Canad. Math. Bull. Vol. **45** (3), 2002 pp. 422–427

On the Essential Dimension of Some Semi-Direct Products

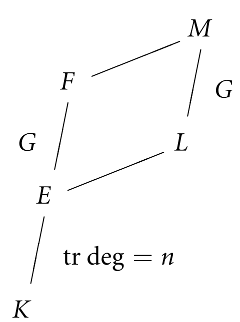
Arne Ledet

Abstract. We give an upper bound on the essential dimension of the group $\mathbb{Z}/q \rtimes (\mathbb{Z}/q)^*$ over the rational numbers, when q is a prime power.

1 Introduction

Let K be an infinite field, let L be an extension field of K, and let M/L be a finite Galois extension with Galois group $G = \mathrm{Gal}(M/L)$ (a G-*extension*). The *essential dimension* of M/L over K, denoted $\mathrm{ed}_K(M/L)$, is then the minimal transcendency degree of a subextension F/K of M/K such that G acts faithfully on F, *cf.* [B&R1, Section 2].

In other words: The essential dimension $\mathrm{ed}_K(M/L)$ is n, if there exists a G-extension F/E with $K \subseteq E \subseteq L$, $\mathrm{tr\,deg}_L\, E = n$ and $M = F \otimes_E L$, and no such extension of transcendency degree $< n$.



It is clear that the essential dimension is finite: Let $\theta \in M$ be a primitive element for M/K, and look at $K(\{\sigma\theta\}_{\sigma\in G})$. It has transcendency degree $\leq |G|$, and G acts faithfully. Thus, $\mathrm{ed}_K(M/L) \leq |G|$.

The concept of essential dimension was introduced by Buhler and Reichstein in [B&R1] as a measure of how many algebraically independent parameters are needed to describe M/L. In their paper, they proved various properties of $\mathrm{ed}_K\, G$, of which we will need the following:

Received by the editors October 31, 2000.
AMS subject classification: 12F10.

Results (a) Let V be a finite-dimensional K-vector space, and let $G \hookrightarrow \mathrm{GL}_K(V)$ be a faithful linear representation. Then the essential dimension of $K(V)/K(V)^G$ over K is greater than or equal to $\mathrm{ed}_K(M/L)$ for *all* G-extensions M/L with $K \subseteq L$. In particular, all faithful linear representations give rise to G-extensions of the same essential dimension, which we will call the *essential dimension of G over K*, denoted $\mathrm{ed}_K\, G$.

(b) If H is a subgroup of G, then $\mathrm{ed}_K\, H \leq \mathrm{ed}_K\, G$.

It follows that $\mathrm{ed}_K\, G \leq n$ if G has a faithful linear representation of degree n.

By the result of [O] (*cf.* also [Ro]) and Lüroth's Theorem, a subextension of transcendency degree 1 in a rational field extension $K(x_1, \ldots, x_n)/K$ is rational. It follows that the essential dimension of a group G over K cannot be 1 unless G is isomorphic to a subgroup of the projective general linear group $\mathrm{PGL}_2(K)$. This, however, is not a sufficient condition: By [B&R1, Corollary 5.5], the Klein Vierergruppe V_4 has essential dimension 2 over any field of characteristic 0, even though it *is* a subgroup of $\mathrm{PGL}_2(\mathbb{Q})$.

The main result of this paper is the following Theorem, which generalises an unpublished result of Buhler and Reichstein [B&R2]:

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

$$\mathrm{ed}_{\mathbb{Q}}\big(\mathbb{Z}/q \rtimes (\mathbb{Z}/q)^*\big) \leq \varphi(p-1)p^{n-1},$$

where φ is the Euler φ-function.

In [B&R2], the Theorem (and more generally the corollary in Section 2 below) is proved for the cyclic group $\mathbb{Z}/q$, rather than the semi-direct product. For a cyclic group of prime order, the result is implicit in the work of Hendrik Lenstra.

The proof we give below is a modification of Buhler and Reichstein's argument, which in turn is based of Lenstra's ideas. In fact, their argument can be obtained simply by removing all references to τ in our proof.

Example Let $q = 7$. Since $\mathrm{ed}_{\mathbb{Q}}\, C_7 > 1$, we get

$$\mathrm{ed}_{\mathbb{Q}}\, C_7 = \mathrm{ed}_{\mathbb{Q}}\, D_7 = \mathrm{ed}_{\mathbb{Q}}\, F_{21} = \mathrm{ed}_{\mathbb{Q}}\, F_{42} = 2,$$

where D_7 is the dihedral group of degree 7 (and order 14) and F_{21} and F_{42} are the Frobenius groups of order 21 and 42, respectively.

2 Proof of the Theorem

Let p be a prime, and let $q = p^n$ be a power of p. Also, let K be an infinite field of characteristic $\neq p$, and assume that the q-th cyclotomic extension K_q/K is cyclic of degree D.

We denote by κ a generator for the Galois group $G_q = \mathrm{Gal}(K_q/K)$. Thus, κ is given by $\kappa\zeta = \zeta^f$ for ζ in the group μ_q of q-th roots of unity, where $f \in \mathbb{Z}$ is some primitive D-th root of unity modulo q. The group we are interested in is then $C_q \rtimes C_D$, where a generator τ of C_D acts on C_q as $\rho \mapsto \rho^f$. We let σ be a generator for C_q.

In order to bound $\mathrm{ed}_K(C_q \rtimes C_D)$ from above, we may use any faithful linear representation of it over K. We obtain such a representation as follows:

Let $\mathbf{x} = (x_\zeta)_{\zeta \in \mu_q}$ be a set of indeterminates indexed by μ_q, and let $C_q \rtimes C_D$ act on the function field $K_q(\mathbf{x})$ by

$$\sigma x_\zeta = \zeta x_\zeta \text{ and } \tau x_\zeta = x_{\kappa\zeta}, \quad \zeta \in \mu_q,$$

with the action understood to be trivial on K_q. Clearly, this gives a faithful $C_q \rtimes C_D$-action, although over K_q rather than K.

Next, extend the action of G_q to $K_q(\mathbf{x})$ by

$$\kappa x_\zeta = x_{\kappa\zeta}, \quad \zeta \in \mu_q.$$

(*i.e.*, κ and τ acts identically on the indeterminates.) Then

$$\sigma\tau = \tau\sigma^f, \quad \sigma\kappa = \kappa\sigma \quad \text{and} \quad \tau\kappa = \kappa\tau,$$

meaning that $G_q \times (C_q \rtimes C_D)$ acts on $K_q(\mathbf{x})$. It is easily seen that this action is in fact faithful.

By the Invariant Basis Lemma (see *e.g.* [Sh, App., Section 3] or [K&M, Lemma 5]), the K_q-vector space $\sum_{\zeta \in \mu_q} K_q x_\zeta$ has a G_q-invariant basis $\mathbf{s} = (s_1, \dots, s_D)$, and $C_q \rtimes C_D$ acts linearly on $K(\mathbf{s}) = K(\mathbf{x})^{G_q}$.

To produce a subfield of $K(\mathbf{s})$ of low transcendency degree on which $C_q \rtimes C_D$ acts faithfully, we make use of *lattices*: For a given finite group G, a G-*lattice* $\mathcal{L}$ is a finitely generated free abelian group on which G acts by automorphisms. Given a G-lattice $\mathcal{L}$ and a field L, we can produce a rational function field $L(\mathcal{L})$ with an L-linear G-action by identifying a basis $(\ell_1, \dots, \ell_r)$ for $\mathcal{L}$ with a set of indeterminates $(t_1, \dots, t_r)$ over L, mapping $\sum_{i=1}^r a_i \ell_i$ to $\prod_{i=1}^r t_i^{a_i}$. *i.e.*, we consider the multiplicative group of monomials in $L(t_1, \dots, t_r)$ as a free abelian group of rank r.

In this case, we are interested in G_q-lattices, and we start by considering the group ring $\mathbb{Z}[\mu_q]$. We write the elements in $\mathbb{Z}[\mu_q]$ as $\sum_{\zeta \in \mu_q} a_\zeta e_\zeta$, and have G_q acting by $\kappa\colon e_\zeta \mapsto e_{\kappa\zeta}$. Moreover, we define a map $\lambda\colon \mathbb{Z}[\mu_q] \to \mu_q$ by

$$\lambda\Big(\sum_{\zeta \in \mu_q} a_\zeta e_\zeta\Big) = \prod_{\zeta \in \mu_q} \zeta^{a_\zeta},$$

and call a G_q-sublattice $\mathcal{L}$ of $\mathbb{Z}[\mu_q]$ *non-degenerate* if $\lambda(\mathcal{L}) = \mu_q$.

Proposition 1 *Let $\mathcal{L} \subseteq \mathbb{Z}[\mu_q]$ be a non-degenerate G_q-sublattice. Then*

$$\mathrm{ed}_K(C_q \rtimes C_D) \le \operatorname{rank} \mathcal{L}.$$

Proof We have $K_q(\mathcal{L}) \subseteq K_q(\mathbf{x})$, when we identify e_ζ and x_ζ.

If we, for convenience, denote the monomial $\prod_{\zeta \in \mu_q} x_\zeta^{a_\zeta}$ corresponding to $a = \sum_{\zeta \in \mu_q} a_\zeta e_\zeta$ by x^a, we see that $\kappa x^a = \tau x^a = x^{\kappa a}$ and $\sigma x^a = \lambda(a) x^a$. So, $K_q(\mathcal{L})$ is closed under the action of $G_q \times (C_q \rtimes C_D)$. We claim that the action is faithful:

Assume that $\chi \in G_q$ and $\rho \in C_q \rtimes C_D$ act identically on $K_q(\mathfrak{L})$. Since $K_q(\mathfrak{L})$ contains K_q, on which G_q acts faithfully and $C_q \rtimes C_D$ acts trivially, we immediately get that $\chi = 1$ and that ρ acts trivially on $K_q(\mathfrak{L})$. Now write $\rho = \tau^i \sigma^j$, where $0 \leq i < q$ and $0 \leq j < d$, and pick $a \in \mathfrak{L}$ with $\lambda(a)$ a primitive q-th root of unity. Then $\rho(x^a) = \lambda(a)^j x^{\kappa^i a} = x^a$, and so we must have $j = 0$ and $\rho = \tau^i$. But on the monomials, τ acts as κ, meaning that the C_D-action is faithful, and so $\rho = 1$.

Stepping down to fixed fields under G_q, we conclude that $C_q \rtimes C_D$ acts faithfully on $K_q(\mathfrak{L})^{G_q} \subseteq K(\mathbf{s})$. And by construction, $\operatorname{tr\,deg}_K K_q(\mathfrak{L}) = \operatorname{rank} \mathfrak{L}$. ■

It remains to produce a non-degenerate G_q-sublattice of $\mathbb{Z}[\mu_q]$ of the desired rank:

Proposition 2 *Let G be a cyclic subgroup of* Aut μ_q *of order $D = dp^e$, where $d|p-1$ and $a \leq n-1$. Then there is a non-degenerate G-sublattice of $\mathbb{Z}[\mu_q]$ of rank $\varphi(d)p^e$.*

Proof Let κ be a generator for G, and let f be a primitive D-th root of unity modulo q, such that $\kappa\zeta = \zeta^D$ for $\zeta \in \mu_q$.

First of all, f is a primitive d-th root of unity modulo p: Since $f^d \equiv f^D \equiv 1 \pmod{p}$, it has order dividing d. On the other hand, if $f^c \equiv 1 \pmod{p}$ for a $c \in \{1, \dots, d-1\}$, we have $f^c = 1 + pi$ for some i, and hence $f^{cp^{n-1}} \equiv 1 \pmod{q}$, since the kernel of $(\mathbb{Z}/q)^* \twoheadrightarrow (\mathbb{Z}/p)^*$ has order p^{n-1}, and so D must divide cp^{n-1}, contradicting $0 < c < d$.

Next, we let

$$P(t) = \prod_{j=0}^{e} \Phi_{dp^j}(t) \quad \text{and} \quad Q(t) = \prod_{j=0}^{e} \prod_{\substack{k|d \\ k<d}} \Phi_{kp^j},$$

where $\Phi_m(t)$ is the m-th cyclotomic polynomial. Then $P(t)Q(t) = t^D - 1$, and $Q(t)$ consists exactly of those factors $\Phi_m(t)$ of $t^D - 1$ for which $p \nmid \Phi_m(f)$. In particular, $p \nmid Q(f)$. Also, $\deg P(t) = \varphi(d)p^e$.

We now look at the G-lattice $\mathbb{Z}[t]/\big(P(t)\big)$, where κ acts as multiplication by t. This is a well-defined G-action, since $P(t)|t^D - 1$.

We have another G-lattice $\mathbb{Z}[t]/(t^D - 1)$, also with κ acting as multiplication by t, and $\mathbb{Z}[t]/\big(P(t)\big) \hookrightarrow \mathbb{Z}[t]/(t^D - 1)$ as G-lattices by $\bar{g} \mapsto \overline{Qg}$.

Finally, $\mathbb{Z}[t]/(t^D - 1) \hookrightarrow \mathbb{Z}[\mu_q]$ by $t^i \mapsto e_{\kappa^i \eta}$, where η is a primitive q-th root of unity, and hence we get $\mathbb{Z}[t]/\big(P(t)\big) \hookrightarrow \mathbb{Z}[\mu_q]$. The image of $\bar{1} \in \mathbb{Z}[t]/\big(P(t)\big)$ has λ-value $\eta^{Q(f)}$, which is a primitive q-th root of unity, and so $\mathbb{Z}[t]/\big(P(t)\big)$ is non-degenerate. ■

Corollary *Assume that K_q/K is cyclic of degree $D = dp^e$, where $d|p-1$ and $e \leq n-1$, and let $G_q = \operatorname{Gal}(K_q/K)$ act on C_q by cyclotomic action (i.e., by identifying C_q and μ_q). Then*

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

For odd primes, this proves the Theorem. For $p = 2$, we note that $\mathbb{Z}/q \rtimes (\mathbb{Z}/q)^*$ has a faithful linear representation over $\mathbb{Q}$ of degree $q/2$, and that we must therefore have $\operatorname{ed}_{\mathbb{Q}}\big(\mathbb{Z}/q \rtimes (\mathbb{Z}/q)^*\big) \leq q/2$.

https://doi.org/10.4153/CMB-2002-044-5 Published online by Cambridge University Press

3 Remarks

In [B&R1, Lemma 4.1(b)], it is shown that $\mathrm{ed}_K(G \times H) \leq \mathrm{ed}_K G + \mathrm{ed}_K H$. Consequently, we get a bound on the essential dimension of any finite abelian group A over $\mathbb{Q}$.

Also, by using that $D_{mn} \hookrightarrow D_m \times D_n$ when m and n are relatively prime (with D_2 understood to be C_2), we see that the bound obtained for C_n will hold for D_n as well, when D_n is the dihedral group of degree n (and order $2n$).

For $q = 3$, 5 and 7, the bounds we obtain for $\mathrm{ed}_{\mathbb{Q}} C_q$ and $\mathrm{ed}_{\mathbb{Q}} D_q$ are the exact values of the essential dimensions. And over the field $K = \mathbb{Q}(\cos \frac{2\pi}{n})$, n odd, the cyclic and dihedral groups are both subgroups of $\mathrm{PGL}_2(K)$, and it is easy to see that they have essential dimension 1, *cf.* also [H&M]. Thus, it seems reasonable to propose

Conjecture *For n odd, the essential dimensions of C_n and D_n coincide over any field in characteristic* 0.

For even n, this is obviously not true: Over the n-th cyclotomic field, C_n has essential dimension 1, whereas D_n has essential dimension 2.

The bound $p^{n-1}\varphi(p-1)$ for $\mathrm{ed}_{\mathbb{Q}} C_{p^n}$ is in fact an upper bound for $\mathrm{ed}_{\mathbb{Q}} P$ of *any* group of order p^n, by the following elementary result:

Lemma *Let K be a field and G a finite group. For any subgroup H of G we then have*

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

In other words: The quantity $\mathrm{ed}_K G/|G|$ does not grow with G.

Proof Let G act regularly on the indeterminates $\mathbf{t} = (t_\sigma)_{\sigma \in G}$. Then H acts regularly on $\mathbf{t}' = (t_\tau)_{\tau \in H}$, and we can find a subfield F of $K(\mathbf{t}')$ such that $\mathrm{tr\,deg}_K F = \mathrm{ed}_K H$ and H acts faithfully on F. Let F' be the composite inside $K(\mathbf{t})$ of the images of F under G's action: $F' = \prod_{\sigma \in G} \sigma F$. Since $\tau F = F$ for $\tau \in H$ and $\sigma F \subseteq K(\sigma \mathbf{t}') = K(\{t_\tau\}_{\tau \in \sigma H})$, there are exactly $[G : H]$ distinct conjugates, and $\sigma F = \sigma' F$ if and only if σ and σ' are in the same coset modulo H, with $\sigma F \cap \sigma' F = K$ otherwise.

Clearly, F' is closed under the action of G, and we claim that the action is faithful: If $\sigma \in G$ acts trivially on F', it in particular maps F to itself, and so $\sigma \in H$. But H acts faithfully on F, and so $\sigma = 1$. ∎

For a group P of order p^n, we can now take a subgroup of order p and get that $\mathrm{ed}_K P \leq p^{n-1} \mathrm{ed}_K C_p$, as claimed. In particular, if $\varphi(p-1)$ is not the exact essential dimension of C_p over $\mathbb{Q}$ for some prime p, the bound on C_{p^n} will not be exact either.

Of course, the bound $p^{n-1}\varphi(p-1)$ on $\mathrm{ed}_{\mathbb{Q}} P$ is very likely not optimal: If P contains a non-cyclic abelian subgroup, we can use that as H to get a lower bound. And for $C_{p^m} \rtimes C_{p^{m-1}}$ the Theorem gives a better bound.

Example The two non-abelian groups of order p^3, p odd prime, are the *Heisenberg group* H_{p^3} of exponent p, and the semi-direct product $C_{p^2} \rtimes C_p$. From the Theorem, we get

$$\mathrm{ed}_{\mathbb{Q}}(C_{p^2} \rtimes C_p) \leq p\,\varphi(p-1),$$

and since H_{p^3} contains an abelian subgroup $\simeq C_p \times C_p$, the Lemma gives us

$$\mathrm{ed}_{\mathbb{Q}}\, H_{p^3} \leq 2p\, \varphi(p-1).$$

In both cases, the bound is better than $p^2\varphi(p-1)$.

References

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

[B&R2] ———, *Versal cyclic polynomials.* unpublished paper.

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

[K&M] G. Kemper and G. Malle, *Invariant fields of finite irreducible reflection groups.* Math. Ann. **315**(1999), 569–586.

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

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

[Sh] I. R. Shafarevich, *Basic Algebraic Geometry 1* (2nd ed.). Springer-Verlag, Berlin 1994.

Mathematical Sciences Research Institute
1000 Centennial Drive
Berkeley, California 94720–5070
U.S.A.
e-mail: ledet@msri.org