0 is a finite fixed point of α, and $x_1, x_2 \in K$ are such that $x_0 = x_1 x_2^{-1}$, then $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ is an eigenvector of A corresponding to a right eigenvalue; if α has a fixed point at infinity, then $\begin{pmatrix} z \\ 0 \end{pmatrix}$ is an eigenvector of A, corresponding to right eigenvalue $z^{-1}az$, where z is an arbitrary non-zero element of K. The eigenvector obtained from a fixed point is thus unique up to right multiples.
3. Eigenvectors of A (with right eigenvalues) which are linearly dependent on the left yield conjugate fixed points of α, whereas eigenvectors linearly dependent

on the right correspond to the same fixed point.

Proof : 1. Suppose A has right eigenvalue λ, i.e.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \lambda \quad . \qquad (4)$$

Then $ax_1 + bx_2 = x_1\lambda$ and $cx_1 + dx_2 = x_2\lambda$.

If $x_2 \neq 0$, then

$(ax_1 + bx_2)(cx_1 + dx_2)^{-1} = (x_1\lambda)(x_2\lambda)^{-1} = x_1x_2^{-1}$, and

$$\begin{aligned}(ax_1 + bx_2)(cx_1 + dx_2)^{-1} &= (ax_1 + bx_2)x_2^{-1}x_2(cx_1 + dx_2)^{-1} \\ &= (ax_1x_2^{-1} + b)(cx_1x_2^{-1} + d)^{-1},\end{aligned}$$

so $x_1x_2^{-1}$ is a fixed point of α as claimed. When $x_2 = 0$, then $c = 0$ and the point at infinity is clearly a fixed point of α.

2. If x_0 is finite and $(ax_0 + b)(cx_0 + d)^{-1} = x_0$, then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_0 \\ 1 \end{pmatrix} = \begin{pmatrix} x_0 \\ 1 \end{pmatrix} (cx_0 + d) \quad .$$

But if $x_0 = x_1x_2^{-1}$, then $\begin{pmatrix} x_0 \\ 1 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} x_2^{-1}$ and so we find that (4) holds with $\lambda = x_2^{-1}(cx_1x_2^{-1} + d)x_2$.

If x_0 is the point at infinity, then $c = 0$, so

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} z \\ 0 \end{pmatrix} = \begin{pmatrix} z \\ 0 \end{pmatrix} z^{-1}az \quad ,$$

for any $z \neq 0$ in K.

Note that if $x_0 = x_1x_2^{-1}$, then

$x_0 = x_1 e e^{-1} x_2^{-1} = x_1 e (x_2 e)^{-1}$, so x_0 yields eigenvector $\begin{pmatrix} x_1 e \\ x_2 e \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} e$, where e is an arbitrary non-zero constant in K; in other words the eigenvector is unique up to right multiples.

3. Suppose two eigenvectors (with right eigenvalues) are linearly dependent on the left. Then their lower entries are either both zero or both non-zero. If they are zero, then by part 2. both eigenvectors correspond to the fixed point at infinity. We may assume therefore that the eigenvectors are $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ and $\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$, where x_2, y_2 are non-zero. We may take x_1, y_1 to be non-zero similarly. Then for some $r,s \neq 0$ $r\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + s\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = 0$, so

i) $rx_1 + sy_1 = 0$ and ii) $rx_2 + sy_2 = 0$. Since $x_2 \neq 0$ we have by ii) $r = -sy_2 x_2^{-1}$. Substitute this for r in i): $-sy_2 x_2^{-1} x_1 + sy_1 = 0$. So since $s \neq 0$, $x_2^{-1} x_1 = y_2^{-1} y_1$. But then $x_1^{-1} x_1 x_2^{-1} x_1 = y_1^{-1} y_1 y_2^{-1} y_1$ and hence $(x_1 y_1^{-1})^{-1} x_1 x_2^{-1} (x_1 y_1^{-1}) = y_1 y_2^{-1}$. So $x_1 x_2^{-1}$ and $y_1 y_2^{-1}$ are conjugate and by part 2. this means that the fixed points yielded by the eigenvectors are conjugate.

If two eigenvectors (with right eigenvalues) are linearly dependent on the right, then we may assume as before that their entries are all non-zero. Then for some $r,s \neq 0$ $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} r + \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} s = 0$ and i) $x_1 r + y_1 s = 0$, ii) $x_2 r + y_2 s = 0$. As before we replace r by $-x_2^{-1} y_2 s$ in i) and find

$x_1x_2^{-1} = y_1y_2^{-1}$, i.e. that the fixed points yielded by both eigenvectors are in fact identical.

The converse of part 3 of this theorem does not in general hold, i.e. if x_0, y_0 are conjugate fixed points of α it does not follow that all the eigenvectors obtained from x_0, y_0 are linearly dependent on the left. What we can say however is the following

Corollary 1.6 : x_0, y_0 are conjugate fixed points of α if and only if there exist two eigenvectors $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$, $\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ for A which are linearly dependent on the left and such that $x_1x_2^{-1} = x_0$ and $y_1y_2^{-1} = y_0$.

Proof : If $y_0 = cx_0c^{-1}$, then we take x_0 to have eigenvector $\begin{pmatrix} x_0e \\ e \end{pmatrix}$ and y_0 to have eigenvector $\begin{pmatrix} cx_0e \\ ce \end{pmatrix}$, where e is an arbitrary non-zero constant in K. Then $c\begin{pmatrix} xe \\ e \end{pmatrix} - \begin{pmatrix} cxe \\ ce \end{pmatrix} = 0$ shows the linear dependence on the left of these particular eigenvectors derived from the fixed points.
The converse is part 3 of theorem 1.5.

We observe that if we choose different constants e in the vectors for x_0 and y_0, then we cannot establish linear dependence on the left of these eigenvectors.

A noteworthy feature of part 3 of theorem 1.5 is the fact that linear dependence on the right and on the left are not symmetrical properties; linear dependence on the

right of eigenvectors with right eigenvalues turns out to be a stronger condition than linear dependence on the left (though the former property does not quite imply the latter). The reason for this lies in the particular representation we chose for α. For instance if $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ were to represent α in the form $x \longmapsto (cx + d)^{-1}(ax + b)$, then part 1 would have to be modified to show that an eigenvector (with right eigenvalue) of form $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ yields a fixed point $x_2^{-1}x_1$. Then the argument for part 3 would make linear dependence on the left the stronger property.

The following lemmas show how fixed points are used to achieve a normal form for α and its matrix.

Lemma 1.7. The matrix A of α is triangularizable (in some extension of K). Equivalently, α is always conjugate to a map of form φ.

Proof : By lemma 1.4 α has a fixed point, so by theorem 1.5 A has a column eigenvector, u say, corresponding to a right eigenvalue, z say. Then $Au = uz$. Let v be a column vector linearly independent of u on the right. Then for some $t, y \in K$, $Av = ut + vy$. Now take $P = (u\ v)$, then P is invertible and

$$P^{-1}AP = \begin{pmatrix} z & t \\ 0 & y \end{pmatrix}.$$

$P^{-1}AP$ has map $x \mapsto zxy^{-1} + ty$, i.e. a map of form φ.

Proposition 1.8. Suppose α has two inconjugate fixed points. Then the matrix of α is diagonalizable.

Proof : By lemma 1.6 α is conjugate to a map of form φ. Since α has two inconjugate fixed points, φ must have a finite fixed point (the other fixed point of φ being at infinity). Let φ be the map $y = axb + c$ and denote the finite fixed point by x_0. Then $x_0 = ax_0b + c$. Change variables, $y = y' + x_0$ and $x = x' + x_0$. Then $y' + x_0 = a(x' + x)b + c$ $= ax'b + ax_0b + c = ax'b + x_0$. Hence $y' = ax'b$ which has matrix $\begin{pmatrix} a & o \\ 0 & b^{-1} \end{pmatrix}$.

An alternative proof runs along the lines of lemma 1.6: Since the fixed points of α are inconjugate they yield two right linearly independent column eigenvectors for the matrix A of α. These are used in place of u and v in the proof of lemma 1.6. $P^{-1}AP$ will then be diagonal.

Note that diagonalizing A amounts to transforming the fixed points x_0, x_1 of α to 0 and ∞ respectively, and indeed one could also prove proposition 1.8 by replacing x in α by $(x - x_0)(x - x_1)^{-1}$ and calculating the resulting form of this conjugate of α.

If we have a set of matrices of $PGL_2(K)$ whose maps share the same two fixed points, then the diagonalization procedure described above can be applied to all the matrices in the set simultaneously. In particular we have

Corollary 1.9. Let G be a group in $PGL_2(K)$ all elements of which have at least two inconjugate fixed points in common. Then G is conjugate to a group in $PGL_2(K)$ all elements of which are diagonal.

If we were able to prove the existence of a second fixed point for every matrix in $PGL_2(K)$ of finite order, then we would have shown that every such matrix is diagonalizable, just as in the commutative case. To this end we note that we have a normal form for triangular matrices:

Lemma 1.10. In $PGL_2(K)$ any (non-unit) upper triangular matrix is conjugate to an upper triangular matrix with 1 as its (1,2) entry.
Equivalently any (non-unit) map $\varphi: x \mapsto axb^{-1} + q$ is conjugate to a map

$$\varphi': x \mapsto axb^{-1} + b^{-1} . \qquad (5)$$

Proof : Let $A = \begin{pmatrix} a & c \\ 0 & b \end{pmatrix}$, where $c \neq 0$, then A has map $y = axb^{-1} + cb^{-1}$. Change variables: $y = cy'$, $x = cx'$; then $y' = c^{-1}acx'b^{-1} + b^{-1}$ which has matrix $\begin{pmatrix} c^{-1}ac & 1 \\ 0 & b \end{pmatrix}$.
If $c = 0$, i.e. A is diagonal, choose an element $p \in K$ such that $ap - pb \neq 0$. This will always be possible unless $a = b \in k$, which is ruled out since A is not the unit matrix. Put $d = ap - pb$. Then noting that

$$\begin{pmatrix} d & p \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} d^{-1} & -d^{-1}p \\ 0 & 1 \end{pmatrix}$$, we find

$$\begin{pmatrix} d & p \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \begin{pmatrix} d & p \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} d^{-1}ad & 1 \\ 0 & b \end{pmatrix} .$$

c) The Existence of the Second Fixed Point

By lemmas 1.3, 1.4, 1.7 and 1.10 we know that every α as in (2) is conjugate to a map of the form (5). Throughout the remainder of this chapter α, or φ as in (5), will be assumed of finite order. Moreover we shall assume that the characteristic of our field K does not divide the order of α, i.e. if $\alpha^n = I$, then char $K \nmid n$.

The following lemma describes the fact that φ is of finite order in terms of its constants.

Lemma 1.11. $\varphi: x \mapsto axb^{-1} + c$ is of finite order n if and only if $a^n = b^n = \lambda \in k$ and $\sum_{i=0}^{n-1} a^i c b^{-i} = 0$.

Proof : If $\varphi x = axb^{-1} + c$, then we claim that

$$\varphi^n x = a^n x b^{-n} + \sum_{i=0}^{n-1} a^i c b^{-i} .$$

If this holds, then $\varphi^n x = x$ if and only if $a^n = b^n = \lambda \in k$ and $\sum_{i=0}^{n-1} a^i c b^{-i} = 0$.

We show the claim by induction on n. For n = 1 it is obvious. Assume the claim holds for n - 1. Then we have

$$\varphi^{n-1} x = a^{n-1} x b^{-(n-1)} + \sum_{i=0}^{n-2} a^i c b^{-i} .$$

But then $\varphi^n x = a^{n-1}(axb^{-1} + c)b^{-(n-1)} + \sum_{i=0}^{n-2} a^i c b^{-i}$

$$= a^n x b^{-n} + a^{n-1} c b^{-(n-1)} + \sum_{i=0}^{n-2} a^i c b^{-i}$$

$$= a^n x b^{-n} + \sum_{i=0}^{n-1} a^i c b^{-i} ,$$

proving the claim.

It follows that $\varphi: x \mapsto axb^{-1} + b^{-1}$ will be of finite order n if and only if $a^n = b^n = \lambda \in k$ and $\sum_{i=0}^{n-1} a^i b^{-i} = 0$.

Now (5) will have a finite - the second - fixed point if $x_0 = ax_0b^{-1} + b^{-1}$ for some x_0, i.e. if

$$ax - xb = -1 \qquad (6)$$

has a solution in some extension of K. Since α is of finite order we know from lemma 1.11 that $a^n = b^n = \lambda \in k$, i.e. that a and b are algebraic over the centre k of K. We recall the relevant parts of theorem 0.11 :

Consider the equation

$$ax - xb = c \quad (a,b,c \in K) \qquad (7)$$

3. If a,b are algebraic over k, but a,b have different minimal equations over k, then (7) has a unique solution in K or any extension of K.
4. If a,b have the same minimal polynomial g over k, then (7) has a solution in K (or in any extension of K) if and only if either $c = 0$, or $(t - cbc^{-1})(t - a)$ divides g in $K[t]$, where $K[t]$ is the polynomial ring over K with central indeterminate t.

For our case (where $c = -1$) this means that if a and b

do not have the same minimal equation over k, a unique second fixed point exists for (5).

If a and b do have the same minimal equation over k we distinguish two cases :

1) The minimal equation of a (and b) is <u>not</u> $t^n - \lambda$, i.e. $t^n - \lambda$ is reducible over k ($\lambda \in k$).

Let $g = 0$ be the minimal equation of a and b over k. Then we have the following

<u>Lemma 1.12</u>. Assume the characteristic of K does not divide n. Then $(t - b)(t - a)$ divides g in $K[t]$ if and only if $(t - b)(t - a)$ divides $t^n - \lambda$ in $K[t]$.

<u>Proof</u> : If $(t - b)(t - a) \mid g$, then clearly $(t - b)(t - a) \mid t^n - \lambda$ since $t^n - \lambda = gh$ for some $h \in K[t]$, by definition of g.
Conversely assume $(t - b)(t - a) \mid t^n - \lambda$. Since the characteristic of K does not divide n we know that $t^n - \lambda$ must be separable. Moreover since $t^n - \lambda$ is reducible in $K[t]$ we have $t^n - \lambda = gh$, where g and h must be coprime. This means that there exist polynomials $u, v \in K[t]$ such that $gu + hv = 1$. It follows that $g^2u + ghv = g$. But by definition $g \in k[t]$, so

$$\begin{aligned} g^2 &= g(t - b)g_2 \\ &= (t - b)gg_2 \\ &= (t - b)(t - a)g_1g_2 \end{aligned}$$

for some $g_1, g_2 \in K[t]$. By hypothesis also $(t - b)(t - a) \mid gh$, therefore $(t - b)(t - a) \mid g$.

It is interesting to observe why the condition on the characteristic of K is necessary in lemma 1.12 : If char K | n, then $t^n - \lambda$ is no longer separable, for

$$t^n - \lambda = (t - b)(t^{n-1} + t^{n-2}b + \ldots + tb^{n-2} + b^{n-1}) \quad (8)$$

since t is a central variable. Put $f(t) = t^{n-1} + t^{n-2}b + \ldots + b^{n-1}$, then the equation $f(t) = 0$ now has the solution $t = b$. So $t - b$ is a factor of $f(t)$. Hence for some $h \in K[t]$, $t^n - \lambda = (t - b)^2 h(t)$ and lemma 1.12 need no longer be true.

With lemma 1.12 the treatment of case 1) becomes the same as that of case 2), i.e. we may assume without loss of generality that $t^n - \lambda$ is irreducible over k.

2) The minimal equation of a and b is $t^n - \lambda$. Then (6) has a solution if and only if $(t - b)(t - a)$ divides $t^n - \lambda$ in $K[t]$. But $t^n - \lambda = (t - b)f(t)$ as in (8). So by the division algorithm in $K[t]$ we know that

$$f(t) = (t - a)\, h(t) + f(a)$$

for some $h \in K[t]$. $f(a)$ is obtained by writing all coefficients of f on the right of t and then substituting a for t. But (6) was derived from (5) which is of finite order n. By lemma 1.11 this means that $\sum_{i=0}^{n-1} a^i b^{-i} = 0$, i.e. $f(a) = 0$. Hence $f(t) = (t - a)\, h(t)$, i.e. $f(t)$ is divisible on the left by $t - a$. By (8) therefore we

must have

$$t^n - \lambda = (t - b)(t - a)\, h(t) \qquad (9)$$

which shows that (6) has a solution and (5) has a second fixed point.

There is also a more direct way of showing that $(t - b)(t - a)$ divides $t^n - \lambda$ (and hence g in case 1)), which does not use the division algorithm of $K[t]$ and which gives h(t) of (9) explicitly : We show that

$$(t - b)(t - a)\left(\sum_{r=0}^{n-2} t^{n-r-2}\left(\sum_{i+j=r} a^i b^j\right)\right) = t^n - \lambda \qquad (10)$$

by evaluating the coefficients on the left hand side : First we note that $(t - b)(t - a) = t^2 + t(a + b) + ba$. Next we observe that the coefficient of t^n on the left hand side of (10) is 1. The term of degree $n - 1$ is $t^2 t^{n-3}(a + b) - t(a + b)t^{n-2}$ which vanishes. Then we evaluate the absolute term :

$$\begin{aligned} ba \sum_{i+j=n-2} a^i b^j &= b \sum_{i+j=n-2} a^{i+1} b^j + b^n - \lambda \\ &= b \sum_{i+j=n-1} a^i b^j - \lambda \\ &= -\lambda \qquad \text{by lemma 1.11.} \end{aligned}$$

Note that $\sum_{i=0}^{n-1} a^i b^{-i} = \sum_{i+j=n-1} a^i b^j$ in this.

Finally we find the coefficient of the general term of degree $n - r$, where $n - 2 \geq r > 0$. The general term is

$$t^2 t^{n-r-2} \sum_{i+j=r} a^i b^j - t(a+b)t^{n-(r-1)-2} \sum_{i+j=r-1} a^i b^j + bat^{n-(r-2)-2} \sum_{i+j=r-2} a^i b^j .$$

Thus the general coefficient of t^{n-r} is

$$\sum_{i+j=r} a^i b^j - a \sum_{i+j=r-1} a^i b^j - b \sum_{i+j=r-1} a^i b^j + ba \sum_{i+j=r-2} a^i b^j$$

which is easily seen to be identically zero. Thus we have proved

Theorem 1.13. Let α be an element of $PGL_2(K)$ of finite order n and assume that the characteristic of K does not divide n. Then α has at least two inconjugate fixed points in some extension of K.

The only remaining questions are now, when does α have more than two fixed points, and how many fixed points can α have? To answer this we need the following.

Definition : Let $A \in PGL_2(K)$ be such that $A \neq I$. We call A a quasiconjugation if it is conjugate to a scalar matrix.

The reason for this name becomes clearer when we consider the map of a quasiconjugation. It will be conjugate to a map of the form $x \mapsto axa^{-1}$ which itself acts as conjugation on $K \cup \{\infty\}$. We shall also call the map of A a quasiconjugation.

Thus we come to the main result of this chapter.

Theorem 1.14. Let α be a tame automorphism of $K_k(x)$ over K of finite order n and assume the characteristic of K does not divide n.

1. If α is not a quasiconjugation, then α has

precisely two fixed points in some extension of K and these will not be conjugate.

2. If α is a quasiconjugation, then α has infinitely many fixed points in some extension of K, amongst which there are at least two inconjugate fixed points.

Proof : By theorem 1.13 every tame automorphism of finite order has at least two inconjugate fixed points. We claim α has more than these two fixed points if and only if it is a quasiconjugation :
If α is a quasiconjugation, then by lemma 1.3 α has as many fixed points as the scalar matrix sI of which α is a conjugate ($s \in K - k$). But sI has map $x \mapsto sxs^{-1}$, so the fixed points are precisely those contained in the centralizer of s in $K \cup \infty$, $C(s) \cup \infty$. But C(s) is known to be infinite by theorem 0.13 (and when char K = 0 this is obvious anyway), showing one half of our claim. Since C(s) contains at least three inconjugate elements, i.e. 0,1,s, this also proves part 2 of the theorem. Conversely suppose α has other fixed points besides the two inconjugate ones α is known to have by theorem 1.13. We transform these inconjugate fixed points to 0 and ∞ to bring α into the form α': $x \mapsto axb^{-1}$ by proposition 1.8. Since α has more than two fixed points so does α' by lemma 1.3. A third fixed point for α' will have to be non-zero and finite. Denote this fixed point by p, then $p = apb^{-1}$, or $pbp^{-1} = a$. So the third fixed point

exists if and only if a and b are conjugate. To see that α' is in fact a quasiconjugation, change variables in $y = axp^{-1}ap$: $y = y'p$ and $x = x'p$. Then $y'p = ax'pp^{-1}ap$ and hence $y' = ax'a^{-1}$. This proves the claim and the theorem.

We note finally that the extension of K referred to in theorems 1.13 and 1.14 is in fact the skew field K' of lemma 1.4. In other words, given an extension K' of K in which we can find the first fixed point of α, then we can find the second fixed point in that same K' (assuming of course that K and K' have the right characteristic).

2. FINITE SUBGROUPS OF $PGL_2(K)$

Introduction

Whereas the previous chapter dealt with elements of $PGL_2(K)$ of finite order, in this chapter we shall be concerned with finite subgroups of $PGL_2(K)$. Ideally one would aim at a complete classification of these groups (as has been done for the complex numbers). But the problems arising appear to be very considerable and only a few results will be given - in section a) - for the general finite groups. A complete classification is attempted of those finite groups which do not contain any quasiconjugations, although even here we meet only with partial success. The classification is complete only when the centre k of K satisfies certain closure conditions, for instance algebraic closure. Here the classification uses a similar method as in the well known case of the complex numbers (section c)). Section b) deals with the main obstacle to the classification over a field K with general centre k : finite groups of diagonal (non-scalar) matrices in $PGL_2(K)$.

Throughout we shall assume that the characteristic of the skew field K does not divide the order of the group in question. K will be assumed large enough to contain the two fixed points of any non-quasiconjugation of finite order that occurs in our discussion.

a) Groups with Quasiconjugations

Although a quasiconjugation is defined to be a matrix (class) conjugate to a scalar matrix (class), it does not follow that a diagonal quasiconjugation is a scalar matrix.

Lemma 2.1. Let $A \in PGL_2(K)$ be diagonal. Then A has conjugate diagonal entries if and only if A is a quasi= conjugation.

Proof : Suppose the diagonal entries of A are conjugate, i.e. $A = \begin{pmatrix} a & 0 \\ 0 & c^{-1}ac \end{pmatrix}$. Then

$A = \begin{pmatrix} 1 & 0 \\ 0 & c^{-1} \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & c \end{pmatrix}$, so A is a quasiconjugation.

Conversely suppose A is a diagonal quasiconjugation. Then for some invertible $B \in PGL_2(K)$, $B^{-1}AB$ is a scalar matrix aI. Put $A = \begin{pmatrix} b & 0 \\ 0 & c \end{pmatrix}$, $B = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, then

$$\begin{pmatrix} b & 0 \\ 0 & c \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$$

Since B is invertible not both α and β can be zero. Say $\alpha \neq 0$, then $b = \alpha a \alpha^{-1}$. Similarly we may assume $\delta \neq 0$, in which case $c = \delta a \delta^{-1}$. But then $b = \alpha^{-1}\delta\, c\, \delta^{-1}\alpha = (\delta^{-1}\alpha)^{-1}c(\delta^{-1}\alpha)$, i.e. b and c are conjugate.

Let Q be the set of quasiconjugations of a group in $PGL_2(K)$ (not necessarily finite) and let S be the fixed point set of the elements of G - Q (i.e. of the non-quasiconjugations). Then we have a group action of G on the set S. To see this we note

Lemma 2.2. Let G be a subgroup of $PGL_2(K)$ and let Q be the set of quasiconjugations in G. Then the group generated by the elements of Q is a normal subgroup of G.

Proof : By lemma 1.3 Q is a normal subset of G, so that the subgroup generated by Q must necessarily be normal.

Let $x \in S$, then there is an element $h \in G - Q$ such that $h(x) = x$. Then for any $g \in G$, $g(x)$ is a fixed point of ghg^{-1}, and by lemma 2.2 $ghg^{-1} \in G - Q$. Hence for any $g \in G$ $g(x) \in S$, i.e. G acts on S.

This simple fact has a number of consequences :

Example : Call an element of $PGL_2(K)$ antidiagonal if it has zeros on the main diagonal (the entries off the main diagonal are then necessarily non-zero).

If the non-quasiconjugations of a group G in $PGL_2(K)$ are diagonal, then the quasiconjugations of G are either diagonal or antidiagonal.

Proof : Let S and Q be as before. Since the elements of G - Q are all diagonal, S consists of just two points, i.e. 0 and ∞. Let $g \in G - Q$, $x_0 \in S$, $s \in Q$. Then $g(x_0) = x_0$

and $sgs^{-1} \in G - Q$ has fixed point $s(x_0)$. So the fixed points of sgs^{-1} must be $s(0)$ and $s(\infty)$. But since G acts on S we must have either $s(0) = \infty$ or $s(0) = 0$. Write $s = (px + q)(rx + t)^{-1}$, then s has matrix $\begin{pmatrix} p & q \\ r & t \end{pmatrix}$. Now if $s(0) = 0$, then clearly also $s(\infty) = \infty$. It follows that $q = r = 0$, i.e. that s is diagonal. On the other hand if $s(0) = \infty$, then $s(\infty) = 0$ and then $p = t = 0$ which means that s is antidiagonal.

Note that any group whose non-quasiconjugations share the same two fixed points can be transformed into a group of the above form.

In the non-commutative case it is conceivable that there is only one G - orbit to the action of G on S, i.e. that the action is transitive. If G is also finite, then we have

Proposition 2.3. Let G be a finite subgroup of $PGL_2(K)$ and let Q be the set of quasiconjugations in G. Let S be the set of fixed points of the elements of G - Q. If the action of G on S is transitive, then G is generated by its quasiconjugations.

Proof : If there is only one orbit in the action of G on S, then by the orbit formula

$$|G| = \sum_{g \in G} \theta(g) ,$$

where $\theta(g)$ is the number of fixed points of $g \in G$ in S. Every element outside Q fixes two points, so there must

be at least as many elements inside Q fixing none. Moreover the unit matrix fixes all points of S, so if we put $q = |S|$ then there must be $\frac{q}{2}$ more elements in Q not fixing any points. Hence $|Q| > |G| - |Q|$. It follows that $\langle Q \rangle = G$.

Unfortunately the converse of this proposition does not hold :

Let $\omega \in K - k$ be such that $\omega^3 = 1$. Then ω and ω^2 both have $t^2 + t + 1 = 0$ as their minimal equation over k and hence must be conjugate. By lemma 2.1 therefore $\begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix}$ is a quasiconjugation. And now we have

$$\begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix} \begin{pmatrix} \omega & 0 \\ 0 & \omega \end{pmatrix} = \begin{pmatrix} \omega^2 & 0 \\ 0 & 1 \end{pmatrix} \qquad (1)$$

the right hand side of which is clearly not a quasicon= gation, If we consider the group generated by

$\begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix}$ and $\begin{pmatrix} \omega & 0 \\ 0 & \omega \end{pmatrix}$, then G contains non-quasiconju= gations and G is generated by quasiconjugations. Since G consists of diagonal matrices the fixed-point-set of G - Q is $S = \{0, \infty\}$ and there are two orbits of one point each.

Note also that the generators of this (abelian) group are by no means unique. For instance $\begin{pmatrix} \omega & 0 \\ 0 & \omega \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & \omega \end{pmatrix}$ is an alternative pair of generators, one of which is no

longer a quasiconjugation.

(1) also illustrates the fact that the product of two quasiconjugations is not necessarily again a quasiconjugation. It is therefore a fairly strong condition if we assume that the quasiconjugations of a group G form a subgroup. In this context we can say a little more :

Proposition 2.4. Let K be a skew field with centre k and let a be non-zero element of K. Let G be a finite subgroup of $PGL_2(K)$ containing aI. Then the following statements are equivalent :

a) $aI \in G$ shares its fixed points with all its conjugates in G.

b) The cyclic group N generated by $aI \in G$ is normal in G.

c) If $x_0 \in \overline{C(a)}$, the centralizer of a including ∞, then the G-orbit of x_0 is a subset of $\overline{C(a)}$.

Proof : Put A = aI.

b)⇒c) : Let x_0 be a fixed point of A. Then for any $B \in G$, Bx_0 is a fixed point namely of BAB^{-1}. Since N is generated by A and N is normal in G, we must have $BAB^{-1} \in N$. But $A \longmapsto BAB^{-1}$ is an automorphism of the cyclic group N. So $BAB^{-1} = A^r$ and both A and A^r generate N. But since Bx_0 is a fixed point of A^r, it must be a fixed point of A, for any $B \in G$.

c)⇒a) : Assume $ABx_0 = Bx_0$ for all $B \in G$ whenever $Ax_0 = x_0$. Then $B^{-1}ABx_0 = x_0$ whenever $Ax_0 = x_0$.

a)⇒b) : We are given that $B^{-1}ABx_0 = x_0$ for all $B \in G$

whenever $Ax_0 = x_0$. Since 0 and ∞ are in the fixed-point-set of A, $B^{-1}AB$ must be a diagonal matrix, C say. Since 1 is also in the fixed-point-set of A, the diagonal entries of C must be equal, say $C = B^{-1}AB = cI$, where $c \in K$ depends on B. Moreover a and c are conjugate in K,

for if $B = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}$, then some b_i is non-zero, say $b_1 \neq 0$.

Then $$\begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}^{-1} \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} = \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix}$$

implies that $b_1^{-1}ab_1 = c$. We form the subgroup N of G which is generated by all conjugates of A under G, i.e.

$$N = \langle B^{-1}AB \mid B \in G \rangle.$$

This group is clearly normal in G. Furthermore since its elements are scalar matrices (modulo central multiples), N is isomorphic to a finite subgroup N' of K^*/k^*, i.e. of the multipilcative group of K modulo that of k. All the elements of N' are conjugate in K^*/k^*. Hence

$$N \cong N' = \langle p^{-1}ap\delta \mid P^{-1}aP = p^{-1}ap\delta I \text{ for some } P \in G, \delta \in k \rangle$$

We note that $a \in N'$. By hypothesis the elements of N' are fixed points of A, hence every element of N' is a fixed point of every element of N. It follows that N is abelian. But then so is N'. Now any finite abelian subgroup of K is contained in a commutative subfield of K. It must therefore be cyclic, and so must its homomorphic image in K^*/k^*. So N' and hence N is cyclic.

It may be worth observing that when the quasiconjugations of G do form a cyclic subgroup N, then G acts on several sets :

Note first that by lemma 2.1 N is normal in G, so condition c) of proposition 2.4 holds. Let S be the fixed-point-set of elements of G - N (we assume here that $G \neq N$ so that S is non-empty). There is no loss of generality in assuming the fixed-point-set to be $\overline{C(a)}$, where aI generates N. Put $S_1 = S \cap \overline{C(a)}$ and $S_2 = S - S_1$.

If S_1 is non-empty, then G acts on S_1 : For if $x_0 \in S_1$, then for some $A \in G$, $Ax_0 = x_0$. But if we choose A to be the generator of N, i.e. $A = aI$, then by proposition 2.4, part c), Bx_0 is also a fixed point of A for any $B \in G$.

Similarly we have a group action on S_2. Note that the elements of G - N fix one or two points in S_1 (and S_2).

The following result illustrates that to some extent questions about quasiconjugations in $PGL_2(K)$ can be reduced to problems in K^*/k^*:

Proposition 2.5. Let G be a finite group in $PGL_2(K)$ suppose $aI \in G$ for some $a \in K$.

Let $M = \{P \in G \mid P^{-1}aP = a^r \delta_1 I$ for some r and some $\delta_1 \in k\}$ be the normalizer of aI in G.

Let $C = \{P \in G \mid P^{-1}aP = a\,\delta_2 I$ for some $\delta_2 \in k\}$ be the centralizer of aI in G.

Let $M_a = \{x \in K^* \mid x^{-1}ax = a^r \delta_3$ for some r such that there is $P \in G$ with $P^{-1}aP = a^r \delta_4 I\}$

Let $C_a = \{x \in K^* \mid xa = ax\,\delta_5$ for some $\delta_5 \in k\}$. Then

$$M / C \cong M_a / C_a$$

Proof : First we note that C is obviously normal in M and C_a is normal in M_a. Let $P_1, P_2 \in G$ be such that $P_i^{-1} a P_i = a^r \delta_i$ $(i = 1,2)$ for some r and $\delta_i \in k$. Then $aP_1P_2^{-1} = aP_1P_2^{-1}\delta$, so $P_1P_2^{-1} \in C$ and P_1, P_2 belong to the same (left) coset in M/C. Similarly $x_1x_2^{-1} \in C_a$ if $x_i^{-1} a x_i = a^r \delta_i$ $(i = 1,2)$ and then x_1 and x_2 belong to the same (left) coset in M_a/C_a. Given $P \in M$, we obtain $x \in M_a$ by taking a non-zero entry of P. We define the isomorphism of the proposition by mapping those cosets to each other whose elements conjugate a (or aI) to the same power of aI (or a).

Several things remain to be remarked in connection with proposition 2.5 :

1. If a has order m, and r is as in M or M_a, then r and m are coprime. If in the definition of M_a there is $P \in G$ such that $P^{-1} a P = a^r \delta I$ for every $r < m$ subject to coprimality, then M_a is the normalizer of a in K .

2. If $\langle aI \rangle$ is a normal subgroup of G, then M = G.

3. $C = G \cap PGL_2(C_a)$ since aI is a scalar matrix.

4. Although the finite subgroups of K^* are known (cf. [1]), the same cannot be said for finite subgroups of K^*/k^* and there seems to be no easy way of deriving them. However when $K = \mathbb{H}$, the real quaternions, then the finite subgroups of $\mathbb{H}^*/\mathbb{R}^*$ turn out to be the cyclic, dihedral, tetrahedral, octahedral and icosahedral groups.

This concludes what we have to say on groups which contain quasiconjugations.

b) Cyclic Diagonal Groups without Quasiconjugations

The remainder of chapter 2 will be devoted to finite groups of $PGL_2(K)$ which contain no quasiconjugations and from here onwards the expression "finite subgroup of $PGL_2(K)$" will always be short for "finite subgroup of $PGL_2(K)$ without quasiconjugations".

Obviously to obtain a complete classification of finite subgroups of $PGL_2(K)$ (without quasiconjugations), we need to know what kinds of diagonal such groups there are. In the commutative case this problem is trivial : All diagonal groups are cyclic since multiolicative subgroups of commutative fields are cyclic. In the general case it turns out that - somewhat surprisingly perhaps - finite diagonal subgroups are the main obstacle to a complete classification. Indeed we shall only deal here with cyclic diagonal groups.

Let G be a finite diagonal subgroup of $PGL_2(K)$ of order n. Since G contains no quasiconjugations we know by lemma 2.1 that the elements of G must have inconjugate diagonal entries. We shall write the elements of G in the form $\overline{(a,b)}$, where a is the top left-hand entry and b the bottom right hand entry. We note that given such an element of G, a and b are not unique. a and b are unique

only up to a common central multiple. Put

$$H = \{b \in K \mid \overline{(a,b)} \in G\}$$

and define an equivalence relation on H :

$$b_1 \sim b_2 \text{ iff } b_1 = b_2\lambda \text{ for some } \lambda \in k .$$

Let G_2 be a set of representatives of the set of equiva= lence classes, i.e. let G_2 be a transversal for the equivalence classes. Define

$$G_1 = \{a \in K \mid \text{there exists } b \in G_2 \text{ such that } \overline{(a,b)} \in G\}$$

When K is commutative (i.e. K = k), then we can take $G_2 = \{1\}$, in which case G_1 is a (necessarily cyclic) subgroup of k^*. In particular this illustrates that G_1 will not in general be a transversal.

What follows will be concerned with finding an appropriate choice of G_2, and hence of G_1.

From its equivalence class we shall pick 1 to be in G_2. It follows from the definition that then also $1 \in G_1$. Since G is finite we can choose G_2 to be finite and hence also G_1. If $\lambda \in k$, then $\overline{(a,b\lambda)} = \overline{(a\lambda^{-1},b)}$, so we may stipulate that G_2 contains no central multiples. Next suppose G_2 is a subgroup of K^* and let $a,c \in G_1$. Then there are $b,d \in G_2$ such that $\overline{(a,b)},\overline{(c,d)} \in G$. Hence $(\overline{a,b})(\overline{c,d}) = (\overline{ac,bd})$ and by assumption $bd \in G_2$. So $ac \in G_1$ and it follows easily that G_1 is also a group. Summing up,

Lemma 2.6. Let G be a finite diagonal subgroup of $PGL_2(K)$. Let G_1 and G_2 be as defined above. Then we can choose G_1 and G_2 such that

1) $1 \in G_1$ and $1 \in G_2$,

2) G_2 contains no central multiples ,

3) G_1 and G_2 are finite.

In this case if G_2 is a group, so is G_1.

Essentially G_1 and G_2 are just the 1-1 and 2-2 entries respectively of elements of G.

Given $(\overline{a,b}) \in G$ of order m, both a and b satisfy the equation $t^m - \lambda = 0$ for some $\lambda \in k$. Since a,b are inconjugate, $t^m - \lambda$ must be reducible.

At this stage we recall the following well known result :

Theorem X . Let F be any field, p a prime number and consider the equation

$$x^p = c \quad (c \in F) \qquad (1)$$

Either (1) has a linear factor or (1) is irreducible over F, according as c is or is not a p-th power in F.

This gives us the important

Corollary 2.7. If G is a finite diagonal group in $PGL_2(K)$ of prime order p (without quasiconjugations), then (G is cyclic and) the elements of G_1 and G_2 can be taken to be roots of 1.

Proof : As shown before, if $(\overline{a,b})$ is the generator of G with $a \in G_1$ and $b \in G_2$, then a,b satisfy $t^p - \lambda = 0$ for some $\lambda \in k$. Hence $t^p - \lambda$ is reducible and by theorem X has a linear factor. This means λ has a p-th root μ in k. So instead of choosing $a \in G_1$, $b \in G_2$ we take $a\mu^{-1} \in G_1$ and $b\mu^{-1} \in G_2$ and these will satisfy $t^p - 1 = 0$. The representatives of the other elements will be powers of $a\mu^{-1}$ and $b\mu^{-1}$ respectively which satisfy the corollary.

Clearly G_1 and G_2 are cyclic subgroups of K^* and if $(\overline{a,b})$ generates G, then a generates G_1 and b generates G_2. Now if $b = 1$, then $G \cong G_1$, i.e. G is isomorphic to a finite cyclic subgroup of K^*. If $b \neq 1$ but $a \in k$, then there is no loss of generality in assuming $a = 1$ since $\overline{(a,b)} = \overline{(1,ba^{-1})}$. So we may assume that $a \notin k$ and $b \neq 1$. Now a,b satisfy $t^p - 1 = 0$. Since $a,b \neq 1$, a,b satisfy

$$f(t) = \sum_{i=0}^{p-1} t^i = 0 \quad .$$

But a,b are not conjugate, so f(t) must be reducible over k and a,b have different minimal equations over k. Let the minimal equation of a be g(t) and assume deg g = m. Then g will have at most m roots in k(a) since k(a) is a commutative field. In particular g will have at most m solutions in $G_1 = \langle a \rangle$ since $G_1 \subset k(a)$. But g is a factor of f, so g must have exactly m roots in G_1 since otherwise fg^{-1} would be a polynomial of degree $p - m - 1$ with more than $p - m - 1$ roots in G_1.

Clearly the elements of G_2 satisfy the same minimal equations as the elements of G_1 (but a^i and b^i have distinct minimal equations for $i = 1,\ldots,p-1$). So a is conjugate to some $b^i \in G_2$ (i.e. a must have the same minimal equation as some $b^i \in G_2$), say $b^i = c^{-1}ac$. Since we may take $\begin{pmatrix} 1 & 0 \\ 0 & c \end{pmatrix} G \begin{pmatrix} 1 & 0 \\ 0 & c^{-1} \end{pmatrix}$ instead of G and b^i generates G_2 for any $i = 1,\ldots,p-1$, we find that $G_1 = G_2 = \langle a \rangle$. Thus we have proved

Proposition 2.8. Let G be a finite diagonal subgroup of prime order p in $PGL_2(K)$ (without quasiconjugations). Then precisely one of the following three possibilities will hold :

We can choose G_1 and G_2 such that

1) $G_1 = \{1\}$, $G_2 = C_p$, or

2) $G_1 = C_p$, $G_2 = \{1\}$, or

3) $G_1 = G_2 = C_p$,

where C_p is a cyclic group in K^* of order p.

Cases 1) and 2) in proposition 2.8 are quite trivial (just as the commutative case, where 3) does not occur) and we shall not consider these any further. So when G is of prime order, we shall assume that the elements of G are of form $(\overline{a^i, a^j})$; in particular the generator of G can be taken to be of form $(\overline{a, a^j})$, where $a \in K^*$ and $j = 2,\ldots,p-1$.

What follows now is an investigation into what a^j are

eligible to be paired with a. In other words, given the prime order p of G, we ask for which j are a and a^j not conjugate. This is equivalent to determining the conjugacy class C_a of a (under the action of K^*) in the cyclic group $\langle a \rangle$ (generated by a) for any given prime (order) p (of a).

This investigation will be justified by

Lemma 2.9. Let G be any diagonal group of prime order p in $PGL_2(K)$. Then G contains no quasiconjugations if and only if its generator is not a quasiconjugation.

Proof : Note that this statement makes sense since G, being of prime order, is necessarily cyclic. If G is generated by $\overline{(a,a^j)}$, then the general element of G is $\overline{(a,a^j)}^i = \overline{(a^i,a^{ji})}$ for i = 1,...,p-1. Now if $\overline{(a^i,a^{ji})}$ is a quasiconjugation for some i, then $a^{ji} = c^{-1}a^ic$. Let i' be such that $a^{ii'} = a$. Then $a^j = a^{jii'}$ $= (c^{-1}a^ic)^{i'} = c^{-1}a^{ii'}c = c^{-1}ac$. So $\overline{(a,a^j)}$ must be a quasiconjugation and the lemma follows.

We shall now attempt to determine the conjugacy class of a when a has prime order p. In fact we shall reduce the determination to a problem about primitive roots mod p.

Lemma 2.10. Let $a \in K$ be of prime order p and denote by C_a the conjugacy class of a in $\langle a \rangle$ under the action of K^*. Then there is an integer s, $0 < s < p$, such that

$$C_a = a^{s^i} \quad i = 0,\ldots,r-1 \quad ,$$

where r is the order of C_a.

In fact $a^{s^i} = c^{-i}ac^i$ for some $c \in K^*$ and $i = 0,\ldots,r-1$.

Proof : Let $C_a = \{a^{i_j} \mid j = 0,1,\ldots,r-1;\ i_0=1\}$. We note first that if $a^{i_1}, a^{i_2} \in C_a$, then $a^{i_1 i_2} \in C_a$. Put $E = \{i_j \pmod p \mid j = 0,\ldots,r-1\}$. Then $1 \pmod p \in E$ since $i_0 = 1$, and E is closed under multiplication; being finite, E must be a (finite) subgroup of $(\mathbb{Z}/p)^* = C_{p-1}$. Hence E is cyclic, with generator $i' \pmod p$. Pick any element $s \in i' \pmod p$ such that $0 < s < p$, then s will satisfy the lemma.

We prove the last part of the lemma by induction :

Since a and a^s are conjugate by assumption there is $c \in K^*$ such that $c^{-1}ac = a^s$. Assume now $a^{s^{i-1}} = c^{-(i-1)}ac^{i-1}$. Then $a^{s^i} = (c^{-1}ac)^{s^{i-1}} = c^{-1}a^{s^{i-1}}c = c^{-i}ac^i$ by induction hypothesis.

Proposition 2.11. Let a, p, C_a be as in lemma 2.10. Then

$$\left|C_a\right| = \left|C_{a^j}\right|$$

for any $j = 1,\ldots,p-1$, where $\left|C_a\right|$ denotes the order of C_a.

Proof : By lemma 2.10,

$$C_a = \{c^{-i}ac^i \mid i = 0,1,\ldots,r-1\} \quad ,$$

where $r = |C_a|$ and $c^{-i}ac^i = a^{s^i}$. So the conjugacy class C_{a^j} of a^j in $\langle a \rangle$ contains the set

$$Q = \{c^{-i}ac^i \mid i = 0,\ldots,r-1\}.$$

We claim Q contains r distinct elements : Suppose it does not. Then without loss of generality $a^j = c^{-i_0}a^j c^{i_0}$ for some $i_0 < r$. So $a^j = (c^{-i_0}ac^{i_0})^j = a^{js^{i_0}}$, hence $a^{js^{i_0}-j} = 1$. This holds if and only if $js^{i_0} \equiv j \pmod p$. Since p is prime and $0 < j < p$ this is equivalent to $s^{i_0} \equiv 1 \pmod p$. But by definition r is the smallest integer satisfying $s^r \equiv 1 \pmod p$, contrary to our assumption that $i_0 < r$. This proves the claim. So C_{a^j} contains at least r distinct elements. Suppose $C_{a^{j_0}}$ contains more than r elements for some j_0, i.e. suppose $|C_{a^{j_0}}| = r' > r$. Since p is a prime, a^{j_0} also generates $\langle a \rangle$. It follows by the same argument as before that C_a contains at least r' distinct elements, a contradiction. Hence the proposition.

Corollary 2.12. If a has minimal equation of degree r, then for $i = 1,\ldots,p-1$, a^i has minimal equation of degree r.

Proof : We know from the remarks preceding proposition 2.8 that the degree of the minimal equation of a is equal to the order of its conjugacy class in $\langle a \rangle$.

The same must obviously hold for every element in $\langle a \rangle$ (other than 1) since p is a prime and every element of $\langle a \rangle$ is a generator. By proposition 2.11 the orders of the conjugacy classes of $\langle a \rangle$ are all equal and the corollary follows.

The next result is well known in elementary number theory but follows independently from proposition 2.11 (cf. [5], theorem 88, p.71).

Corollary 2.13. If r is the order of the conjugacy classes in $\langle a \rangle$ and a is of prime order p, then r divides p-1.

Proof : We know that $\{\langle a \rangle - 1\}$ is divided into t conjugacy classes say, each class containing r elements. Hence $tr = p - 1$.

A direct consequence of this is

Corollary 2.14. If a is of prime order p and r is the order of the conjugacy classes in $\langle a \rangle$, then there are $\frac{p-1}{r}$ inconjugate (diagonal) groups G of order p in $PGL_2(K)$ such that $G_1 = G_2 = \langle a \rangle$.

Proof : Suppose G is generated by $\overline{(a, a^i)}$ and a^i and a^j are conjugate for some $j \neq i$. Then for some $c \in K^*$, $c^{-1}a^ic = a^j$, so $\begin{pmatrix} 1 & 0 \\ 0 & c \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & a^i \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & c^{-1} \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a^j \end{pmatrix}$. So the group generated by $\overline{(a, a^j)}$ is conjugate to G.

On the other hand if a, a^i, a^j are pairwise inconjugate in K but $(\overline{a,a^i})$ and $(\overline{a,a^j})$ are conjugate in $PGL_2(K)$, then there are $u,v,x,y \in K$ such that $\begin{pmatrix} u & v \\ x & y \end{pmatrix}$ is invertible and

$$\begin{pmatrix} u & v \\ x & y \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & a^i \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a^j \end{pmatrix} \begin{pmatrix} u & v \\ x & y \end{pmatrix} .$$

But then $va^i = av$, so $v = 0$, and $ya^i = a^j y$, so $y = 0$. This contradicts the invertibility of $\begin{pmatrix} u & v \\ x & y \end{pmatrix}$. So $(\overline{a,a^i})$ and $(\overline{a,a^j})$ must be inconjugate in $PGL_2(K)$.
Thus we have shown that for every conjugacy class in $\langle a \rangle$ there is precisely one conjugacy class of diagonal groups G in $PGL_2(K)$ such that $G_1 = G_2 = \langle a \rangle$. By corollary 2.14 there are $\frac{p-1}{r}$ conjugacy classes in $\langle a \rangle$, hence corollary 2.14 follows.

At this stage our problem is best described in number-theoretic terms and we shall therefore recall some definitions from [5] (p.71, §6.8) :

Let a,m be integers. Then the smallest positive value of x for which $a^x \equiv 1 \pmod m$ is called the order of $a \pmod m$. Denote this order by d, then we say that a belongs to $d \pmod m$. We note that $d \mid \varphi(m)$, where φ is Euler's function. If $d = \varphi(m)$, then we say that a is a primitive root of m.

It is clear then that in lemma 2.10 r is the order of $s \pmod p$ or equivalently that s belongs to $r \pmod p$, and that if $r = p - 1$, then s will be a primitive root of p.

So the question now is : Given that the conjugacy

class C_a of a in $\langle a \rangle$ contains r elements, which integers s are such that $C_a = \{a^{s^i} \mid i = 0,1,\ldots,r-1\}$? Or in number-theoretic terms : Given a factor r of p-1, which integers s belong to r(mod p) ?

If we knew what these integers s were (for any given prime p), then we could check that a^j is <u>not</u> of form $a^j = a^{s^i}$, so that $(\overline{a,a^j})$ is not a quasiconjugation.

A complete answer to this problem is not known, so we shall quote one or two familiar results and give an example as illustration.

<u>Theorem</u> ([5] , p.85, thm.109):

$$s^r \equiv 1 (\text{mod } p) \qquad (3)$$

has r solutions for s.

This does not in fact offer new insights. Applied in our context it just says that if $a^i \in C_a$, and $r = |C_a|$, then $a^{i^r} = a$.

<u>Theorem</u> ([5], p.85, thm.110): Of the r integers satisfying (3) for s, $\varphi(r)$ belong to r(mod p) (where φ is Euler's function).

So although we do not know what these s are (for any given p and r), at least we know how many there are. However a special case is resolved by

Lemma 2.15. Let p be an odd prime. Then $s = p - 1$ if and only if 2 is the order of $s \pmod p$. (Or in our context : $s = p-1$ iff $|C_a| = 2$)

Proof : If $s = p - 1$, then $s^i = (p-1)^i$, and either $(p-1)^i \equiv 1 \pmod p$ - when i is even - or else $(p-1)^i \equiv p-1 \pmod p$ - when i is odd. So only p-1 belongs to $2 \pmod p$, which means p-1 has order 2. Conversely assume $s \pmod p$ has order 2, i.e. $s^2 \equiv 1 \pmod p$. Then $(s+1)(s-1) \equiv 0 \pmod p$ and either $p \mid s+1$ or $p \mid s-1$. But since $s < p$, only $p \mid s+1$ can hold, with $s = p - 1$.

Generally the - unsolved - problem is to find those integers $s<p$ which satisfy $s^{r-1} + s^{r-2} + \ldots + 1 \equiv 0 \pmod p$ for a given odd prime p and integer r such that $r \mid p-1$.

Note that we can leave the case $p = 2$ out of our considerations since p is just the order of the group G and a diagonal group of order 2 cannot fall into the third category of proposition 2.8, the only one under discussion here.

Example : Let G be a (cyclic) diagonal group of order 13 without quasiconjugations in $PGL_2(K)$. Assume G is of type 3) in proposition 2.8, i.e. assume $G_1 = G_2 = \langle a \rangle$, where $a \in K$ satisfies $a^{13} = 1$.

1) $s = 2$: Then a is conjugate to a^2 and hence to all elements of $\langle a \rangle$ since 2 is a primitive root of 13. Similarly 6,7,11 are primitive roots of 13 (and note

$\varphi(12) = 4$). So for G to have no quasiconjugations, a must not be conjugate to a^2, a^6, a^7, or a^{11}.

2) s = 3 : Then a is conjugate to a^3 and to a^9 and no other elements in $\langle a \rangle$. So $C_a = \{a, a^3, a^9\}$ $(=C_{a^3}=C_{a^9})$ and $|C_a| = 3$, i.e. 3 and 9 belong to 3(mod 13).

3) s = 4 : Then $C_a = \{a, a^4, a^3, a^{12}, a^9, a^{10}\}$, so $|C_a| = 6$ and we find that 4 and 10 belong to 6(mod 13).

4) s = 5 : Then $C_a = \{a, a^5, a^{12}, a^8\}$ and 5 and 8 belong to 4(mod 13).

5) s = 12 : Then $C_a = \{a, a^{12}\}$ and 12 belongs to 2(mod 13), as promised by lemma 2.15.

This concludes what we have to say about groups of prime order (without quasiconjugations) in $PGL_2(K)$. Turning to general cyclic (diagonal) groups we find that the entries need no longer be roots of unity in K and in particular that G_1 and G_2 are not necessarily subgroups of K^*.

If we make the assumption that the diagonal entries of the (diagonal) group G are roots of 1, i.e. that G_1 and G_2 consist of roots of 1, then we can show that if such a group is abelian it must in fact be cyclic. First we need

Lemma 2.16. Let G be a cyclic (diagonal) subgroup of $PGL_2(K)$ (without quasiconjugations) of order p^r, where p is a prime. If $(\overline{a,b})$ is the generator of G and $a^{p^r} = b^{p^r} = 1$, then one of G_1 and G_2 is a cyclic subgroup of K^* of order

p^r and the other is conjugate to a (possibly trivial) subgroup of the former.

Proof : Clearly if G is generated by $(\overline{a,b})$, then either $a^j = 1$ or $b^j = 1$ for all $j < p^r$. Assume then that $G_1 = \langle a \rangle$ is of order p^r. The remainder of this lemma is proved in a way similar to that of proposition 2.8 and we shall only sketch the proof :

a,b satisfy $t^{p^r} - 1 = 0$ and by assumption a is of order p^r. If $b = 1$ there is nothing to prove, so we assume $b \neq 1$. Then a,b satisfy

$$f(t) = \sum_{i=0}^{p^r-1} t^i = 0 .$$

But a,b are not conjugate, so f(t) must be reducible. Let g be the minimal equation of a, and put deg g = s. Then g(t) = 0 will have exactly s solutions in $G_1 = \langle a \rangle$. Now the elements of $G_2 = \langle b \rangle$ satisfy minimal equations which are also satisfied by some elements of G_1. So in particular b satisfies the same minimal equation as a^e for some $e > 1$, i.e. b is conjugate to some $a^e \in G_1$ which is what we wanted to show.

We note that lemma 2.16 is a generalization of proposition 2.8.

Theorem 2.17. Let G be an abelian diagonal group of order m, without quasiconjugations, in $PGL_2(K)$. If G_1 and G_2 (can be taken to) consist of roots of 1, then G

is cyclic.

Proof : Let $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, where the p_i are distinct primes. For every prime power $p_i^{\alpha_i}$ there will be precisely one subgroup H_i of G of order $p_i^{\alpha_i}$, necessarily cyclic. By assumption the (diagonal) entries of elements of H_i are roots of 1 which commute with each other. So $(H_i)_1$ and $(H_i)_2$ can be taken to be finite cyclic subgroups of K^*. By lemma 2.16 one of $(H_i)_1$ and $(H_i)_2$ is of order $p_i^{\alpha_i}$ and the other has order dividing $p_i^{\alpha_i}$. Let $(H_i)_2$ be generated by a_i. Then $a_i^{p_i^{\beta_i}} = 1$ for some $\beta_i \leq \alpha_i$. Put $p_i^{\beta_i} = q_i$. We claim that G_2 is a group generated by $\prod a_i$: Firstly we note that the elements of G_2 commute since G is abelian. Secondly if $a \in G_2$, then we may take $a^j \in G_2$ for all j less than the order of a. Thus we need to find a of the same order as G_2. But clearly

$$|G_2| = \prod_i |(H_i)| = \prod_i q_i$$

and so we are reduced to showing that $\prod a_i$ has order $\prod q_i$. Put $n = \prod q_i$ and $n_i = \frac{n}{q_i} = q_1 \cdots q_{i-1} q_{i+1} \cdots q_r$. If a has order n, then $a_i = a^{n_i}$. To prove the converse (and hence the claim) we have to show that $\sum n_i$ is coprime to n, i.e. our problem is to show that

$\sum_{i=1}^{r} q_i$ and $\sum_{i=1}^{r} q_1 \cdots q_{i-1} q_{i+1} \cdots q_r$ are coprime :

$\prod_{i=1}^{r} q_i$

Suppose they are not coprime. Then they must share a prime factor, p_1 say. Now $\sum_{i=2}^{r} q_1 \cdots q_{i-1} q_{i+1} \cdots q_r$ also has factor p_1, so

$$\sum_{i=1}^{r} q_1 \cdots q_{i-1} q_{i+1} \cdots q_r - \sum_{i=2}^{r} q_1 \cdots q_{i-1} q_{i+1} \cdots q_r = q_2 \cdots q_r$$

must have a factor p_1, contradicting our assumption that the p_i are distinct. This proves the claim. Clearly now $n \mid m$ and similarly (using lemma 2.6) we show that G_1 is a cyclic group (of order dividing m). But if both G_1 and G_2 are cyclic, then G must be cyclic.

Corollary 2.18. Let G be a cyclic group of order m in $PGL_2(K)$ (diagonal and without quasiconjugations). Then if G_1 and G_2 are subgroups of K^* of orders m_1, m_2 respectively, m is the lowest common multiple of m_1 and m_2.

Proof : We have already shown that if $m_i = |G_i|$ for $i = 1,2$, then $m_i \mid m$. If $(\overline{a,b})$ is the generator of G, and $(\overline{a^t,b^t}) = I$ for some t, then $m \mid t$. Hence the corollary.

The main application of theorem 2.17 is

Corollary 2.19. Let G be an abelian diagonal group of squarefree order m in $PGL_2(K)$ (without quasiconjuga=

tions). Then G is cyclic and if $(\overline{a,b})$ is the generator of G, then $a^m = b^m = 1$.

Proof : All we have to show is that the hypothesis of theorem 2.17 is satisfied, i.e. that G_1 and G_2 (can be taken to) consist of roots of 1. Let $m = \prod p_i$ be a decomposition of m into distinct primes. Then for every p_i there will be precisely one subgroup H_i of G of order p_i. Hence any two of these subgroups intersect trivially. So we can apply proposition 2.8 and take the (non-zero) entries of their generators to be roots of 1. This proves the corollary.

Turning to general cyclic groups, let C_n be a cyclic diagonal group of order n (without quasiconjugations) in $PGL_2(K)$. If $(\overline{a,b})$ is the generator of C_n, then a,b satisfy $t^n - \lambda = 0$ for some $\lambda \in k$. Let p be a prime dividing n and put $q = \frac{n}{p}$. Then $(\overline{a,b})^q = (\overline{a^q,b^q})$ generates a cyclic subgroup C_p of order p in C_n. a^q and b^q both satisfy $t^p - \lambda = 0$. Since a^q and b^q are incon= jugate this must be reducible, so by theorem X, λ has a p-th root in k. This gives us

Proposition 2.20. Let C_n be a cyclic group of order n (without quasiconjugations) in $PGL_2(K)$, with generator $(\overline{a,b})$. Then a,b satisfy an equation $t^n - \lambda = 0$ for some $\lambda \in k$ such that λ has a p-th root in k for every prime p dividing n.

Example : Let $\dot{G}$ be a diagonal group of order 4 (without quasiconjugations) in $PGL_2(K)$. Then G is cyclic : For otherwise every element $(\overline{a,b}) \in G$ (except I) would be of order 2. But then for some $\lambda \in k$, a,b would satisfy an equation $t^2 - \lambda = 0$ which must be reducible since a,b are inconjugate. It follows that both a and b satisfy linear equations over k, i.e. $a,b \in k$. But then $G \subset PGL_2(k)$. Being diagonal this means that G is cyclic, contradicting our assumption. So G is cyclic. If $(\overline{a,b})$ is the generator of $G = C_4$, then a,b satisfy $t^4 - \lambda = 0$. By proposition 2.20, λ has a square root μ in k, so $t^4 - \lambda = (t^2 + \mu)(t^2 - \mu)$. Assuming that λ does not have a 4-th root in k we see that $t^2 + \mu$ and $t^2 - \mu$ are irreducible and $a^2 = \mu$ and $b^2 = -\mu$. Noting that $(\overline{-\mu, \mu}) = (\overline{-1,1})$ we find that $C_4 = \{(\overline{a,b}) , (\overline{-1,1}) , (\overline{-a,b}) , (\overline{1,1})\}$.

This concludes our remarks on cyclic diagonal groups without quasiconjugations.

c) The Classification of Finite Groups without Quasiconjugations

In this section we shall determine the finite subgroups of $PGL_2(K)$ which contain no quasiconjugations. It turns out that diagonal groups are essentially the only ones which need further analysis. The method used here is a generalization of the well known treatment for

the complex numbers.

First we need some terminology : Let G be a finite group of order n (without quasiconjugations) in $PGL_2(K)$. By hypothesis (and theorem 1.14) every non-unit element of G has exactly two fixed points in some extension of K. Let us assume throughout that K is large enough to contain these fixed points. Let S be the fixed-point-set of G - {I}. Note that S may include the point at infinity. A fixed point $x_0 \in S$ is said to have multiplicity e, or to be e-tuple, if it is a fixed point of exactly e matrices in G including I. We recall from chapter 1 that if $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then the map α corresponding to A is given by $\alpha : x \longmapsto (ax + b)(cx + d)^{-1}$, and vice versa. If $x_0 \in S$ is e-tuple, then the stabilizer of x_0,

$$G_{x_0} = \{\alpha \in G \mid \alpha(x_0) = x_0\} ,$$

has order e, and the G - orbit of x_0,

$$G(x_0) = \{\alpha(x_0) \mid \alpha \in G\} ,$$

has $\frac{n}{e}$ members since $|G(x_0)| = |G|/|G_{x_0}|$. All these members of $G(x_0)$ are fixed points, i.e. $G(x_0) \subset S$: If x_0 is a fixed point of α , then $\beta(x_0)$ is a fixed point of $\beta\alpha\beta^{-1}$. So we have an action of G on S. Let S fall into t orbits, and let the i-th orbit have r_i points. For each i let m_i be such that $n = r_i m_i$.

Then the points of the i-th orbit have in their stabilizers m_i elements, i.e. they must be m_i-tuple. Since by assumption there are no quasiconjugations in G, every non-identity matrix in G fixes precisely two points, while the identity fixes all points (of S), i.e. $r_1 + \ldots + r_t$. Thus by the orbit formula

$$t = \frac{2(n-1)}{n} + \frac{1}{n}\sum_{i=1}^{t} r_i \quad .$$

Hence
$$2(1 - \tfrac{1}{n}) = \sum_{i=1}^{t}(1 - \tfrac{1}{m_i}) \qquad (4)$$

Excluding the trivial group, we have $n > 1$, hence $2(1 - \frac{1}{n}) \geqslant 1$, but $2(1 - \frac{1}{n}) < 2$. Now $m_i \geqslant 2$ since all matrices fix two points except the identity, so for each i, $1 - \frac{1}{m_i} \geqslant \frac{1}{2}$, but $1 - \frac{1}{m_i} < 1$. So there are at least two terms on the right hand side of (4), but no more than three. We take these cases separately :

1. There are two terms, i.e. $t = 2$, so there are two orbits. Then

$$2 - \frac{2}{n} = (1 - \tfrac{1}{m_1}) + (1 - \tfrac{1}{m_2}) \ ,$$

hence $r_1 + r_2 = 2$. By assumption $r_1, r_2 > 0$, so $r_1 = r_2 = 1$, hence $m_1 = m_2 = n$. This means that all elements of G share the same two fixed points. Since these are inconjugate this means by corollary 1.9 that G is conjugate to a diagonal group.

In the special case where the centre k of K is

algebraically closed we can in fact say more :

Lemma 2.21. Let K be a skew field with algebraically closed centre k. Then any finite subgroup of K^* lies in k^* and hence is cyclic.

Proof : Denote the finite subgroup of K^* by C and assume it is of order n. Then every element of C satisfies an equation of the form $t^m - 1 = 0$, where $m \mid n$, i.e. every element of C satisfies an equation of some degree m over k. Since k is algebraically closed k will contain m solutions of this equation. Because of the unique factorization property of K[t] K will not contain any other solutions. This means that every element of C lies in k, so C lies in k . It is a well known fact that every finite subgroup of a commutative field is cyclic.

As a consequence we obtain

Proposition 2.22. Let K have algebraically closed centre k. Then any finite diagonal group G in $PGL_2(K)$ is cyclic.

Proof : Let $(\overline{a,b})$ be any element of G. Since $(\overline{a,b})$ is of finite order, a,b satisfy the equation $t^s - \lambda = 0$ over k, for some s. Since k is algebraically closed λ will have an s-th root in k, so we may take $\lambda = 1$. By lemma 2.21 it follows that $a,b \in k$. But this means that G is a finite diagonal subgroup of $PGL_2(k)$, hence C is

cyclic.

Note that when the centre k of K is algebraically closed $PGL_2(K)$ does not contain any quasiconjugations of finite order, since these would only amount to the unit matrix.

Note also that we do not really need the full force of algebraic closure in lemma 2.21 and proposition 2.22. All we have used in fact is that for $\lambda \in k$, k contains all roots of λ. So the condition we need on k is that for any $\lambda \in k$ (including $\lambda = 1$) λ has one (primitive) n-th root in k, for any n (k will then contain all other n-th roots), i.e. that k is root-closed.

Returning to our classification,

2. There are three terms in (4), so there are three orbits. Then

$$2 - \frac{2}{n} = (1 - \frac{1}{m_1}) + (1 - \frac{1}{m_2}) + (1 - \frac{1}{m_3})$$

so
$$\frac{1}{m_1} + \frac{1}{m_2} + \frac{1}{m_3} = 1 + \frac{2}{n} \quad .$$

Each m_i is at least 2, but not all m_i are greater because $\frac{1}{3} + \frac{1}{3} + \frac{1}{3} = 1 < 1 + \frac{2}{n}$. Hence we may take $m_1 = 2$ and then

$$\frac{1}{m_2} + \frac{1}{m_3} = \frac{1}{2} + \frac{2}{n}$$

Not both of m_2, m_3 are greater than 3, so we may take m_2 to be 2 or 3. We consider these cases in turn :

a) $m_1 = m_2 = 2$, $m_3 = \frac{n}{2}$

We note that in this case the order n of G is even. One orbit consists of $\frac{n}{2}$ - tuple fixed points, x_0 and x_1 say. The other two orbits consists of $\frac{n}{2}$ double fixed points each. The stabilizer G_{x_0} of x_0 is a subgroup of G of index 2 such that any element outside G_{x_0} maps x_0 to x_1. Clearly all the elements of G_{x_0} share the same two fixed points, so G_{x_0} can be taken to be a diagonal group. Let y_0 be a double fixed point in one of the other orbits. Then G_{y_0} is a group with two elements. Let T be the non-identity element of G_{y_0}. If $S \in G_{x_0}$, then $TS(x_0) = T(x_0) = x_1$, so $TS \notin G_{x_0}$, hence G_{x_0} and TG_{x_0} partition G into two sets with $\frac{n}{2}$ elements each; in other words, $G = \{G_{x_0}, TG_{x_0}\}$. There is no loss of generality in taking G_{x_0} to be diagonal and $T = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

In the special case where the centre of K is algebraically closed, G_{x_0} is cyclic by proposition 2.22, so G turns out to be the dihedral group which has defining relations $S^{\frac{n}{2}} = T^2 = (ST)^2 = I$.

In the remaining cases we have $m_1 = 2$, $m_2 = 3$, $m_3 \geq 3$ and we get

$$\frac{1}{m_3} = \frac{1}{6} + \frac{2}{n}$$

This holds when $m_3 = 3$ and $n = 12$; when $m_3 = 4$ and

$n = 24$; when $m_3 = 5$ and $n = 60$ and for no other values.

b) $m_1 = 2$, $m_2 = m_3 = 3$

Then G has order $n = 12$. Two orbits consist of four 3-tuple fixed points. Then the stabilizer G_{x_0} of one of them will contain three elements and hence must be cyclic, generated by A say. But then G_{x_0} (and A in particular) fixes another point, x_1 say. Note that any element out= side G_{x_0} maps x_0 to x_1 and x_1 to x_0. Similarly there is one other stabilizer of order 3, G_{y_0} say, which fixes y_0 and y_1 and which is generated by B say. Again any ele= ment outside G_{y_0} maps y_0 to y_1 and vice versa. The third orbit has six double fixed points, so their stabilizers are of order 2. This means that the cyclic subgroups (and hence all the elements) of G are of order 2 and 3 only. We claim that AB is of order 2 : For suppose AB is of order 3. Then AB is contained in $<A>$ or in $<B>$. So AB keeps either x_0 or y_0 fixed. But $AB(x_0) = A(x_1)$ $= x_1$ and $AB(y_0) = A(y_0) = y_1$. Hence AB is outside $<A>$ and $<B>$, a contradiction, and the claim follows. This gives us the defining relations for G : $A^3 = B^3 = (AB)^2$ $= I$. G is also known as the tetrahedral group, or as alternating group on four letters, Alt_4.

c) $m_1 = 2$, $m_2 = 3$, $m_4 = 4$

Then G has order 24. We obtain stabilizer groups of orders 2,3 and 4. The stabilizer groups of order 4 must

be cyclic as shown in the example following proposition 2.20 (that these stabilizers are diagonal follows from the fact that all the elements of a stabilizer share at least one fixed point, which is impossible in the dihedral group, the only other kind of group of order 4). The rest of the argument goes as in the previous case. Thus we obtain defining relations $A^4 = B^3 = (AB)^2 = I$ for G. G in this case is the symmetric group on four letters, Sym_4 ; it is sometimes referred to as the octahedral group.

d) $m_1 = 2$, $m_2 = 3$, $m_3 = 5$

Then G has order 60. All the stabilizer groups are cyclic because they are of prime order. As before we obtain defining relations $A^5 = B^3 = (AB)^2 = I$. This is the alternating group on five letters, Alt_5 , also called the icosahedral group.

Call a skew field K "closed under quadratic equations" if for any $p,q \in K$ the equation $x^2 + px + q = 0$ has a solution in K. Then we can sum up the result of this section in

Theorem 2.23. Let K be a skew field which is closed under quadratic equations and which is root-closed. Let G be a finite group in $PGL_2(K)$ without quasiconjugations and such that the characteristic of K does not divide the order of G. Then G is conjugate to one of the following types of groups :

1. The diagonal group.
2. The diagonal group with $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ adjoined.
3. The tetrahedral group.
4. The octahedral group.
5. The icosahedral group.

Note that the assumptions on K in this theorem are weaker than existential closure. We need closure under quadratic equations because of lemma 1.4 which ensures the existence of the first fixed point in K (and indeed also of the second fixed point).

If in addition the centre k of K is algebraically closed, then the condition that G contain no quasiconjugations becomes redundant as we have seen. Moreover by proposition 2.22 the diagonal groups are all cyclic. This gives us

Theorem 2.24. Let K be as in theorem 2.23. Assume furthermore that the centre k of K is algebraically closed. Then $PGL_2(K)$ contains only cyclic, dihedral, tetrahedral, octahedral, and icosahedral groups.

In fact we shall see in chapter 3 that any finite group of $PGL_2(K)$ is conjugate to one in $PGL_2(k)$ (cf. theorem 3.13).

3. FIXED FIELDS

Introduction

Throughout this chapter the centre k of the skew field K will be assumed algebraically closed unless stated otherwise. K itself will be taken to be large enough to contain the two fixed points of every matrix involved (note that there are no quasiconjugations of finite order in $PGL_2(K)$).

Whereas chapter 1 dealt with the action of a finite subgroup G of $PGL_2(K)$ on a general skew field K, this chapter will be concerned with the action of G on $K_k(x)$, where k is algebraically closed. The object then is to determine the fixed fields in $K_k(x)$ of the finite subgroups of $PGL_2(K)$. This was ~~been~~ done for the complex numbers by Felix Klein around 1870 [6]. We shall modify (and sometimes simplify) the treatment of this as given by Weber [7] to apply to our more general setting. In doing so we shall prove the other main result of this chapter, i.e. that every finite subgroup of $PGL_2(K)$ is conjugate to a finite subgroup of $PGL_2(k)$.

Section a) on invariants and groundforms does not contain any original work. It is not included in chapter 0 because its understanding requires some of the facts and definitions given in the two previous chapters. Appropriate references will be given. Section b) prepares the ground for the subsequent determination of the

fixed fields. Essentially what we shall show there is that if a finite subgroup of $PGL_2(K)$ is conjugate to one in $PGL_2(k)$, then we can find its fixed field.

After this we shall deal with each type of group separately. In each case we show that the group in question has a conjugate in $PGL_2(k)$. For the cyclic and dihedral groups this fact leads us straight to their fixed fields (and groundforms). For the remaining groups we have to determine their groundforms first. Over the complex numbers this is found in Weber's book [7] (which does not however derive the fixed fields). We shall employ more direct methods in places. For instance in the octahedral group Weber derives the invariant W as Hessian of the groundform f and the invariant M as Jacobian of f and W. We shall obtain W and M by a straight calculation using the fact that the octahedral group contains the tetrahedral group as normal subgroup of index 2. Or finding the groundforms of the icosahedral group represents a considerable simplification of Weber's treatment which requires knowledge about polars and invariants of quartics. And showing that these groundforms are in fact absolute invariants is done by virtue of the fact that the icosahedral group is simple, also a shortcut compared with Weber's treatment.

We conclude this chapter with a brief outlook on finding the fixed field of the cyclic group when the

centre k of K is not algebraically closed.

a) Groundforms and Invariants

The treatment of groundforms given below roughly follows the account given by Weber in [7]. Throughout this section k will denote an algebraically closed commutative field.

Let G be a finite group of order n in $PGL_2(k)$. By a relative invariant of G we shall understand a polynomial $f(x) \in k[x]$ such that for all $A \in G$, we have

$$f(A(x)) = cf(x)$$

for some $c \in k$. When $c = 1$ we call f an absolute invariant.

Let $a \in k$ be an m - tuple fixed point of G in k (i.e. a fixed point of m elements of G in k). The stabilizer of a clearly forms a group, so m divides n. Put $r = \frac{n}{m}$, then the G - orbit of a consists of r fixed points, $\{a=a_0, a_1, \ldots, a_{r-1}\}$ say. Recall that for any $A \in G$,

$$\{A(a_0), \ldots, A(a_{r-1})\} = \{a_0, \ldots, a_{r-1}\} .$$

Let $A \in G$ be of form $x \longmapsto (\alpha x + \beta)(\gamma x + \delta)^{-1}$ and assume $\det A = 1$, i.e. $\alpha\delta - \beta\gamma = 1$. Put

$$f(x) = \prod_{i=0}^{r-1} (x - a_i) .$$

Then $(\gamma x + \delta)^r f(A(x))$ has roots $A^{-1}(a_0),\ldots,A^{-1}(a_{r-1})$ i.e. $a_0,\ldots,a_{r-1}$. Hence $f(x)$ and $(\gamma x + \delta)^r f(A(x))$ differ only by a constant c.

Let x_1,x_2 be parameters such that $\frac{x_1}{x_2} = x$. Define

$$x_2^r f(\frac{x_1}{x_2}) = f(x_1,x_2) \quad . \qquad (1)$$

Then $f(x_1,x_2)$ is a form of degree r (i.e. for any $\lambda \in k$, $f(\lambda x_1, \lambda x_2) = \lambda^r f(x_1,x_2)$) which is invariant under transformations A of G :

Since $A(\frac{x_1}{x_2}) = (\alpha x_1 + \beta x_2)(\gamma x_1 + \delta x_2)^{-1}$, we have $A(x_1,x_2) = (\alpha x_1 + \beta x_2, \gamma x_1 + \delta x_2)$. Furthermore

$$f(x) = c(\gamma x + \delta)^r f(A(x)) \qquad (2)$$

for some $c \in k$. So

$$\begin{aligned} f(x_1,x_2) &= x_2^r f(\frac{x_1}{x_2}) \\ &= x_2^r c(\gamma \frac{x_1}{x_2} + \delta)^r f(A(\frac{x_1}{x_2})) \\ &= c(\gamma x_1 + \delta x_2)^r f(A(\frac{x_1}{x_2})) \\ &= cA(x_2^r) f(A(\frac{x_1}{x_2})) \\ &= cf(A(x_1,x_2)) \qquad (3) \end{aligned}$$

Summing up (cf. [7], §70, p.267): For every orbit we have a (relative) invariant form whose degree is the order of the orbit and whose roots consist of the elements of that orbit.

If G is not cyclic there is more than one such f. We call these f's (as defined by (1)) groundforms of G. We shall need two lemmas about groundforms (cf. [7], §70, p.267,268) :

Lemma A. If some invariant form of G, $F(x_1,x_2)$ say, shares a factor with a groundform $f(x_1,x_2)$, then $f(x_1,x_2)$ divides $F(x_1,x_2)$.

Proof : If $F(x,1)$ and $f(x,1)$ have a root in common, then all roots of f must be roots of F : For by assumption if $A \in G$, then $F(x,1)$ and $F(A(x),1)$ have the same roots. If therefore $F(a_i,1) = 0$, where a_i is a root of $f(x,1)$, and $A(a_i) = a_j$, then $F(A(a_i),1) = F(a_j,1) = 0$. This proves the lemma.

Lemma B. A non-zero invariant form F of G whose degree is lower than the order of G is a product of groundforms (and a constant).

Proof : Clearly the restriction on the degree of F is necessary. Let y_0 be a root of the invariant form $F(x,1)$. Then for all $A \in G$, $A(y_0)$ are roots of $F(x,1) = 0$. Since deg $F < |G|$, not all $A(y_0)$ can be distinct, so for $A_1,A_2 \in G$, $A_1(y_0) = A_2(y_0)$ or $y_0 = A_1^{-1}A_2(y_0)$. This means that y_0 belongs to the fixed-point-set of G. It follows from lemma A that F is divisible by a groundform, and lemma B follows since the same holds for the quotient of this division.

We can rephrase lemma B as follows :

Lemma C. If $F(x_1,x_2)$ is an invariant form of G whose degree is lower than the order of G and F is not repre= sentable (up to a constant) as a product of groundforms, then it must vanish identically.

b) Some Technical Results from Galois Theory

To make our aim more precise we recall the following

Definition : Let F be any skew field and A the group of all its automorphisms. For any subgroup H of A let

$$H' = \{x \in F \mid x^\sigma = x \text{ for all } \sigma \in H\}.$$

H' is called the fixed field of H.
For any subfield E of F let

$$E' = \{\sigma \in A \mid x^\sigma = x \text{ for all } x \in E\}.$$

If E'' = E, then E' is called the Galois group of F over E.

Let K be a skew field with algebraically closed centre k. Let G be a subgroup of $PGL_2(K)$. Then we have an action of G on $K_k(x)$ defined by $f(x) \longmapsto f(\alpha x)$, where $\alpha \in G$, $f(x) \in K_k(x)$. Our task is to find the fixed fields of the action on $K_k(x)$ by the cyclic, dihedral, tetra= hedral, octahedral, and icosahedral groups, these being the only types of finite groups occurring in $PGL_2(K)$, as

demonstrated in chapter 2.

To do this we note that the mapping $K_k(x) \longrightarrow K_k(\alpha x)$ induced by $\alpha \in G$ is an automorphism of $K_k(x)$ over K (i.e. keeping K fixed) which will be of the same order as α. There will be no ambiguity in this chapter in calling this automorphism of $K_k(x)$ α as well. We need a preliminary result which is easily seen to be a weaker version of theorem 3.3.4 in [4].

Theorem. Let G be a finite group of automorphisms of $K_k(x)$ over K. Then

$$[K_k(x) : G']_L = (G : G_0)\,[C : k] \qquad (4)$$

(if either side is finite), where G_0 denotes the group of inner automorphisms in G, and C is the centralizer of G' in $K_k(x)$; $[K_k(x) : G']_L$ is the left degree of $K_k(x)$ over G'; $(G : G_0)$ is the index of G_0 in G.

Now an inner automorphism of $K_k(x)$ induced by $\alpha \in G$ is such that for any $h \in K_k(x)$ we have

$$h(\alpha x) = f^{-1}h(x)f\ , \qquad (5)$$

where $f \in K_k(x)$ is fixed in the the sense that it depends only on α but not on h. In particular (5) holds for $h = x$. Then

$$\alpha x = f^{-1}xf\ . \qquad (6)$$

We may assume without loss of generality that f is

defined and finite and non-zero at $0,1,\infty$: For if f or f^{-1} has a pole at 0,1 or ∞ we only need to change variables to rectify the situation. For instance if f(x) has a pole at x = 0, put x = y - e, where $e \neq 0,1$. Then f(y) has a pole at y = e, and now $\alpha y = f^{-1}(y)yf(y)$, where f satisfies the requirements.

We claim αx has a pole at ∞: For suppose αx is finite at ∞. Since f is non-zero at ∞, f^{-1} will be finite at ∞, so $f\alpha xf^{-1}$ is finite at ∞, a contradiction since x is not finite at ∞, and proving the claim.

Now if

$$\alpha x = (ax + b)(cx + d)^{-1} \qquad (a,b,c,d \in K),$$

then c = 0 since αx has a pole at ∞. Similarly since f and f^{-1} are finite and non-zero at 0, α vanishes at 0 by (6). Hence b = 0. Since α is of finite order it follows by lemma 2.21 that $\alpha(x) = \omega x$ for some $\omega \in k$. Since f is non-zero and finite at 1, we have $\alpha(1) = 1$, so $\omega = 1$. It follows that α is the identity in G and hence that G_0 is trivial.

So $(G : G_0) = |G|$ and (4) becomes

$$\left[K_k(x) : G'\right]_L = |G|\left[C : k\right] \qquad (7)$$

Suppose that $h \in K_k(x)$ generates the fixed field G' of a subgroup G of $PGL_2(K)$. Then for any $\alpha \in G$, $h^\alpha = h$. Hence for any $\sigma \in GL_2(K)$, $h^{\sigma\sigma^{-1}\alpha\sigma} = h^{\alpha\sigma} = h^\sigma$ and so h^σ is contained in the fixed field $(G^\sigma)'$ of $\sigma^{-1}G\sigma$. Since

σ is an automorphism of $K_k(x)$ over K, h^σ must in fact be the generator of $(G^\sigma)'$ in $K_k(x)$. Thus we obtain

Lemma 3.1. Let G be a finite group in $PGL_2(K)$ and assume its fixed field in $K_k(x)$ is of the form $K_k(h)$ for some $h \in K_k(x)$. Then the fixed field of $\sigma^{-1} G \sigma$ for any $\sigma \in GL_2(K)$ is $K_k(h^\sigma)$.

Therefore if we find the (generator of the) fixed field of any one group of a conjugacy class of groups, then we can easily find the fixed field of any other group in that class.

The next proposition shows how our general case can be reduced to the commutative case :

Proposition 3.2. Let G be a finite group in $PGL_2(k)$, where k is the algebraically closed centre of K. Assume $h \in k(x)$ generates the fixed field of G in k(x) over k. Then h generates the fixed field of G in $K_k(x)$ over K, i.e. then $K_k(h)$ is the fixed field of G in $K_k(x)$.

Proof : First we note that h is indeed in the fixed field of G in $K_k(x)$. Let G be of order n, then deg h = n. Let F_0 be the fixed field of G in $K_k(x)$. Then clearly $K_k(h) \subseteq F_0$. Moreover because $h \in k(x)$, the elements $1, x, \ldots, x^{n-1}$ form a left as well as right basis for $K_k(x)$ over $K_k(h)$, so

$$[K_k(x) : K_k(h)]_L = [K_k(x) : K_k(h)]_R = n \quad .$$

Since F_0 is Galois in $K_k(x)$, $[K_k(x) : F_0]_R = [K_k(x) : F_0]_L$. And now we use formula (7) to see that $[K_k(x) : F_0]_L \geq |G| = n$. It follows that we must have $K_k(h) = F_0$.

The proof shows also that $C = k$ in (7), a fact which can be verified directly.

One of the objects in what follows will be to show that all our finite groups meet the condition of proposition 3.2, i.e. that any finite group in $PGL_2(K)$ is conjugate to a group in $PGL_2(k)$.

c) The Cyclic Group of Order n, C_n

Let α be an element of $PGL_2(K)$ and assume $f \in K_k(x)$ belongs to the fixed field of α in $K_k(x)$. Then $f^{\alpha} = f$. Hence $f^{\alpha^i} = f$ for any i. So the fixed field of α is contained in the fixed field of any power α^i of α. In particular this gives

Lemma 3.3. The fixed field in $K_k(x)$ of a cyclic group of automorphisms is that of its generator.

Suppose $\alpha \in PGL_2(K)$ is of finite order n. Then we know that α is conjugate to $x \mapsto axb^{-1}$, where $a^n = b^n = \lambda \in k$. Since k is algebraically closed it follows that $a, b \in k$. Hence α is of form

$$x \longmapsto \omega x , \qquad (8)$$

where $\omega \in k$ is a primitive n-th root of 1. Note that (8) is in fact an element of $PGL_2(k)$. So by lemmas 3.1 and 3.3 and proposition 3.2 we need only find the fixed field of (8) to determine the fixed field of any cyclic group C_n of order n in $PGL_2(K)$.

The next lemma is a consequence of Galois theory and used to form part of the exposition of Galois theory before Dedekind.

Lemma 3.4. Let $\alpha \in PGL_2(k)$ be of finite order n. Then the $f \in k(x)$ such that $f^{\alpha} = f$ are precisely those generated by the elementary symmetric functions in the elements $x, x^{\alpha}, \ldots, x^{\alpha^{n-1}}$.

Proof : Put
$$\begin{aligned} p_1(x) &= x + x^{\alpha} + \ldots + x^{\alpha^{n-1}} \\ &\vdots \\ p_i(x) &= \sigma_i(x, \ldots, x^{\alpha^{n-1}}) \qquad (9) \\ &\vdots \\ p_n(x) &= x\, x^{\alpha} \ldots x^{\alpha^{n-1}} , \end{aligned}$$
where the σ_i are the elementary symmetric functions. Clearly all these p_i satisfy $p_i^{\alpha} = p_i$. Denote by F_0 the fixed field of α in $k(x)$, and by F_1 the subfield of $k(x)$ generated by all the p_i. Then $F_1 \subseteq F_0$ by the last remark. Also $[k(x) : F_0] = n$ since α has order n. And we must have $[k(x) : F_1] \leq n$, hence $F_1 = F_0$.

In particular if any of the p_i is of degree n in x, then this will generate the fixed field of α over k.

More generally if $h \in k(x)$ is any function of degree n which is contained in the fixed field F_0 (in $k(x)$) of α, then $k(h) \subseteq F_0$ and $[k(x) : k(h)] = n = [k(x) : F_0]$, so $k(h) = F_0$. Note that if $h = \frac{g_1}{g_2}$ for some $g_1, g_2 \in k[x]$, then deg h is defined here as max(deg g_1, deg g_2).

For the cyclic group C_n generated by (8) we just need a p_i of (9) to be of degree n. Clearly

$$p_n(x) = x^n \omega^{\Sigma^{n-1} i}$$

is of degree n. So $p_n(x)$, and hence x^n generates the fixed field of C_n over k. It follows that $K_k(x^n)$ is the fixed field C_n' of C_n in $K_k(x)$.

There is an alternative and in some respects more convenient way of describing this fixed field :

Consider the subfield E of $K_k(x)$ generated by all $x^{-i}Kx^i$ ($i \in \mathbb{Z}$) and x^n. This is clearly contained in the fixed field of α (in $K_k(x)$). We recall lemma 5.5.4, p.120 of [4] which says that the subfield of $K_k(x)$ generated by all $x^{-i}Kx^i$ is their field coproduct, $L = \bigcirc_{i \in Z} x^{-i}Kx^i$. L has an automorphism θ: $a \mapsto x^{-1}ax$ for all $a \in K$, so we can form the skew polynomial ring $L[x; \theta]$ (where $qx = xq^{\theta}$ for all $q \in L$), which has field of fractions $L(x; \theta)$, and $L(x; \theta) = K_k(x)$. Now E is generated over L by x^n, so $E = L(x^n; \theta)$. It is clear then that $[L(x; \theta) : L(x^n; \theta)] = n$ and hence $L(x^n) \cong K_k(x^n)$. Since $L(x^n) \subseteq K_k(x^n)$, equality must hold. Summing up,

More generally if $h \in k(x)$ is any function of degree n which is contained in the fixed field F_0 (in $k(x)$) of α, then $k(h) \subseteq F_0$ and $[k(x) : k(h)] = n = [k(x) : F_0]$, so $k(h) = F_0$. Note that if $h = \frac{g_1}{g_2}$ for some $g_1, g_2 \in k[x]$, then deg h is defined here as max(deg g_1, deg g_2).

For the cyclic group C_n generated by (8) we just need a p_i of (9) to be of degree n. Clearly

$$p_n(x) = x^n \omega^{\Sigma^{n-1} i}$$

is of degree n. So $p_n(x)$, and hence x^n generates the fixed field of C_n over k. It follows that $K_k(x^n)$ is the fixed field C_n' of C_n in $K_k(x)$.

There is an alternative and in some respects more convenient way of describing this fixed field :

Consider the subfield E of $K_k(x)$ generated by all $x^{-i}Kx^i$ ($i \in \mathbb{Z}$) and x^n. This is clearly contained in the fixed field of α (in $K_k(x)$). We recall lemma 5.5.4, p.120 of [4] which says that the subfield of $K_k(x)$ generated by all $x^{-i}Kx^i$ is their field coproduct, $L = \bigcirc_{i \in Z} x^{-i}Kx^i$. L has an automorphism θ: $a \mapsto x^{-1}ax$ for all $a \in K$, so we can form the skew polynomial ring $L[x; \theta]$ (where $qx = xq^{\theta}$ for all $q \in L$), which has field of fractions $L(x; \theta)$, and $L(x; \theta) = K_k(x)$. Now E is generated over L by x^n, so $E = L(x^n; \theta)$. It is clear then that $[L(x; \theta) : L(x^n; \theta)] = n$ and hence $L(x^n) \cong K_k(x^n)$. Since $L(x^n) \subseteq K_k(x^n)$, equality must hold. Summing up,

(Suite au prochain page)

Proposition 3.5. The fixed field of the cyclic group with generator $\alpha : x \mapsto \omega x$, where ω is a primitive n-th root of 1, is given by $L(x^n; \theta^n)$, where $L = \bigcirc_{i \in Z} x^{-i} K x^i$ and $\theta : a \mapsto x^{-1}ax$ for all $a \in K$.

Note that $\alpha : x \mapsto \omega x$ has matrix $\begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix}$, where $\varepsilon = \omega^{\frac{1}{2}}$, which is of determinant 1.

Note also that C_n has two orbits, consisting of one fixed point each (cf. chapter 2). So C_n has two ground-forms of degree 1. Since C_n is assumed to have generator as in (8), 0 and ∞ are the two points in the orbits; so one groundform is $f_1 = x_1$ and the other is $f_2 = x_2$.

d) The Dihedral Group of Order 2n, D_{2n}

First we find a normal form for D_{2n}, in $PGL_2(k)$:

Lemma 3.6. Any dihedral group in $PGL_2(K)$ of order 2n is conjugate to the (dihedral) group generated by

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

where $\varepsilon \in k$ is such that ε^2 is a primitive n-th root of 1.

Proof : Suppose $A, B \in PGL_2(K)$ are the generators of any dihedral group of order 2n. Then $A^n, B^2, (AB)^2 \in kI$ (where kI denotes the group of central scalar matrices in $GL_2(K)$). So we know that A can be diagonalized,

say $A = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$, where $\lambda^n = \mu^n \in k$. Since k is algebraically closed it follows that $\lambda, \mu \in k$. But

$$\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} = \lambda^{\frac{1}{2}} \mu^{\frac{1}{2}} \begin{pmatrix} (\lambda \mu^{-1})^{\frac{1}{2}} & 0 \\ 0 & (\mu \lambda^{-1})^{\frac{1}{2}} \end{pmatrix}$$

Note that $\lambda^{\frac{1}{2}}, \mu^{\frac{1}{2}} \in k$ and put $\varepsilon = (\lambda \mu^{-1})^{\frac{1}{2}}$, then A is of the required form.

Let $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then $AB = \begin{pmatrix} \varepsilon a & \varepsilon b \\ \varepsilon^{-1} c & \varepsilon^{-1} d \end{pmatrix}$. Since

$$B^2 = \begin{pmatrix} a^2 + bc & ab + bd \\ ca + dc & cb + d^2 \end{pmatrix} \qquad (10)$$

and $B^2 \in kI$, we have $ab + bd = 0$. Similarly since $(AB)^2 \in kI$ we obtain $\varepsilon^2 ab + bd = 0$. Together these equations give us $(1 - \varepsilon^2)bd = 0$. Now if $\varepsilon^2 = 1$, then $\varepsilon = \pm 1$ and $A \in kI$ which is trivial and we may exclude this case. So either $b = 0$ or $d = 0$. By a similar argument we must have either $a = 0$ or $c = 0$. Since A is invertible we cannot have $a = b = 0$, nor $c = d = 0$. $b = c = 0$ cannot hold since then $AB = BA$ which is im= possible in a dihedral group. Hence $a = d = 0$, i.e. B is of form $\begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}$. Since $B^2 \in kI$ we find that $bc = cb \in k$. Put $T = \begin{pmatrix} b & 0 \\ 0 & 1 \end{pmatrix}$ and note that $T^{-1} A T = A$. Then

$T^{-1}B\,T = \begin{pmatrix} 0 & 1 \\ bc & 0 \end{pmatrix}$. Write $\delta = (bc)^{-\frac{1}{2}}$, then $\delta \in k$ since k is algebraically closed and $\delta\, T^{-1}B\,T = \begin{pmatrix} 0 & \delta \\ \delta^{-1} & 0 \end{pmatrix} = B'$ say. Put $S = \begin{pmatrix} \delta & 0 \\ 0 & 1 \end{pmatrix}$, then $S^{-1}A\,S = A$ and $S^{-1}B'\,S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ as required.

Proposition 3.7. The fixed field of D_{2n} (in the form of lemma 3.6) over K is $K_k(x^n + x^{-n})$, or $L(x^n + x^{-n}; \theta)$, where $L = \bigcirc_{i\in Z} y^{-i}Ky^i$ with $y = x^n + x^{-n}$, and $\theta : a \mapsto y^{-1}ay$ for all $a \in K$.

Proof : Put $A = \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix}$, $B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Then A,B generate D_{2n}. Now the map α of A is $x \mapsto \omega x$, where ω is a primitive n-th root of 1, and the map of B is $\beta : x \mapsto x^{-1}$. We already know the generator of the fixed field of α : it is $g(x) = x^n$. To find the generator of the fixed field of β we look at the symmetric polynomials (9) again. Since β is of order 2 there is only $p_1(x) = x + x^{-1}$ and $p_2(x) = 1$. So $p_1(x)$ generates the fixed field of β. Now every element of D_{2n} has the form $\alpha^i\beta^j$ for i = 0,1,...,n-1 and j = 0,1. Next we have

$$g(x^{\beta}) = (\, g(x)\,)^{\beta}, \qquad (11)$$

where $g(x) = x^n$. Hence

$$p_1(g^{\alpha^i \beta^j}) = p_1(g^{\beta^j})$$

$$= p_1(g^{\beta}) \quad \text{(for if } j = 0, \text{ then } \beta^j = 1, \text{ so we take } j = 1)$$

$$= p_1(g)^{\beta} \quad \text{(by (11))}$$

$$= p_1(g)$$

Therefore $p_1(g(x)) = x^n + x^{-n}$ is the generator of the fixed field of D_{2n} (in the form of lemma 3.6) over k and thus over K.

As before we can write $K_k(x^n + x^{-n})$ in the form $L(y; \theta)$ with $y = x^n + x^{-n}$, $L = \bigcirc_{i \in Z} y^{-i} K y^i$ and θ: $a \mapsto y^{-1}ay$ for all $a \in K$.

To determine the groundforms of D_{2n} we recall from chapter 2 that D_{2n} has three orbits, two consisting of n double fixed points each and the third having two n-tuple fixed points. If D_{2n} is taken in the form of lemma 3.6, then the n-tuple points are 0 and ∞. Thus the groundform corresponding to the third orbit is $f_3 = x_1x_2$. To find the double fixed points (and hence the other two groundforms) we note that

$$\begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon \end{pmatrix}^r \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & \varepsilon^r \\ \varepsilon^{-r} & 0 \end{pmatrix}$$ which has map $x \mapsto \frac{\varepsilon^{2r}}{x}$,

$r = 0,1,\ldots,n-1$. So $\pm \varepsilon^r$ are the 2n elements in the first two orbits. Thus one groundform arises from $(x + 1)(x + \varepsilon) \ldots (x + \varepsilon^{n-1}) = x^n - 1$, hence it is $f_1 = x_1^n - x_2^n$. Similarly the other groundform turns out to be $f_2 = x_1^n + x_2^n$.

e) The Tetrahedral Group, Alt_4

We show first that any tetrahedral group in $PGL_2(K)$ is conjugate to one in $PGL_2(k)$, where k is the algebraically closed centre of K.

Lemma 3.8. Any tetrahedral group in $PGL_2(K)$ is conjugate to the group generated by

$$A = \begin{pmatrix} \frac{i-1}{2} & -\frac{i-1}{2} \\ -\frac{i+1}{2} & -\frac{i+1}{2} \end{pmatrix}, \quad B = \begin{pmatrix} \frac{i-1}{2} & -\frac{i+1}{2} \\ -\frac{i-1}{2} & -\frac{i+1}{2} \end{pmatrix},$$

where $i^2 = -1$.

Proof : The defining relations of Alt_4 are $A^3 = \delta I$, $B^3 = \mu I$, $(AB)^2 = \gamma I$, where $\delta, \mu, \gamma \in k$. We may take $\delta = \mu = 1$ without loss of generality for otherwise we consider the matrices $A\delta^{-\frac{1}{3}}$, $B\mu^{-\frac{1}{3}}$, which is possible since k is algebraically closed.
With δ, μ thus fixed it remains to be seen what γ comes to. Without loss of generality we may take

$A = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^2 \end{pmatrix}$, where $\lambda = -\frac{1}{2}(1 + i\sqrt{3})$ and $\lambda^2 = -\frac{1}{2}(-1 + i\sqrt{3})$ (i.e. $\lambda^2 = \lambda^{-1}$). Then

$$BAB = \gamma A^{-1} = \begin{pmatrix} \gamma\lambda^2 & 0 \\ 0 & \gamma\lambda \end{pmatrix}.$$

Put $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, where $a,b,c,d \in K$, then

$$BAB = \begin{pmatrix} \lambda a^2 + \lambda^2 bc & \lambda ab + \lambda^2 bd \\ \lambda ca + \lambda^2 dc & \lambda cb + \lambda^2 d^2 \end{pmatrix},$$

so equating entries: $bc = \gamma - \lambda^2 a^2$ and $-\lambda^2 a = bdb^{-1}$.

Now $\begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix}^{-1} = \begin{pmatrix} a & 1 \\ bc & bdb^{-1} \end{pmatrix}$

$$= \begin{pmatrix} a & 1 \\ \gamma - \lambda^2 a^2 & -\lambda^2 a \end{pmatrix} \quad (12)$$

Also $$B^{-1} = \begin{pmatrix} \lambda^2 \gamma^{-1} a & \gamma^{-1} \\ 1 - \lambda^2 a^2 \gamma^{-1} & -a\gamma^{-1} \end{pmatrix}$$

and $$B^2 = \begin{pmatrix} a^2 + \gamma - \lambda^2 a^2 & (1-\lambda^2)a \\ (\gamma - \lambda^2 a^2)(1-\lambda^2)a & \gamma - \lambda^2 a^2 + \lambda a^2 \end{pmatrix}.$$

Since $B^{-1} = B^2$, this gives us four equations :

1) $a^2 + \gamma - \lambda^2 a^2 = \lambda^2 a \gamma^{-1}$.

2) $(1 - \lambda^2)a = \gamma^{-1}$

3) $\gamma a - \lambda^2 a^3 - \gamma\lambda^2 a + \lambda a^3 = 1 - \lambda^2 a^2 \gamma^{-1}$

4) $\gamma - \lambda^2 a^2 + \lambda a^2 = -a\gamma^{-1}$.

Of these equations 2) gives us a and it remains to specify γ:

By 1), $$a^2(1 - \lambda^2) + \gamma = \lambda^2 \gamma^{-1} a$$

$$\gamma(1 - \lambda^2)a^2 + \gamma^2 - \lambda^2 a = 0$$

by 2), $$a + \gamma^2 - \lambda^2 a = 0$$

$$a(1 - \lambda^2) + \gamma^2 = 0$$

and $$\gamma^{-1} + \gamma^2 = 0$$

$$\gamma^3 = -1 .$$

Equation 3) is equivalent to equation 2), and equation 4) is equivalent to equation 1). This gives us three choices for γ: $\gamma = -1$, $\gamma = -\lambda$, and $\gamma = -\lambda^2$. Trying $\gamma = -1$ first and hence $a = (1 - \lambda^2)^{-1}$ and substituting these in (12) gives us

$$B = \begin{pmatrix} -\frac{1}{6}(3 + i\sqrt{3}) & 1 \\ -\frac{2}{3} & -\frac{1}{6}(3 - i\sqrt{3}) \end{pmatrix} \qquad (13)$$

Note that this has determinant 1. Put

$$C = \begin{pmatrix} 1 + i & \frac{3}{2} + \sqrt{3} + \frac{\sqrt{3}}{2}i \\ 1 + \sqrt{3} & -\frac{3}{2} + \frac{\sqrt{3}}{2}i \end{pmatrix}$$

and note that C is invertible. Then

$$C^{-1}AC = \begin{pmatrix} \frac{i-1}{2} & -\frac{i-1}{2} \\ -\frac{i+1}{2} & -\frac{i+1}{2} \end{pmatrix}, \quad C^{-1}BC = \begin{pmatrix} \frac{i-1}{2} & -\frac{i+1}{2} \\ -\frac{i-1}{2} & -\frac{i+1}{2} \end{pmatrix}$$

which proves the lemma.

The other two choices of γ offer nothing new : Denote the matrix (13) by B_{-1} and the matrix obtained when $\gamma = -\lambda$ by $B_{-\lambda}$ (note that then $a = (1 - \lambda)^{-1}$).

Then $$\begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix} B_{-\lambda} \begin{pmatrix} 1 & 0 \\ 0 & \lambda^{-1} \end{pmatrix} = B_{-1} \qquad (14)$$

Note that A remains unaffected by this conjugacy trans= formation of Alt_4. This means that Alt_4 with $\gamma = -\lambda$

is conjugate in $PGL_2(k)$ to Alt_4 with $\gamma = -1$ and hence to Alt_4 as given in lemma 3.8. Moreover by (14) and since $\det B_{-1} = 1$, we must have $\det B_{-\lambda} = \lambda^{-2}$.
The case $\gamma = -\lambda^2$ is similar.

Lemma 3.8 and proposition 3.2 reduce the search for the fixed field of Alt_4 to a problem in commutative algebraically closed fields. To settle this problem we need to determine the groundforms of Alt_4 first.

Since Alt_4 has three orbits there must be three groundforms. We recall from chapter 2 that the first orbit contains 6 double fixed points. If we take Alt_4 to be generated by A and B as in lemma 3.8, then $AB = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$ which is of order 2 with map $x \mapsto -x$. So $0, \infty$ are two double fixed points. Next $BA = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ which is of order 2 with map $x \mapsto x^{-1}$. So ± 1 are two more double fixed points. Finally $\begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ which is of order 2 with map $x \mapsto -x^{-1}$. So the last two double points are $\pm i$. Note that these really are double fixed points since Alt_4 only has double and triple fixed points. All these fixed points are obtained as roots of

$$f(x_1,x_2) = x_1x_2(x_1^4 - x_2^4)$$

which is our first groundform, of degree 6.

We observe that all other fixed points are 3-tuple and we recall that there are 4 such points in each of

the two remaining orbits. We start by determining the fixed points of A of lemma 3.8. A has map $x \longmapsto i\,\frac{x-1}{x+1}$, so its fixed points must satisfy $x^2 + (i+1)x - i = 0$. The two solutions are $x_0 = \frac{1}{2}(i+1)(-1-\sqrt{3})$ and $y_0 = \frac{1}{2}(i+1)(-1+\sqrt{3})$. Obviously x_0 and y_0 are not in the same orbit. We determine the orbit of x_0 : Apply AB which has map $x \longmapsto -x$, then $-x_0$ is in the orbit. Next apply $BA \equiv x^{-1}$, then $x_0^{-1} = \frac{1}{2}(i-1)(-1+\sqrt{3})$ is in the orbit. Finally applying $AB^2A \equiv -x^{-1}$ gives us $-x_0^{-1}$. Thus our groundform is

$$(x-x_0)(x+x_0)(x-x_0^{-1})(x+x_0^{-1}) = x^4 - x^2(x_0^{-2}+x_0^2) + 1$$
$$= x^4 - 2i\sqrt{3}\,x^2 + 1 \quad ;$$

or in parameters, $x_1^4 - 2i\sqrt{3}\,x_1^2x_2^2 + x_2^4$.

Denote this groundform by ϕ.

Similarly we find the other groundform,

$$\psi(x) = x^4 + 2i\sqrt{3}\,x^2 + 1 \quad ;$$

or in parameters, $x_1^4 + 2i\sqrt{3}\,x_1^2x_2^2 + x_2^4$.

It is interesting to observe a relation between f, ϕ, ψ:

$$12i\sqrt{3}\,f^2 = \psi^3 - \phi^3 \quad .$$

Next we note that the constant c in (3) turns out to be a cube root ω of 1 in the case of ϕ. We see this

by applying A (of lemma 3.8) to ϕ. Similarly we find that $c = \omega^2$ when A is applied to ψ, $c = \omega^2$ when B is applied to ϕ and $c = \omega$ when B is applied to ψ (explicitly : $\psi(x) = \omega(\frac{1-i}{2}x - \frac{i+1}{2})\psi(Bx)$). Hence we see that by (3) $(\frac{\phi}{\psi})^3$ is a function of degree 12 which is an element of the fixed field of Alt_4. By the remark after lemma 3.4 it will generate the fixed field of Alt_4. Summing up :

Proposition 3.9. If Alt_4 is in the form of lemma 3.8, then its fixed field is

$$K_k\left(\frac{(x^4-2i\sqrt{3}\,x^2+1)^3}{(x^4+2i\sqrt{3}\,x^2+1)^3}\right) .$$

Proof : This follows from lemma 3.2 .

As before we can write this in the form $L(y;\theta)$, where $L = \bigcirc_{i\in Z} y^{-i}Ky^i$ and θ: $a \mapsto y^{-1}ay$ (for all $a \in K$) with $y = (\frac{\phi}{\psi})^3$.

f) The Octahedral Group, Sym_4

Lemma 3.10. Any octahedral group Sym_4 in $PGL_2(K)$ is conjugate to the (octahedral) group generated by

$$A = \begin{pmatrix} \sqrt{i} & 0 \\ 0 & -i\sqrt{i} \end{pmatrix}, \qquad B = \begin{pmatrix} \frac{i+1}{2} & \frac{i-1}{2} \\ \frac{i+1}{2} & -\frac{i-1}{2} \end{pmatrix},$$

where $i^2 = -1$.

Proof : The proof of this lemma is very similar to that of lemma 3.8, so we shall omit some of the details. The generating relations of Sym_4 are $A^4 = \delta I$, $B^3 = \mu I$, $(AB)^2 = \gamma I$. Without loss of generality we may assume that $\delta = \mu = -1$. We have to determine $\gamma \in k$. We may also assume A to be diagonal, i.e. $A = \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix}$, where $\varepsilon^4 = -1$. So $\varepsilon = \sqrt{i}$ and $\varepsilon^{-1} = -i\sqrt{i}$ which is as given in the lemma. Write $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then

$BAB = \gamma A^{-1} = \begin{pmatrix} \gamma\varepsilon^{-1} & 0 \\ 0 & \gamma\varepsilon \end{pmatrix}$, and

$BAB = \begin{pmatrix} \varepsilon a^2 + \varepsilon^{-1}bc & \varepsilon ab + \varepsilon^{-1}bd \\ \varepsilon ca + \varepsilon^{-1}dc & \varepsilon cb + \varepsilon^{-1}d^2 \end{pmatrix}$. This gives us

$bc = \gamma - \varepsilon^2 a^2$ and $bdb^{-1} = -\varepsilon^2 a$. Since

$\begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix} B \begin{pmatrix} 1 & 0 \\ 0 & b^{-1} \end{pmatrix} = \begin{pmatrix} a & 1 \\ bc & bdb^{-1} \end{pmatrix}$, B can be taken to be

of form $B = \begin{pmatrix} a & 1 \\ \gamma - \varepsilon^2 a^2 & -\varepsilon^2 a \end{pmatrix}$. (15)

Then $B^2 = -B^{-1}$ is $\begin{pmatrix} a^2 + \gamma - \varepsilon^2 a^2 & a - \varepsilon^2 a \\ (\gamma - \varepsilon^2 a^2)(1 - \varepsilon^2)a & \gamma - \varepsilon^2 a^2 + \varepsilon a^2 \end{pmatrix}$

i.e. $\begin{pmatrix} -\gamma^{-1}\varepsilon^2 a & -\gamma^{-1} \\ \varepsilon^2 a^2 \gamma^{-1} - 1 & a\gamma^{-1} \end{pmatrix}$. The (1,2) entries give us

$a = -\gamma^{-1}(1 - \varepsilon^2)^{-1}$ and the (1,1) entries give us

$a^2(1-\varepsilon^2) + \gamma = -\gamma^{-1}\varepsilon^2 a$, or $\gamma^3 = -1$. The other entries contain no further information. Choose $\gamma = -1$, then $a = \frac{1}{2}(i+1)$. Substitute this in (15), then

$$B = \begin{pmatrix} \frac{1}{2}(i+1) & 1 \\ -\frac{1}{2} & -\frac{1}{2}(i-1) \end{pmatrix} .$$

Put $\delta = \frac{1}{2}(i-1)$, then

$$\begin{pmatrix} 1 & 0 \\ 0 & \delta^{-1} \end{pmatrix} B \begin{pmatrix} 1 & 0 \\ 0 & \delta \end{pmatrix} = \begin{pmatrix} \frac{1}{2}(i+1) & \frac{1}{2}(i-1) \\ \frac{1}{2}(i+1) & -\frac{1}{2}(i-1) \end{pmatrix}$$

as desired.

As before the other two choices of γ do not give $\det B = 1$.

In determining the invariants of Sym_4 we note first of all that Sym_4 (in the form of lemma 3.10) is generated by $A = \begin{pmatrix} \sqrt{i} & 0 \\ 0 & -i\sqrt{i} \end{pmatrix}$ (which has map $x \mapsto ix$) and Alt_4 (as given by lemma 3.8), i.e. Sym_4 contains Alt_4 as normal subgroup of index 2. Next we recall that Sym_4 has three orbits, one of them consisting of 6 quadruple fixed points. Hence there is a groundform f of Sym_4 of degree 6. Now A has map $x \mapsto ix$ and is of order 4, so $0, \infty$ are quadruple fixed points. Secondly BA^3 has map $x \mapsto \frac{x-1}{x+1}$ and is of order 4, so ± 1 are quadruple fixed points. Finally AB^2 has map $x \mapsto \frac{1+x}{1-x}$ and is of order 4,

so $\pm i$ are quadruple fixed points. Hence

$$f(x_1,x_2) = x_1x_2(x_1+x_2)(x_1-x_2)(x_1+ix)(x_1-ix_2)$$
$$= x_1x_2(x_1^4 - x_2^4)$$

is our first groundform.

Recall the groundforms ϕ and ψ of Alt_4 and put $W = \phi\psi$. This is obviously an invariant of Alt_4, so if W stays invariant under $x \mapsto ix$, then it must be an invariant of Sym_4. But

$$W = x_1^8 + 14x_1^4x_2^4 + x_2^8$$

which is clearly an absolute invariant of $x \mapsto ix$. We claim that W is in fact the second groundform of Sym_4, belonging to the orbit containing 8 triple fixed points: First we note that the third groundform M (belonging to the third orbit containing 12 double fixed points) is of degree 12. So M cannot be a factor of W. On the other hand, since W is a non-zero invariant of Sym_4, by lemma B it must be a product (up to a constant) of groundforms. But f cannot be a factor of W, for if W = fg, then g is an invariant of degree 2 and which is therefore not re= presentable as a product of groundforms. By lemma C this is impossible. It follows that W must itself be a groundform, as claimed.

Similarly we find that $M = \phi^3 + \psi^3$ is an invariant of Sym_4, and hence the third groundform. M is given explicitly by

$$2M = x_1^{12} - 33x_1^8x_2^4 - 33x_1^4x_2^8 + x_2^{12}$$
$$= (x_1^4 + x_2^4)^4 - 36x_1^4x_2^4(x_1^4 + x_2^4) \quad .$$

Write W in the form $W = (x_1^4 + x_2^4)^2 + 12x_1^4x_2^4$, then we obtain the following relation for f,M, and W :

$$W^3 - 4M^2 = 108f^4$$

or
$$\frac{W^3}{f^4} - \frac{4M^2}{f^4} = 108$$

Put $\frac{W^3}{f^4} = V$ and $\frac{4M^2}{f^4} = L$, then we can regard V and L as functions in one variable $x = \frac{x_1}{x_2}$. Clearly V,L are (relative) invariants of Sym_4,i.e. if $A \in Sym_4$, then $V(A(x)) = c_1V(x)$ and $L(A(x)) = c_2L(x)$. But then $V(x) - L(x) = c_1V(x) - c_2L(x) = 108$, hence $c_1 = c_2 = 1$. This means that V,L are in fact absolute invariants of Sym_4. Since both are of degree 24, either will generate the fixed field of Sym_4 over k (and hence over K). Thus we have proved

Proposition 3.11. Let Sym_4 be the octahedral group as given by lemma 3.10. Then the fixed field of Sym_4 in $K_k(x)$ is

$$K_k(V) = K_k\left(\frac{(x^8 + 14x^4 + 1)^3}{x^4(x^4 - 1)^4}\right)$$

As before we can write this in the form $L(V; \theta)$,

where $L = \bigcirc_{i\in Z} V^{-i}KV^{i}$ and θ: $a \mapsto V^{-1}aV$, $V = \frac{W^3}{f^4}$, for all $a \in K$.

g) The Icosahedral Group, Alt_5

First we shall derive a normal form for Alt_5, in $PGL_2(k)$. A presentation for Alt_5 is given by Weber [7], as for the previous groups. We shall here give a different presentation, which arises more naturally from the relations obtained in chapter 2.

Lemma 3.12. Any icosahedral group in $PGL_2(K)$ is conjugate to the (icosahedral) group in $PGL_2(k)$ generated by

$$A = \begin{pmatrix} \varepsilon^{\frac{1}{2}} & 0 \\ 0 & \varepsilon^{-\frac{1}{2}} \end{pmatrix}, \qquad B = \begin{pmatrix} \frac{1}{\varepsilon-1} & \frac{\omega}{\varepsilon-1} \\ \frac{\omega\varepsilon}{\varepsilon-1} & \frac{-\varepsilon}{\varepsilon-1} \end{pmatrix},$$

where ε is a primitive 5-th root of 1 and $\omega = \varepsilon + \varepsilon^{-1}$.

Proof : We may assume that $A^5 = -I$, $B^3 = I$, and $(AB)^2 = \gamma I$ for some $\gamma \in k$. Moreover we may assume that A is in the form given by the lemma.

Put $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Then $BAB = \gamma A^{-1} = \begin{pmatrix} \gamma\varepsilon^{-\frac{1}{2}} & 0 \\ 0 & \gamma\varepsilon^{\frac{1}{2}} \end{pmatrix}$, and

$$BAB = \begin{pmatrix} a^2\varepsilon^{\frac{1}{2}} + bc\,\varepsilon^{-\frac{1}{2}} & ab\,\varepsilon^{\frac{1}{2}} + bd\,\varepsilon^{-\frac{1}{2}} \\ ca\,\varepsilon^{\frac{1}{2}} + dc\,\varepsilon^{-\frac{1}{2}} & cb\,\varepsilon^{\frac{1}{2}} + d^2\varepsilon^{-\frac{1}{2}} \end{pmatrix}$$

So $a^2\varepsilon^{\frac{1}{2}} + bc\,\varepsilon^{-\frac{1}{2}} = \gamma\varepsilon^{-\frac{1}{2}}$ or $bc = \gamma - a^2\varepsilon$, and

$ab\varepsilon^{\frac{1}{2}} + bd\varepsilon^{-\frac{1}{2}} = 0$ or $-a\varepsilon = bdb^{-1}$, assuming $b \neq 0$.

Then we can take B to be of the form

$$\begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & b^{-1} \end{pmatrix} = \begin{pmatrix} a & 1 \\ bc & bdb^{-1} \end{pmatrix} = \begin{pmatrix} a & 1 \\ \gamma - a^2\varepsilon & -a\varepsilon \end{pmatrix}$$

using the above equalities.

We note that this matrix is contained in $PGL_2(k(a))$ and $k(a)$ is a commutative subfield of K. So if we insist on det B = 1, then we must have $\gamma = -1$. Moreover B satisfies its characteristic equation, so

$$B^2 + Ba(\varepsilon - 1) + 1 = 0 \qquad (16)$$

$$B^3 + B^2a(\varepsilon - 1) + B = 0$$

$$I + (1 - Ba(\varepsilon - 1))a(\varepsilon - 1) + B = 0 \quad \text{by (16)}$$

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

In this the (1,2)-entries give $a^2(\varepsilon - 1)^2 - 1 = 0$;

the (1,1)-entries give $1 + a(\varepsilon - 1) - a^3(\varepsilon - 1)^2 - a = 0$.

Hence we have $-1 + a(\varepsilon - 1) = 0$ or $a = \frac{1}{\varepsilon - 1}$.

Substitute for a in B, then

$$B = \begin{pmatrix} \frac{1}{\varepsilon - 1} & 1 \\ -1 - \frac{\varepsilon}{(\varepsilon - 1)^2} & \frac{-\varepsilon}{\varepsilon - 1} \end{pmatrix} = \begin{pmatrix} \frac{1}{\varepsilon - 1} & 1 \\ \frac{\omega^2\varepsilon}{(\varepsilon - 1)^2} & \frac{-\varepsilon}{\varepsilon - 1} \end{pmatrix},$$

where $\omega = \varepsilon + \varepsilon^{-1}$.

$$\begin{pmatrix} 1 & 0 \\ 0 & \frac{\varepsilon - 1}{\omega} \end{pmatrix} B \begin{pmatrix} 1 & 0 \\ 0 & \frac{\varepsilon - 1}{\omega} \end{pmatrix}^{-1} = \begin{pmatrix} \frac{1}{\varepsilon - 1} & \frac{\omega}{\varepsilon - 1} \\ \frac{\omega\varepsilon}{\varepsilon - 1} & \frac{-\varepsilon}{\varepsilon - 1} \end{pmatrix}.$$

Since these transformations leave A unaffected we have proved the lemma.

Summing up the results of lemmas 3.6, 3.8, 3.10, 3.12 we have proved a main result of this chapter, i.e.

Theorem 3.13. Let K be skew field with algebraically closed centre k. Then any finite subgroup of $PGL_2(K)$ is conjugate to one in $PGL_2(k)$.

Next we turn to the invariants of the icosahedral group, Alt_5. Alt_5 has three orbits, one of them consisting of 12 quintuple fixed points, so its groundform f must be of degree 12 in x_1, x_2. Now A of lemma 3.12 has map $x \longmapsto \epsilon x$, where ϵ is a primitive fifth root of 1; and Alt_5 contains $A^4BA^3BA^4B \equiv \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ which has map $x \longmapsto -x^{-1}$. f must have a factor x_1x_2 since 0 and ∞ are the fixed points of $x \longmapsto \epsilon^i x$ $(i = 0,1,\ldots,4)$. To be an invariant of $x \longmapsto \epsilon x$ it is necessary that the remaining factor is expressed by fifth powers in x_1 and x_2 ; and to be an invariant of $x \longmapsto -x^{-1}$ this remaining factor must have summands x_1^{10} and x_2^{10} with different signs. Since a groundform is a homogeneous polynomial in x_1, x_2 it must be of the form

$$f(x_1,x_2) = x_1x_2(x_1^{10} + mx_1^5x_2^5 - x_2^{10}),$$

where m remains to be determined.

Now the points of the orbits other than $0, \infty$ must be the

roots of $x^{10} + mx^5 - 1 = 0$, where $x = \frac{x_1}{x_2}$. So we have

$$x^5 = -\frac{m}{2} \pm \left(\frac{m^2+4}{4}\right)^{\frac{1}{2}} \qquad (17)$$

But A^3B has order 5 with map $x \longmapsto \frac{-\varepsilon^2 x + \varepsilon^3 + \varepsilon}{(\varepsilon + \varepsilon^4)x + 1}$. So its fixed points, which are necessarily quintuple, are the roots of $x^2 + \varepsilon x - \varepsilon^2 = 0$. This has solutions $x = \frac{\varepsilon}{2}(-1 \pm \sqrt{5})$. Raising this to the fifth power enables us to equate the result to (17). In this way we shall obtain m :

We take $x = \frac{\varepsilon}{2}(-1 - \sqrt{5})$:

$$\left(\tfrac{\varepsilon}{2}(-1-\sqrt{5})\right)^5 = -\tfrac{1}{2}(11+5\sqrt{5})$$

So now $$-\tfrac{1}{2}(11+5\sqrt{5}) = \tfrac{1}{2}(-m \pm \sqrt{m^2+4})$$

$$(m-11-5\sqrt{5})^2 = m^2+4$$

$$(-22-10\sqrt{5})m + 242 + 110\sqrt{5} = 0$$

$$m = 11$$

Thus our first groundform is

$$f(x_1, x_2) = x_1 x_2 (x_1^{10} + 11 x_1^5 x_2^5 - x_1^{10}) .$$

To determine the other two groundforms we need Hessian and Jacobian determinants, the relevant facts about which we shall briefly recount :

Let k be a commutative algebraically closed field and let A be a non-singular m x m matrix over k, with

determinant $r \neq 0$. Let $F(x) = F(x_1,\ldots,x_m)$ be a form of degree n. If the variables x are changed to $y_1,\ldots,y_m$ by A, i.e. $x = Ay$, then F(x) becomes G(y) for some form G.

Put $F_{x_i} = \frac{\partial F(x_1,\ldots,x_n)}{\partial x_i}$ and $G_{y_i} = \frac{\partial G(y)}{\partial y_i}$. Then

$$\begin{pmatrix} G_{y_1} \\ \vdots \\ G_{y_n} \end{pmatrix} = A^T \begin{pmatrix} F_{x_1} \\ \vdots \\ F_{x_n} \end{pmatrix}, \qquad (18)$$

where A^T is the transpose of A.

Given m forms $F^{(1)},\ldots,F^{(m)}$, put

$$\Delta = \begin{pmatrix} F^{(1)}_{x_1} & \cdots & F^{(1)}_{x_m} \\ \vdots & & \\ F^{(m)}_{x_1} & \cdots & F^{(m)}_{x_m} \end{pmatrix}$$

and let Δ' be the corresponding matrix for $G^{(1)},\ldots,G^{(m)}$. So $\Delta' = A^T\Delta$ by (18) (and $A^T\Delta = \Delta A$). In particular we have

$$|\Delta'| = r\,|\Delta| \,. \qquad (19)$$

$|\Delta| = \det\Delta$ is the Jacobian determinant of $F^{(1)},\ldots,F^{(m)}$.

Given some form F, put $F_{x_ix_j} = \frac{\partial F(x_1,\ldots,x_m)}{\partial x_i \partial x_j}$ and

$$H = \begin{pmatrix} F_{x_1x_1} & F_{x_1x_2} & \cdots & F_{x_1x_m} \\ \vdots & \vdots & & \vdots \\ F_{x_mx_1} & F_{x_mx_2} & \cdots & F_{x_mx_m} \end{pmatrix}$$

Let H' be the corresponding matrix for G. Then

$$H' = A^T H A \qquad (20)$$

In particular we have $|H'| = r^2|H|$. $|H|$ = det H is called the Hessian determinant of F.

Now we take the form F to be our groundform f and A any matrix of Alt_5, then (f =) F = G and formula (20) shows that the Hessian H of f must be a relative invariant of Alt_5. We find

$$\begin{aligned} H &= f_{x_1x_1} f_{x_2x_2} - (f_{x_1x_2})^2 \\ &= 121\ (-(x_1^{20}+x_2^{20}) + 228(x_1^{15}x_2^5 - x_2^{15}x_1^5) - 494x_1^{10}x_2^{10}) \end{aligned}$$

As before it follows from lemma B that this must in fact be our second groundform. As groundforms are only determined up to a constant we may omit the factor 121.

Next we form the Jacobian T of f and H. By formula (19) this will again be an invariant of Alt_5.

$$\begin{aligned} T &= f_{x_1} H_{x_2} - f_{x_2} H_{x_1} \\ &= 20\ ((x_1^{30}+x_2^{30}) + 522(x_1^{25}x_2^5 - x_1^5x_2^{25}) - 10005(x_1^{20}x_2^{10} + x_1^{10}x_2^{20})) \end{aligned}$$

Again lemma B ensures that this is our third and last groundform; and again we may omit the factor 20. Then we have the following relation between the groundforms :

$$T^2 + H^3 = 1728\ f^5$$

Now groundforms F are relative invariants : $F(x_1,x_2) = cF(x_1,x_2)$, which is (3), and A is an element of Alt_5. Let N be the set of all elements of Alt_5 such that $c = 1$. Clearly $I \in N$. If $A,B \in N$, then $A^{-1}, AB \in N$. So N is a subgroup of Alt_5. Moreover if $A \in N$, then $C^{-1}AC \in N$ for all $C \in Alt_5$. Hence N must be a normal subgroup of Alt_5. But it is a well known fact that Alt_5 is simple, so N is either I or the whole group. It is easily checked that $N \neq I$, e.g. $A^4BA^3BA^4B$ has map $x \longmapsto -x^{-1}$ which is in N. Hence $N = Alt_5$. This means that f,H,T are all absolute invariants of Alt_5.

Put $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in Alt_5$ and $x = \frac{x_1}{x_2}$. Then we recall (2) : $F(x) = (\gamma x + \delta)^{\mu} F(A(x))$, where F stands for f,H, or T. Hence $F(A(x)) = \frac{F(x)}{(\gamma x+\delta)^{\mu}}$ and it follows that $\frac{T^2}{H^3}(A(x)) = \frac{T^2}{H^3}(x)$ i.e. $\frac{T^2}{H^3}$ is an element of degree 60 which belongs to the fixed field of Alt_5. Thus we have proved

Proposition 3.14. Let Alt_5 be the icosahedral group as given by lemma 3.12. Then the fixed field of Alt_5 in $K_k(x)$ is

$$K_k\left(\frac{T^2}{H^3}\right) = K_k\left(\frac{(x^{30}+522x^{25}-10005x^{20}-10005x^{10}+522x^5+1)^2}{(-x^{20}+228x^{15}-494x^{10}-228x^5-1)^3} \right)$$

We may write this in the form $L(\frac{T^2}{H^3}; \theta)$ as usual.

This completes our investigation into the fixed fields of finite subgroups of $PGL_2(K)$ when the centre k of K is algebraically closed.

h) Outlook on the General Case

Finally we make some remarks about fixed fields in the general case, i.e. when k is no longer algebraically closed. To illustrate the problems that arise there we confine our considerations to the case of the cyclic group C_n of order n which is assumed not to contain any quasiconjugations. Without loss of generality C_n can be taken to be diagonal, with generator $\alpha: x \longmapsto axb^{-1}$. Now when k is algebraically closed we have lemma 3.4; and since the generator of the fixed field of C_n must be of degree n, those symmetric functions p_i of lemma 3.4 which have degree less than n must vanish identically. The following result might lead one to expect a similar situation in the general case of C_n (without quasiconjugations).

Proposition 3.15. Let K be a skew field with centre k. Let $a,b \in K$ be such that $a^n = b^n = \lambda$ for some $\lambda \neq 0$ in k and some positive integer n. If a and b are not conjugate, then

$$p_1(x) = \sum_{i=0}^{n-1} a^i x b^{-i} = 0 \quad . \qquad (21)$$

Proof : Consider the automorphism $\alpha: x \longmapsto axb^{-1}$ of $K_k(x)$

over K. By assumption $\alpha^n = 1$, so any conjugate of α has order n. Change variables in $y = axb^{-1}$, say $y' = y - x_0$, $x' = x - x_0$, where $x_0 \in K$ remains to be specified. Then $y' + x_0 = a(x' + x_0)b^{-1} = ax'b^{-1} + ax_0b^{-1}$. Hence $y' = ax'b + ax_0b^{-1} - x_0$. If we pick x_0 such that $ax_0b^{-1} \neq x_0$, then by lemma 1.10, $c = ax_0b^{-1} - x_0$ is a non-trivial solution of (21). Now since a and b are not conjugate, a,b do not have the same minimal equation over k by theorem 0.12. To prove the proposition we need to show that any $c \in K$ is a solution of (21). Thus given $c \in K$ we want x_0 such that $ax_0b^{-1} - x_0 = c$, or $ax_0 - x_0b = cb$. By hypothesis and theorem 0.11 this always has a (unique) solution for x_0. So $y' = ax'b^{-1} + c$ is of finite order for any $c \in K$ and by lemma 1.10 c is a solution of (21).

This means that the first symmetric polynomial p_1 always vanishes; however we are disappointed in our expectations when we consider the second symmetric polynomial (and assume $n > 2$). We have

$$p_2(x) = \sum_{\substack{i,j \leq n-1 \\ i \neq j}} \alpha^i(x)\,\alpha^j(x) = \sum_{\substack{i,j \leq n-1 \\ i \neq j}} a^i x b^{-i} a^j x b^{-j}$$

So $p_2(x) = p_1^2(x) - \sum_{i=0}^{n-1} (a^i x b^{-i})^2$. But we know $p_1(x) = 0$, so $p_2(x) = 0$ if and only if $\sum_{i=0}^{n-1} (a^i x b^{-i})^2 = 0$. As the following example shows, this is not true in general :

Take K to be the real quaternions $\mathbb{H}$. Then $k = \mathbb{R}$.

Take $a = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$, then $a^3 = 1$; and $b^{-1} = j$, then $b^4 = 1$. So a and b are not conjugate. Take x = 1. We can check that $\sum_{n=0}^{11}(-\frac{1}{2} - i\frac{\sqrt{3}}{2})^n j^n = 0$, confirming proposition 3.15, but

$$\sum_{n=0}^{11}((-\frac{1}{2} - i\frac{\sqrt{3}}{2})^n\ j^n)^2 = -6$$

So in the general case there may be functions of degree less than n in the fixed field of C_n.

There also seems no reason to suppose that the fixed field of C_n (without quasiconjugations) is still generated over K by a single element of $K_k(x)$. Finally, though this looks plausible enough, it remains to be proved that the field generated over K by the elementary symmetric functions is indeed the whole fixed field of C_n (this would be the generalization of lemma 3.4). For the reasons given above, the arguments used when k is algebraically closed can no longer be applied in the general case.

References

1. Amitsur, S.A., Finite Subgroups of Division Rings, Trans. Amer. Math. Soc. 80 (1955), p.361-386.

2. Benz, W., Vorlesungen über die Geometrie der Algebren, Springer Verlag Berlin Heidelberg New York (1973)

3. Cohn, P.M., Free Rings and their Relations, LMS monographs No. 2, Academic Press (1971).

4. Cohn, P.M., Skew Field Constructions, LMS Lecture Notes, Cambridge University Press (1977).

5. Hardy,G.H. & Wright,E.M., The Theory of Numbers, 4-th edition, Oxford at the Clarendon Press (1959).

6. Klein, F., Über binäre Formen mit linearen Transformationen in sich selbst, Mathematische Annalen, Bd. 9 (1875/76). Also in : Gesammelte mathematische Abhandlungen, Bd. 2, Verlag von J. Springer (1922).

7. Weber, H., Lehrbuch der Algebra, vol. 2, 3-rd edition, Chelsea Publishing Company, New York.