ESSENTIAL DIMENSION

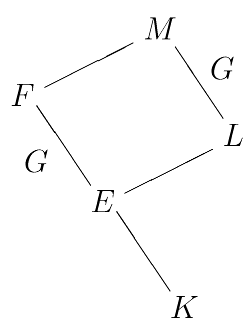
ARNE LEDET

Abstract. We give a brief survey of the theory of essential dimension for a finite group over a field.

Introduction

Let K be an *infinite* field,[1] and let G be a finite group. A *G-estension over K* is then a Galois extension M/L with $\mathrm{Gal}(M/L) \simeq G$ and $L \supseteq K$. For example, K can be the prime field in some characteristic p, and M/L is then simply a G-extension in characteristic p.

The question that motivates the concept of essential dimension is then the following: How 'complex' is the extension M/L really? That is, how large a G-extension do we need to capture the structure of M/L? After all, if we take an intermediate field F, $K \subseteq F \subseteq M$, on which G acts faithfully, and let $E = F^G$, we have a diagram



and M/L is simply the scalar extension to L of F/E. Thus, everything about the Galois structure of M/L is given by F/E.

As our measure of how large an extension field of K is, we take the transcendence degree. Thus, the question is: What is the minimal transcendence degree $\mathrm{trdeg}_K F$ of an intermediate field F as above?

Certainly, this minimum is less that the order $|G|$ of the group G, since we can let $F = K(\{\sigma\theta\}_{\sigma \in G})$, where $\{\sigma\theta\}_{\sigma \in G}$ is a normal basis for M/L with $\sum_{\sigma \in G} \sigma\theta = 1$.

[1] It is not necessary for the definition that K be infinite, but as some of the proofs depend on it, it is easier to assume it once and for all.

We define the *essential dimension* of M/L over K, $\operatorname{ed}_K(M/L)$, to be this minimal transcendence degree.

This concept was introduced by Buhler and Recihstein in [B&R1, 1997].

Example. The trivial group 1 has essential dimension 0, since we can pick $F = K$. It is also the *only* group with essential dimension 0, since $\operatorname{ed}_K G = 0$ means that *every* G-extension over K is in fact induced by a G-extension that is algebraic over K.

Example. The cyclic group C_2 of order 2 has essential dimension 1, since any C_2-extension is the splitting field of a polynomial of the form $X^2 - a$ or $X^2 - X - a$, and we can let $E = K(a)$.

Example. The cyclic group C_3 of order 3 and the symmetric group S_3 on three letters both have essential dimension 1: An extension with Galosi group C_3 or S_3 is the splitting field of a cubic polynomial $X^3 + aX^2 + bX + c$. By a standard transformation, we can get $a = 0$, and if $b \neq 0$ we can rescale to get a polynomial $X^2 + bX + b$. Thus, the extension is the splitting field of a polynomial $X^3 - a$ or $X^3 + aX + a$.

For the groups in the above examples, computing the essential dimension directly is easy. However, in general this is an impractical approach.

Definition. Let $G \hookrightarrow \mathrm{GL}_K(V)$ be a faithful linear representation of G over K.

We denote the *commutative tensor algebra* for V over K by $K[V]$. (Thus, $K[V]$ is a polynomial ring in $\dim_K V$ variables, in which the space of homogeneous first-order polynomials has been identified with V.) The field of fractions for $K[V]$ is denoted by $K(v)$.

The G-action on V extends to an action on $K(V)$, and we will refer to a G-extension over K of the form $K(V)/K(V)^G$ as a *linear Noether extension.*

Theorem. *Let $K(V)/K(V)^G$ be a linear Noether extension. Then*

$$\operatorname{ed}_K G = \operatorname{ed}_K(K(V)/K(V)^G).$$

For a proof, see [B&R1] or [JL&Y].

In particular: If G has a faithful representation of degree n, then $\operatorname{ed}_K G \leq n$. And if the image of G has trivial intersection with the scalars, then $\operatorname{ed}_K G \leq n - 1$.

Example. If $\operatorname{char} K \neq 2$, then C_2 has a one-dimensional representation. If $\operatorname{char} K = 2$, the matrix $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ has order 2, and gives a representation without scalars. Thus, $\operatorname{ed}_K C_2 = 1$.

The matrix $\left(\begin{smallmatrix} 0 & 1 \\ -1 & -1 \end{smallmatrix}\right)$ has order 3 over any field, and gives a representation with no scalars. Therefore, $\operatorname{ed}_K C_3 = 1$.

Example. If $\operatorname{char} K = p$, then matrices of the form $\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$ provide a two-dimensional scalar-free representation of the elementary Abelian group C_p^n. Therefore,

$$\operatorname{ed}_K C_p^n = 1.$$

Example. If $\mathbb{F}_{2^n} \subseteq K$, then $\mathrm{PSL}(2, 2^n) \hookrightarrow \mathrm{GL}_2(K)$ is a two-dimensional scalar-free representation, and so

$$\operatorname{ed}_K \mathrm{PSL}(2, 2^n) = 1.$$

For instance, the alternating group $A_5 = \mathrm{PSL}(2, 4)$ has essential dimension 1 over $K \supseteq \mathbb{F}_4$.

Another consequence of the Theorem is

Corollary. *If H is a subgroup of G, then $\operatorname{ed}_K H \leq \operatorname{ed}_K G$.*

The reason is simply that any representation of G restricts to a representation of H.

Also, we get

Corollary. $\operatorname{ed}_K(G \times H) \leq \operatorname{ed}_K G + \operatorname{ed}_K H$.

This is clear, since a representation of $G \times H$ is just a representation of G *and* a representation of H.

We not necessarily have equality in this last Corollary: Consider the cyclic groups C_2 and C_3 over the field $\mathbb{C}$ of complex numbers. They both have essential dimension 1, and so does their product $C_2 \times C_3 = C_6$, by Kummer theory.

However, we have the following result, due to Buhler and Reichstein:

Proposition. *Let p be a prime, and let K be a field of characteristic $\neq p$ containing the primitive p^{th} roots of unity. Then*

$$\operatorname{ed}_K(G \times C_p) = \operatorname{ed}_K G + 1$$

for any p-group G.

In [B&R1], a more general result is proved, assuming $\operatorname{char} K = 0$, but a closer look at the proof will show that it gives the Proposition above as well.

Corollary. *If $\operatorname{char} K \neq 2$, then $\operatorname{ed}_K C_2^n = n$.*

Conjecture. *If G and H are p-groups and $\operatorname{char} K \neq p$, then*

$$\operatorname{ed}_K(G \times H) = \operatorname{ed}_K G + \operatorname{ed}_K H.$$

Very little is known about lower bounds for the essential dimension, and most of it comes from using the above Corollary on a subgroup. For instance:

Example. Let $\operatorname{char} K \neq 2$. The largest elementary Abelian 2-subgroup of the symmetric group S_n, $n \geq 2$, has order $2^{\lfloor n/2 \rfloor}$, and so

$$\lfloor n/2 \rfloor \leq \operatorname{ed}_K S_n.$$

For $n = 4$, this gives us $\operatorname{ed}_K S_4 = 2$, since a quartic polynomial can be rewritten as $X^4 + aX^3 + bX + b$ by suitable transformations.

For $n \geq 5$, we get an upper bound of $n - 3$ by standard methods: Consider S_n as acting on $K(x_1, \dots, x_n)$, and take the usual cross-ratios to get a subfield of transcendence degree $n-3$ with a faithful S_n-action. Thus, for $n \geq 5$ we get

$$\lfloor n/2 \rfloor \leq \operatorname{ed}_K S_n \leq n - 3.$$

In particular, $\operatorname{ed}_K S_5 = 2$ and $\operatorname{ed}_K S_6 = 3$.

For $n \geq 7$, the exact value of $\operatorname{ed}_K S_n$ is not known.

Example. If $\operatorname{char} K \neq 2$, then $\operatorname{ed}_K A_5 = 2$, since $C_2^2 \subseteq A_5 \subseteq S_5$. In characteristic 2, this is not necessarily true, as we have seen.

Example. Let $q > 2$ be a prime power, and assume that $\mathbb{F}_q \subseteq K$. Then

$$\operatorname{ed}_K \operatorname{GL}(n, q) = n.$$

For: Let p be a prime divisor of $q - 1$. Then $\operatorname{ed}_K C_p^n = n$ by the above Proposition, and $\operatorname{GL}(n, q)$ contains a subgroup isomorphic to C_p^n, namely the diagonal matrices with p^{th} roots of unity in the diagonal. On the other hand, $\operatorname{GL}(n, q)$ clearly has an n-dimensional representation.

A very rough lower bound is proved in [Le4]:

Result. *Let G be a non-trivial finite group. Then* $\operatorname{ed}_K G = 1$ *if and only if G has a faithful two-dimensional scalar-free representation.*

Thus, the examples above of groups with essential dimension 1 were all 'typical'.

Example. $\operatorname{ed}_{\mathbb{Q}} C_4 = 2$, since C_4 has a two-dimensional representation over $\mathbb{Q}$, but not one without scalars. (Specifically: If A is a 2×2 matrix over $\mathbb{Q}$ of order 4, it is a root both of $X^4 - 1 = (X^2 + 1)(X + 1)(X - 1)$ and its own characteristic polynomial, and therefore also of the greatest common divisor of these two polynomials. This greatest common divisor cannot be $X - 1$, $X + 1$ or $X^2 - 1$, since A has order 4, so it must be $X^2 + 1$, meaning that $A^2 = -1$.)

Example. $\mathrm{ed}_{\mathbb{Q}} C_5 = 2$, since $C_5 \subseteq S_5$, and $\mathrm{GL}_2(\mathbb{Q})$ has no elements of order 5.

Example. $\mathrm{ed}_{\mathbb{Q}} C_6 = 2$, since a 2×2 matrix over $\mathbb{Q}$ of order 6 must have third power -1, meaning that there is no scalar-free representation.

It is easy to see that $\mathrm{GL}_2(\mathbb{Q})$ contains no elements of order ≥ 7, and therefore (using the above examples) that the only groups with essential dimension 1 over $\mathbb{Q}$ are C_2, C_3 and S_3.

To complement the result that $\mathrm{ed}_K H \leq \mathrm{ed}_K G$ when $H \subseteq G$, we mention that

$$\mathrm{ed}_K G \leq [G : H]\, \mathrm{ed}_K H,$$

(provided of course that $H \neq 1$,) i.e.,

$$\frac{\mathrm{ed}_K G}{|G|} \leq \frac{\mathrm{ed}_K H}{|H|}.$$

So far, this result has not proved particularly useful. It is also a very crude bound on $\mathrm{ed}_K G$: Consider the case $G = \mathrm{GL}(n,q)$ and $H = C_2^n$ above. Here, the two groups have the same essential dimension, although

$$[G : H] = \frac{(q^n - 1)(q^{n-1} - 1)\cdots(q-1)q^{n(n-1)/2}}{2^n},$$

which will tend to be quite large.

A related result is: Let L/K be a finite Galois extension. Then

$$\mathrm{ed}_K G \leq [L : K]\, \mathrm{ed}_L G$$

for any finite group G.

Example. $\mathrm{ed}_{\mathbb{Q}} C_n \leq \varphi(n)$, where φ is the Euler φ-function, since we can let L be the n^{th} cyclotomic field. We will lower this bound significantly below.

On the other hand, we clearly have $\mathrm{ed}_L G \leq \mathrm{ed}_K G$ for *any* field extension L/K.

Cyclic groups over the rational numbers

As a special case, let us look at cyclic groups C_n over the field $\mathbb{Q}$ of rational numbers. By the Chinese Remainder Theorem, we obviously have

$$\mathrm{ed}_{\mathbb{Q}} C_n \leq \mathrm{ed}_{\mathbb{Q}} C_{p_1^{e_1}} + \ldots \mathrm{ed}_{\mathbb{Q}} C_{p_r^{e_r}},$$

when $n = p_1^{e_1} \cdots p_r^{e_r}$ is the prime factorisation of n.

Generalising a unpublished result by Buhler and Reichstein, that in turn is based on an idea by H. W. Lenstra, the following is proved in [Le1]:

Theorem. *Let $q = p^n$ be a prime power, and let K be a field of characteristic $\neq p$. Let $K_q = K(\mu_q)$ denote the q^{th} cyclotomic extension of K, and let $G_q = \mathrm{Gal}(K_q/K)$. Then $|G_q| = dp^e$, where $d \mid p-1$ and $e \neq n-1$, and G_q acts in a natural way on the cyclic group C_q. In this case,*

$$\mathrm{ed}_K(C_q \rtimes G_q) \leq \varphi(d)p^e,$$

where φ is the Euler φ-function.

Corollary. *Let $q = p^n$ be a prime power. Then*

$$\mathrm{ed}_{\mathbb{Q}}\, C_q \leq \varphi(p-1)p^{n-1}.$$

Example. $\mathrm{ed}_{\mathbb{Q}}\, C_7 = 2$.

The Corollary gives the lowest known bounds for $\mathrm{ed}_{\mathbb{Q}}\, C_q$. Note, however, that the bound for C_q is exactly the one we get from $\mathrm{ed}_{\mathbb{Q}}\, C_p$ by applying the last result in the previous section: If G has order p^n, then $\mathrm{ed}_{\mathbb{Q}}\, G \leq \varphi(p-1)p^{n-1}$. Thus, if it is possible to improve the bound for some C_p (or C_{p^e}), it will automatically improve the bounds for all higher powers of p as well.

Of course, we get the same upper bound for $\mathrm{ed}_{\mathbb{Q}}\, D_q$, where D_q is the dihedral group of degree q (and order $2q$). And since $D_{mn} \hookrightarrow D_m \times D_n$, we in fact get the same bound for all dihedral groups.

Example. $\mathrm{ed}_{\mathbb{Q}}\, D_4 = \mathrm{ed}_{\mathbb{Q}}\, D_5 = \mathrm{ed}_{\mathbb{Q}}\, D_6 = \mathrm{ed}_{\mathbb{Q}}\, D_7 = 2$.

Conjecture. $\mathrm{ed}_{\mathbb{Q}}\, C_n = \mathrm{ed}_{\mathbb{Q}}\, D_n$.

Conjecture. *If* $\mathrm{char}\, K \nmid 2n$ *and n is odd, then* $\mathrm{ed}_K\, C_n = \mathrm{ed}_K\, D_n$.

Note that this last claim is not necessarily true for even n: In that case, $C_2^2 \subseteq D_n$, so $\mathrm{ed}_K\, D_n \geq 2$, whereas $\mathrm{ed}_K\, C_n$ can be 1 (if, for instance, K contains the primitive n^{th} roots of unity). See [H&M] and [Mi] for a description of the situation when $\mathrm{ed}_K\, C_n = \mathrm{ed}_K\, D_n = 1$.

p-Groups in characteristic p

Now, let $\mathrm{char}\, K = p$ be a prime, and assume G to be a p-group. In this situation, $\mathrm{ed}_K\, G$ turns out to be surprisingly small: We have already seen that $\mathrm{ed}_K\, C_p^n = 1$ for all n.

Example. $\mathrm{ed}_K\, C_{p^n} \leq n$, since any C_{p^n}-extension M/L over K can be written as $M = L(\mathbf{w})$, where $\mathbf{w}$ is an n-dimensional Witt vector, and

$\sigma\mathbf{w} = \mathbf{w} + 1$ when σ is a chosen generator for C_{p^n}. Therefore, we can let $F = K(\mathbf{w})$.

Trivially, $\operatorname{ed}_K C_p = 1$, and since $\mathrm{GL}_2(K)$ contains no elements of order p^2, we must have $\operatorname{ed}_K C_{p^2} = 2$.

Conjecture. $\operatorname{ed}_K C_{p^n} = n$.

A proof of this conjecture would provide a valuable lower bound of the essential dimension of a p-group. It would also demonstrate that Witt vectors are the 'most economical' way of describing C_{p^n}-extensions in characteristic p.

A classical result by Witt (see [Wi]) says that if N is a normal subgroup of the p-group G, contained in the Frattini subgroup $\Phi(G)$, then any G/N-extension L/K in characteristic p can be extended to a G-extension M/K. It follows in particular that $\operatorname{ed}_K(G/N) \leq \operatorname{ed}_K G$ (a result that is conjecturally false in general), and that we can get a bound on $\operatorname{ed}_K G$ by looking at how many extra parameters we need to introduce in constructing M on top of L.

In the case where N is elementary Abelian, we only need one parameter, and so we get the following result from [Le3]:

Proposition. *Let N be an elementary Abelian subgroup of $\Phi(G)$, and assume $N \lhd G$. Then*

$$\operatorname{ed}_K(G/N) \leq \operatorname{ed}_K G \leq \operatorname{ed}_K(G/N) + 1.$$

Since we can certainly always pick N to be cyclic of order p, we have in particular:

Corollary. *If $|\Phi(G)| = p^e$, then $\operatorname{ed}_K G \leq e + 1$.*

Thus, unconditionally, we have $\operatorname{ed}_K G \leq n$ when $|G| = p^n$.

Example. Let A be an Abelian p-group of exponent p^n. Then $\operatorname{ed}_K A \leq n$.

Example. If $\operatorname{char} K = 2$, then $\operatorname{ed}_K D_{2^n} \leq n$.

It is also possible to obtain low bounds for some groups that are 'almost p-groups', namely semi-direct products $C_{p^n} \rtimes C_d$, where $d \mid \varphi(p^n)$, and C_d acts in the natural way on C_{p^n}. This is done by means of Witt vectors again: As is shown in [Le2], a $C_{p^n} \rtimes C_d$-extension M/L in characteristic p can be written as $M = L(\mathbf{w})$, where $\mathbf{w}$ is an n-dimensional Witt vector, and the Galois action is given by $\sigma\mathbf{w} = \mathbf{w} + 1$ and $\tau\mathbf{w} = a\mathbf{w}$, with σ being a generator for C_{p^n}, τ a generator for C_d, and $a \in \mathbb{Z}_{p^n}^*$ an element of order d. Thus,

$$\operatorname{ed}_K(C_{p^n} \rtimes C_d) \leq n.$$

Example. $\mathrm{ed}_K\, D_{p^n} \leq n$.

References

[B&R1] J. Buhler & Z. Reichstein, *On the essential dimension of a finite group*, Compositio Mathematica **106** (1997), 159–179.

[H&M] K. Hashimoto & K. Miyake, *Inverse Galois problem for dihedral groups*, Developments in Mathematics **2**, Kluwer Academic Publishers, 1999, 165–181.

[JL&Y] C. U. Jensen, A. Ledet & N. Yui, *Generic Polynomials: Constructive Aspects of the Inverse Galois Problem,*, MSRI Publication Series 45, Cambridge University Press, 2002.

[Le1] A. Ledet, *On the essential dimension of some semi-direct products*, Can. Math. Bull. **45** (2002), pp. 422–427.

[Le2] ______, *On p-groups in characteristic p*, in 'Algebra, Arithmetic and Geometry with Applications' (eds. C .Christensen, G. Sundaram, A. Sathaye & C. Bajaj), Springer-Verlag, 2004, pp. 591–600.

[Le3] ______, *On the essential dimension of p-groups*, in 'Galois Theory and Modular Forms' (eds. K. Hashimoto, K. Miyake & H. Nakamura), Developments in Mathematics 11, Kluwer Academic Publishers, 2004, pp. 159–172.

[Le4] ______, *On groups with essential dimension one*, preprint, 2004.

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

[Wi] E. Witt, *Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung* p^f, J. Reine Angew. Math. **174** (1936), 237–245.

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

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