Available online at www.sciencedirect.com
ScienceDirect
Journal of Algebra 311 (2007) 31–37
JOURNAL OF Algebra
www.elsevier.com/locate/jalgebra

Finite groups of essential dimension one

Arne Ledet

Department of Mathematics and Statistics, Texas Tech University, Lubbock, TX 79409-1042, USA

Received 30 April 2004
Available online 30 January 2007
Communicated by Michel Broué

Abstract

We give necessary and sufficient conditions for a finite group to have essential dimension 1 over an infinite ground field.

Keywords: Galois theory; Essential dimension; Group representations

1. Introduction

Let K be a field, and let G be a finite group. The *essential dimension* of G over K, written $\mathrm{ed}_K\, G$, is then a measure of the complexity of G-extensions over K, i.e., Galois extensions M/L with Galois group $\mathrm{Gal}(M/L) \simeq G$ and $L \supseteq K$. It was introduced by Buhler and Reichstein in [1] and is defined as follows: Given M/L as above, we consider all G-subextensions F/E over K, i.e., G-extensions F/E with $K \subseteq E$, $F \subseteq M$, where the G-action on F is given by restriction from M:

$$\begin{tikzcd}
 & M \arrow[dl, dash] \arrow[dr, dash, "G"] & \\
F \arrow[dr, dash, "G"'] & & L \\
 & E \arrow[ur, dash] \arrow[dr, dash] & \\
 & & K
\end{tikzcd}$$

E-mail address: arne.ledet@ttu.edu.

0021-8693/$ – see front matter © 2007 Elsevier Inc. All rights reserved.
doi:10.1016/j.jalgebra.2006.12.027

The essential dimension of M/L over K is then the minimal possible transcendence degree of such an F over K, and $\mathrm{ed}_K\, G$ is the maximal essential dimension of any G-extension M/L over K. (The essential dimension is always finite, since we can take F to be generated over K by a normal basis for M/L, ensuring that the essential dimension is bounded by the group order.)

Thus, $\mathrm{ed}_K\, G$ is the maximal number of algebraically independent elements that it is necessary to adjoin to K to describe the Galois group action on a G-extension over K.

The simplest case is essential dimension 0, which happens only for the trivial group $\{1\}$.

In this paper, we consider the next case, of essential dimension 1. In [1, Thm. 6.2], it was observed that cyclic groups, and dihedral groups of odd degree, have essential dimension 1 over fields containing all roots of unity. Here, our main result is

Theorem 1. *A finite group G has essential dimension* 1 *over an infinite field K if and only if there exists an embedding $G \hookrightarrow \mathrm{GL}_2(K)$ such that the image of G contains no scalar matrices other than the identity.*

We prove Theorem 1 in Section 3 below. In so doing, we also get a more detailed description of the groups of essential dimension 1 in terms of their Sylow subgroups.

Example 2. The projective special linear group $\mathrm{PSL}(2, 2^n)$ has essential dimension 1 over an infinite field $K \supseteq \mathbb{F}_{2^n}$, since it equals $\mathrm{SL}(2, 2^n)$ and contains no non-trivial scalar matrices. See also [13].

2. Preliminaries

It was observed in [1] that the essential dimension $\mathrm{ed}_K\, G$ for a finite group G over an infinite ground field K is equal to the essential dimension of any *Noether extension* $K(V)/K(V)^G$, where G acts faithfully on a finite-dimensional vector space V, and this action is extended to the rational function field $K(V)$. (In [1], the fields are assumed to have characteristic 0. However, this assumption is not important for the argument. An alternative proof, without assumptions on the characteristic, is given in [8, §8.2].)

Thus, $\mathrm{ed}_K\, G = 1$ if and only if the essential dimension of any Noether extension $K(V)/K(V)^G$ is 1. In that case, a G-extension F/E of transcendence degree 1 sits inside $K(V)/K(V)^G$, and Corollary 8.1.3 in [8] (to a theorem of Roquette [15,16]) gives that F/K is rational, and therefore that G is a subgroup of the projective general linear group $\mathrm{PGL}_2(K)$.

Conversely, if we have G as a subgroup of $\mathrm{PGL}_2(K)$ and can embed $K(t)/K(t)^G$ into a Noether extension, then $\mathrm{ed}_K\, G = 1$. We will refer to such an embedding of G into $\mathrm{PGL}_2(K)$ as a *generic* embedding. It is a consequence of the general theory that $K(t)/K(t)^G$ then embeds into *any* Noether extension $K(V)/K(V)^G$.

Remark. The reason for using the term ‘generic’ is the connection with generic polynomials and generic extensions. However, we will not make use of this connection in this paper. We refer to [10] or [8] for details.

3. Proof of Theorem 1

We consider a finite group G over an infinite field K.

Proof of 'If'. In this case, we have a Noether extension $K(x,y)/K(x,y)^G$, corresponding to the two-dimensional representation $G \hookrightarrow \mathrm{GL}_2(K)$. If $\sigma \in G$ maps to the matrix $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ then $\sigma x = ax + cy$ and $\sigma y = bx + dy$.

Let $t = x/y$. Then

$$\sigma t = \frac{ax+cy}{bx+dy} = \frac{at+c}{bt+d} \in K(t),$$

so G acts on the subfield $K(t)$. This action is faithful, since the non-trivial group elements correspond to non-scalar matrices. Thus, we have a G-extension $K(t)/K(t)^G$ inside $K(x,y)/K(x,y)^G$, and the essential dimension is 1.

This proves 'if' in the theorem. □

Remarks. (1) We note as a consequence of this proof that the induced embedding $G \hookrightarrow \mathrm{PGL}_2(K)$ is generic.

(2) The construction in the proof above is a special case of [9, Prop. 1.1(a)], and can be used more generally to prove that $K(x,y)^G/K$ is rational whenever G is a finite subgroup of $\mathrm{GL}_2(K)$.

To prove 'only if', we first make the following observation: If $G \hookrightarrow \mathrm{PGL}_2(K)$ is a generic embedding, we wish to lift it to an embedding $G \hookrightarrow \mathrm{GL}_2(K)$. Denote the pre-image of G in $\mathrm{GL}_2(K)$ by $\widetilde{G}$. Then we have a group extension

$$1 \to K^* \to \widetilde{G} \to G \to 1,$$

and our goal is to prove that it is split. By standard results from group cohomology (see e.g. [5, Thms. VI.10.3 and VI.16.4]) this is the case for G if and only if it is the case for all Sylow subgroups in G.

Lemma 3. *If G has essential dimension* 1, *every non-trivial subgroup H of G also has essential dimension* 1, *and a generic embedding of G into* $\mathrm{PGL}_2(K)$ *restricts to a generic embedding of H.*

Proof. To prove genericity, it is enough to obtain a Noether extension. But if we have $K(t)/K(t)^G$ contained in $K(V)/K(V)^G$, then $K(t)/K(t)^H$ is contained in $K(V)/K(V)^H$. □

Thus, it is enough to prove the theorem for groups of prime power order. Here, as usual, the prime 2 must be treated separately from the odd primes.

Remark. We are considering subgroups of $\mathrm{PGL}_2(K)$. It may therefore be worth noting the following: If $\operatorname{char} K = p \neq 0$, any finite subgroup G of $\mathrm{PGL}_2(K)$ is also a subgroup of $\mathrm{PGL}(2, p^n)$ for some n. This is because G is defined over a finitely generated $\mathbb{F}_p$-subalgebra R of K, and for a suitably chosen maximal ideal $\mathfrak{m}$ in R we have $G \hookrightarrow \mathrm{PGL}_2(R/\mathfrak{m})$. By the results in [6, II.§7], this means that a subgroup of $\mathrm{PGL}_2(K)$ of odd prime power order is either cyclic (if the prime is not p) or elementary Abelian (if the prime is p). A subgroup of 2-power order is elementary Abelian if $\operatorname{char} K = 2$, and dihedral otherwise (with the Klein Vierergruppe considered a degenerate dihedral group).

On the other hand, if $\operatorname{char} K = 0$, a finite subgroup of $\mathrm{PGL}_2(K)$ must be cyclic or dihedral, or one of S_3, S_4 or A_5, by Klein's classification [11]. Also, an argument similar to the above will work: If G is a finite subgroup of $\mathrm{PGL}_2(K)$ in this case, then the subgroup is defined over a finitely generated $\mathbb{Z}$-algebra, and consequently G is a subgroup of $\mathrm{PGL}(2, p^n)$ for suitable powers p^n of all but finitely many primes p. A subgroup of prime power order is therefore either cyclic or dihedral.

Odd prime power order. Let p be an odd prime.

Lemma 4. *If G is a subgroup of* $\mathrm{PGL}_2(K)$ *of odd order, then G can be lifted isomorphically to a subgroup of* $\mathrm{GL}_2(K)$.

Proof. We first note that G is a subgroup of $\mathrm{PSL}_2(K)$, since the factor group $\mathrm{PGL}_2(K)/\mathrm{PSL}_2(K)$ is an elementary Abelian 2-group. Let $\widehat{G}$ denote the pre-image of G in $\mathrm{SL}_2(K)$. The kernel of the homomorphism $\pi: \widehat{G} \to G$ is either trivial (if $\operatorname{char} K = 2$) or of order 2. In either case, the extension

$$1 \to \ker \pi \to \widehat{G} \to G \to 1$$

is split, since $\gcd(|G|, |\ker \pi|) = 1$, cf. [6, I.§18]. Thus, G lifts to a subgroup $\mathrm{PGL}_2(K)$. □

In particular, any embedding of G into $\mathrm{PGL}_2(K)$ is generic.

Proposition 5. *Let G be a non-trivial p-group, where p is an odd prime, and let K be an infinite field.*

If $\operatorname{char} K \neq p$, *then G has essential dimension* 1 *over K if and only if G is cyclic of order p^n and $\zeta + \zeta^{-1} \in K$, where ζ is a primitive p^nth root of unity.*

If $\operatorname{char} K = p$, *then G has essential dimension* 1 *over K if and only if G is elementary Abelian.*

Proof. Assume first that $\operatorname{char} K \neq p$:

If G is cyclic of order p^n and $\zeta + \zeta^{-1} \in K$, then the matrix

$$A = \begin{pmatrix} \zeta + \zeta^{-1} & -1 \\ 1 & 0 \end{pmatrix}$$

gives a representation of G in $\mathrm{GL}_2(K)$: Since the eigenvalues are ζ and ζ^{-1}, it diagonalises to $\left(\begin{smallmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{smallmatrix}\right)$ over $K(\zeta)$, and for this second matrix it is obvious that it has order p^n and that no non-trivial power is a scalar.

Next, assume that there is an element of order p^n in $\mathrm{PGL}_2(K)$. It lifts to a matrix $A \in \mathrm{GL}_2(K)$ of order p^n by the lemma, meaning that $\mathrm{ed}_K C_{p^n} = 1$. Now, A's eigenvalues must be p^nth roots of unity, and since A is diagonalisable over $K(\zeta)$ by Maschke's Theorem (see e.g. [7, §5.2]), at least one of the eigenvalues must be a primitive p^nth root of unity. Since it is a root of the characteristic polynomial of A, we get that $K(\zeta)/K$ is at most a quadratic extension. This is only possible if $\zeta + \zeta^{-1} \in K$.

If G is not cyclic, it will contain a subgroup isomorphic to $C_p \times C_p$ by [6, Satz III.8.2]. However, $C_p \times C_p$ is not a subgroup of $\mathrm{PGL}_2(K)$, as observed above. It follows that a non-cyclic p-group cannot have essential dimension 1 over K.

For the second part of the proposition, assume that $\operatorname{char} K = p$, and let $G \subseteq \mathrm{PGL}_2(K)$ be a p-group. By Lemma 4, G lifts to a subgroup of $\mathrm{GL}_2(K)$. It is well known that a p-subgroup of $\mathrm{GL}_n(K)$ in characteristic p can be conjugated to consist of upper triangular matrices with 1's in the diagonal, cf. [3] or [12]. In this case, that means matrices of the form $\left(\begin{smallmatrix}1 & a\\ 0 & 1\end{smallmatrix}\right)$. These matrices form a subgroup isomorphic to $(K,+)$, so G must be elementary Abelian. On the other hand, any finite elementary Abelian p-group can be embedded into $(K,+)$, and will therefore have essential dimension 1.

Thus, the only p-groups that have essential dimension 1 in characteristic p are the elementary Abelian p-groups. □

Remarks. (1) If n is an odd number that is not a prime power, and K is a field of characteristic not dividing n, it is still necessary and sufficient for $\mathrm{ed}_K\, C_n = 1$ that the nth cyclotomic field over K is at most a quadratic extension. However, since there will be several subgroups of $\mathbb{Z}_n^*$ of order 2, there will be several possible conditions on K, only one of which has to be satisfied.

For instance: If ζ is a primitive fifteenth root of unity, we get essential dimension 1 for C_{15} over K if $\zeta + \zeta^{-1} \in K$ *or* $\zeta^3, \zeta^5 + \zeta^{-5} \in K$ *or* $\zeta^5, \zeta^3 + \zeta^{-3} \in K$, corresponding to the three subgroups of $(\mathbb{Z}/15)^* \simeq (\mathbb{Z}/3)^* \times (\mathbb{Z}/5)^*$ of order 2. (Note that ζ^3 is a primitive fifth root of unity, and that ζ^5 is a primitive third root of unity.)

(2) One-parameter generic descriptions for cyclic groups of odd order n over $\mathbb{Q}(2\cos\frac{2\pi}{n})$ are considered in [14]. We see that for a prime power n, this ground field is the best possible (i.e., the smallest) in characteristic 0. The same is true for the dihedral groups considered in [4]. On the other hand, the standard condition of Kummer theory that K should contain the primitive nth roots of unity is in fact a little stronger than necessary.

2-power order. Next, we consider the case of a 2-group.

Example 6. Assume that $A \in \mathrm{GL}_2(K)$ represents an element of order 2 in $\mathrm{PGL}_2(K)$. Conjugating if necessary, we may assume

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

and then have

$$A^2 = aI.$$

The induced action on $K(t)$ is $t \mapsto a/t$, from which it is clear that a is a norm in $K(t)/K(t)^{C_2} = K(t)/K(t + a/t)$. If the action is generic, this extension sits inside the Noether extension $K(x,y)/K(u,v)$, where $u = x + y$ and $v = xy$. There, the only elements in K that are norms are the squares, and so a must be a square in K.

Thus, if the action is generic, we can lift it isomorphically to $\mathrm{GL}_2(K)$ by taking $\frac{1}{\sqrt{a}}A$ instead of A.

For instance, the action $t \mapsto 1/t$ is generic for C_2 over all fields (infinite or not). On the other hand, $t \mapsto 2/t$ is not generic over $\mathbb{Q}$.

Proposition 7. *Let G be a 2-group, and let K be an infinite field.*

If $\operatorname{char} K \neq 2$, *then G has essential dimension* 1 *over K if and only if G is cyclic of order 2^n and K contains the 2^nth roots of unity.*

If $\operatorname{char} K = 2$, *then G has essential dimension* 1 *if and only if G is elementary Abelian.*

Proof. First, assume $\operatorname{char} K = 2$. Then a finite elementary Abelian 2-group can be realised by triangular matrices, so it will have essential dimension 1. On the other hand: If G has essential dimension 1, it is a subgroup of $\mathrm{PGL}(2, 2^n)$ for some n, and therefore elementary Abelian.

Next, let $\operatorname{char} K \neq 2$. We have already considered quadratic extensions in Example 6, so we look first at the cyclic group C_{2^n} for $n > 1$, and assume it to be a subgroup of $\mathrm{PGL}_2(K)$.

We must then have a matrix A representing an element of order 2^n in $\mathrm{PGL}_2(K)$, and after conjugating and scaling, we may assume

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

for $\gamma \in K^*$. Also, $A^{2^n} = aI$. Over some extension field, A is diagonalisable (by Maschke's Theorem again), i.e.,

$$A \sim \begin{pmatrix} \sqrt[2^n]{a} & 0 \\ 0 & \zeta \sqrt[2^n]{a} \end{pmatrix},$$

where $\sqrt[2^n]{a}$ is some root of $X^{2^n} - a$, and ζ is a primitive 2^nth root of unity. It follows that $\det A = -\gamma = \zeta(\sqrt[2^n]{a})^2$ and that $\operatorname{Tr} A = 1 = \sqrt[2^n]{a}(1+\zeta)$. Thus,

$$a = \frac{1}{(1+\zeta)^{2^n}} \quad \text{and} \quad \gamma = -\frac{\zeta}{(1+\zeta)^2} = -\frac{1}{\zeta + \zeta^{-1} + 2}.$$

In particular, the 'double cosine' $\zeta + \zeta^{-1}$ is in K. Also,

$$a = -\frac{1}{(\zeta + \zeta^{-1} + 2)^{2^{n-1}}}.$$

If $i = \sqrt{-1} \in K$, then $K(\zeta) = K(\zeta + \zeta^{-1}, i) = K$, so $\zeta \in K$, and A can be rescaled to have order 2^n. In particular, the embedding of C_{2^n} into $\mathrm{PGL}_2(K)$ is generic.

If $i \notin K$ and $\zeta + \zeta^{-1} + 2 = -b^2$ for some $b \in K^*$, we get $a = -1/b^{2^n}$, so by rescaling we can get $A^{2^n} = -I$.

If $i \notin K$, and $\zeta + \zeta^{-1} + 2$ is not minus a square, then the field $K(\xi)$ obtained by adjoining $\xi = \sqrt{\zeta + \zeta^{-1} + 2}$ will not contain i, and in $K(\xi)$ we get $a = -1/\xi^{2^n}$.

In either case, we get a field $K' \supseteq K$ not containing i, over which the element in $\mathrm{PGL}_2(K')$ lifts to a matrix A of order 2^{n+1}.

If the embedding is to be generic, it is necessary that the restricted embedding $C_2 \hookrightarrow \mathrm{PGL}_2(K)$ is generic. By Example 6, this requires that $A^{2^{n-1}}$ can be rescaled to have order 2. As it is, it has order 4, since $A^{2^n} = -I$. Thus, it cannot be generic unless $i \in K'$.

All in all: C_{2^n} has a generic embedding over K if and only if K contains the primitive 2^nth roots of unity.

We must now show that a non-cyclic 2-group G cannot have essential dimension 1. A non-cyclic 2-subgroup of $\mathrm{PGL}_2(K)$ must contain Klein Vierergruppe V_4. But V_4 has essential dimension 2 over any field K of characteristic $\neq 2$, by the results of [2]. (The proof in [1] assumes characteristic 0.)

Hence, a non-cyclic 2-group cannot have essential dimension 1 over a field of characteristic $\neq 2$. □

In both cases, generic embeddings lift to $\mathrm{GL}_2(K)$. Also, if $|G| > 2$ and K contains the $|G|$th roots of unity, any embedding of G into $\mathrm{PGL}_2(K)$ is generic.

Remark. We note that in characteristic $\neq 2$, the condition of Kummer theory is in fact necessary and sufficient for C_{2^n} to allow a one-parameter description.

A complete formulation of Theorem 1 is now

Theorem 8. *An embedding $G \subseteq \mathrm{PGL}_2(K)$ is generic if and only if it lifts isomorphically to $\mathrm{GL}_2(K)$. A necessary condition for this is that the p-Sylow subgroups of G are cyclic for $p \neq \operatorname{char} K$ and elementary Abelian for $p = \operatorname{char} K$. If G has odd order, this condition is also sufficient. If $|G| = 2^e m$ with $e \geqslant 2$ and m odd, it is in addition necessary that $\operatorname{char} K = 2$ or that the primitive 2^eth roots of unity are in K.*

As proved above, the condition for odd p requires that $\zeta + \zeta^{-1} \in K$ when ζ is a primitive pth root of unity.

Acknowledgments

The author would like to thank the referees for various suggestions that resulted in considerable simplifications of the original proofs.

References

[1] J. Buhler, Z. Reichstein, On the essential dimension of a finite group, Compos. Math. 106 (1997) 159–179.

[2] J. Buhler, Z. Reichstein, On Tschirnhaus transformations, in: S.D. Ahlgren, et al. (Eds.), Topics in Number Theory, Kluwer Academic Publishers, 1999, pp. 127–142.

[3] W. Gaschütz, Fixkörper von p-Automorphismengruppen rein-transzendenter Körpererweiteriungen von p-Charakteristik, Math. Z. 71 (1959) 466–468.

[4] K. Hashimoto, K. Miyake, Inverse Galois problem for dihedral groups, in: Dev. Math., vol. 2, Kluwer Academic Publishers, 1999, pp. 165–181.

[5] P.J. Hilton, U. Stammbach, A Course in Homological Algebra, Grad. Texts in Math., vol. 4, Springer-Verlag, 1971.

[6] B. Huppert, Endliche Gruppen I, Grundlehren Math. Wiss., vol. 134, Springer-Verlag, 1967.

[7] N. Jacobson, Basic Algebra II, W.H. Freeman and Company, New York, 1989.

[8] C.U. Jensen, A. Ledet, N. Yui, Generic Polynomials: Constructive Aspects of the Inverse Galois Problem, Math. Sci. Res. Inst. Publ. Ser., vol. 45, Cambridge University Press, 2002.

[9] G. Kemper, A constructive approach to Noether's Problem, Manuscripta Math. 90 (1996) 343–363.

[10] G. Kemper, E. Mattig, Generic polynomials with few parameters, J. Symbolic Comput. 30 (2000) 843–857.

[11] F. Klein, Über binäre Formen mit linearen Transformationen in sich selbst, Math. Ann. 9 (1875/1876) 183–208.

[12] H. Kuniyoshi, Certain subfields of rational function fields, in: Proc. International Symp. on Algebraic Number Theory, Tokyo, Nikko, 1955, pp. 241–243.

[13] A. Ledet, $\mathrm{PSL}(2, 2^n)$-extensions over $\mathbb{F}_{2^n}$, Canad. Math. Bull. 49 (2006) 113–116.

[14] K. Miyake, Linear fractional transformations and cyclic polynomials, Adv. Stud. Contemp. Math. (Pusan) 1 (1999) 137–142.

[15] J. Ohm, On subfields of rational function fields, Arch. Math. 42 (1984) 136–138.

[16] P. Roquette, Isomorphisms of generic splitting fields of simple algebras, J. Reine Angew. Math. 214/215 (1964) 207–226.