Generic Extensions and Generic Polynomials for Semidirect Products

Sebastian Jambor

Lehrstuhl B für Mathematik, RWTH Aachen University, Templergraben 64, D–52062 Aachen, Germany

Abstract

This paper presents a generalization of a theorem of Saltman on the existence of generic extensions with group $A \rtimes G$ over an infinite field K, where A is abelian, using less restrictive requirements on A and G. The method is constructive, thereby allowing the explicit construction of generic polynomials for those groups, and it gives new bounds on the generic dimension.

Generic polynomials for several small groups are constructed.

Key words: Constructive Galois theory, Kummer theory, Generic polynomials, Semidirect products

1. Introduction

Inverse Galois theory is concerned with the question of whether a given finite group G is realizable as Galois group over some field K (cf. Malle and Matzat, 1999). Once this question is settled, one can go a step further and ask for a description of *all* Galois extensions of K with group G. This is done using parametric polynomials, i.e. polynomials $f(x_1, \ldots, x_k, X)$ with coefficients in some rational function field $K(x_1, \ldots, x_k)$, such that the splitting field of f over $K(x_1, \ldots, x_k)$ has Galois group G and that every G-extension of K is the splitting field of $f(a_1, \ldots, a_k, X)$ for a specialization of f with certain $a_1, \ldots, a_k \in K$. Usually, one also requires that these polynomials describe all Galois extensions with group G, where the fixed field is an arbitrary extension field of K; in this case, f is called generic. For an excellent reference for generic polynomials see Jensen et al. (2002).

In Saltman (1982), the concept of *generic extensions* for a group G is introduced, and Ledet (2000) showed that over infinite ground fields K, the existence of a generic G-extension is equivalent to the existence of a generic G-polynomial. Kemper (2001) then showed that every generic polynomial is in fact descent generic, i.e. every subgroup of G is the splitting field of some specialization.

In this paper, we will prove the following theorem:

Email address: sebastian@momo.math.rwth-aachen.de (Sebastian Jambor)

Theorem 1. *Let A be a finite abelian group and K an infinite field. Let G be a finite group acting on A by automorphisms, such that for every prime p the order of the image of G in $\mathrm{Aut}(A_p)$ is coprime to p, where A_p denotes the p-Sylow subgroup of A. If there exist generic extensions for G and A over K then there exists a generic extension for $A \rtimes G$ over K.*

This is a generalization of Saltman (1982, Theorem 3.5), where the same result is proved under the condition that $|A|$ and $|G|$ are coprime. Saltman proves this as an easy corollary of his theorem which states that a generic $A \wr G$-extension exists, provided that generic extensions for A and G exist. While this conclusion is quite elegant and in particular shows the existence of generic $A \rtimes G$-polynomials for certain A and G, it is not trivial to extract those polynomials from the generic extensions. This extraction has been carried out in Jensen et al. (2002, Section 5.5) for dihedral groups of prime power degree (i.e. $G = \mathrm{C}_2$), but the number of parameters of the generic polynomials thus constructed is not optimal. The authors of Jensen et al. (2002) deem it already too involved to construct generic polynomials for Frobenius groups of prime degree, which is naturally the next family of semidirect products to study after dihedral groups.

The approach of this paper uses Kummer theory as outlined in Section 2. The proof of Theorem 1 is constructive, and the extraction of a generic $A \rtimes G$-polynomial is straightforward. In particular, the construction of generic polynomials for dihedral groups or Frobenius groups is now an easy task.

In Section 4 we will construct generic polynomials for most of the groups of order 24.

2. Kummer theory

We prove two easy results in Kummer theory, which will be our motivation for the construction of the generic $A \rtimes G$-extensions. In this whole section, let $n \in \mathbb{N}$, let K be a field with characteristic coprime to n, and let L/K be a finite Galois extension such that L contains a primitive nth root of unity ζ_n. By the classical Kummer theory, the abelian extensions E/L with $\exp(\mathrm{Aut}_E(L)) \big| n$ are in bijection to the subgroups $U \leq L^*/L^{*n}$, where the bijection maps each such subgroup U to the field extension $L(\sqrt[n]{U})/L$. (Cf. Lang (2002, VI, §8). Here, $\exp(A)$ denotes the exponent of the group A, i.e. the least common multiple of orders of elements in A, and $L(\sqrt[n]{U})$ is the field extension of L where all nth roots of elements $a \in L^*$ with $aL^{*n} \in U$ are adjoined.)

The first result is a criterion to decide whether $L(\sqrt[n]{U})/K$ is Galois. Note that the action of $\mathrm{Aut}_K(L)$ on L^* induces an action on L^*/L^{*n}.

Proposition 2. *Let $U \leq L^*/L^{*n}$. The extension $L(\sqrt[n]{U})/K$ is a Galois extension if and only if U is invariant under the action of the Galois group of L/K.*

Proof. Set $G := \mathrm{Aut}_K(L)$. Let first U be invariant under G. By definition, $L(\sqrt[n]{U})$ is the splitting field of $\mathcal{P}_U = \{t^n - a \,|\, a \in L^* \text{ and } aL^{*n} \in U\}$ over L, and this set is invariant under G, i.e. for $t^n - a \in \mathcal{P}_U$ and $g \in G$ we have $t^n - g(a) \in \mathcal{P}_U$. Consider the set

$$\mathcal{Q} := \left\{ \prod_{b \in Ga} (t^n - b) \,\middle|\, a \in L^* \text{ and } aL^{*n} \in U \right\} \subseteq K[t],$$

where Ga is the G-orbit of a. Then $L(\sqrt[n]{U})$ is the splitting field of $\mathcal{Q}$ over L, and it contains the splitting field E of $\mathcal{Q}$ over K, which is therefore Galois over K, as the polynomials in $\mathcal{Q}$ are separable. To prove that $L(\sqrt[n]{U}) = E$, we have to show that $L \subseteq E$; but for $a \in L^*$ the polynomial $t^n - a^n$ is an element of $\mathcal{P}_U$ and hence a divisor of an element of $\mathcal{Q}$, therefore $a \in E$.

Now let $L(\sqrt[n]{U})/K$ be Galois, and consider the set $\mathcal{Q}$ as above. Then every polynomial in $\mathcal{Q}$ has a zero in $L(\sqrt[n]{U})$ and hence splits completely. In particular, the polynomial $t^n - g(a)$ splits for every $g \in G$ and every aL^{*n}, and by the bijection between subgroups of L^*/L^{*n} and abelian extensions of L this implies $g(a)L^{*n} \in U$. □

If we know that an extension $L(\sqrt[n]{U})/K$ is Galois, we can try to determine the isomorphism type of the Galois group. This can be done if the Galois group is known to be a semidirect product of $N := \mathrm{Aut}_L(L(\sqrt[n]{U}))$ by $G := \mathrm{Aut}_K(L)$. To describe the action of G on N we use the following non-degenerate pairing (cf. Lang, 2002, VI, §8):

$$\langle \cdot, \cdot \rangle \colon N \times U \to \langle \zeta_n \rangle \colon (h, xL^{*n}) \mapsto \frac{h(\alpha)}{\alpha} \quad \text{for any root } \alpha \text{ of } t^n - x.$$

Proposition 3. *Let $U \leq L^*/L^{*n}$ be a finite subgroup invariant under $G := \mathrm{Aut}_K(L)$. Assume that $N := \mathrm{Aut}_L(L(\sqrt[n]{U}))$ has a complement in $\mathrm{Aut}_K(L(\sqrt[n]{U}))$ (which is then isomorphic to G). Let $g \in G$ and $h \in N$; then ghg^{-1} is determined by*

$$\langle ghg^{-1}, xL^{*n} \rangle = g(\langle h, g^{-1}(x)L^{*n} \rangle) \text{ for all } xL^{*n} \in U.$$

Proof. Let $xL^{*n} \in U$ and let $\alpha \in L(\sqrt[n]{U})$ be a root of $t^n - x$. Then

$$\langle ghg^{-1}, xL^{*n} \rangle = \frac{ghg^{-1}(\alpha)}{\alpha} = g\left(\frac{hg^{-1}(\alpha)}{g^{-1}(\alpha)}\right) = g(\langle h, g^{-1}(x)L^{*n} \rangle).$$

Since the pairing is non-degenerate, this determines ghg^{-1} uniquely. □

Corollary 4. *Assume that K contains a primitive nth root of unity. Let $U \leq L^*/L^{*n}$ be a subgroup isomorphic to $(\mathbb{Z}/n\mathbb{Z})^k$ for some $k \in \mathbb{N}$, and assume that U is invariant under the action of $G := \mathrm{Aut}_K(L)$. Furthermore, assume that the Galois group of $L(\sqrt[n]{U})/K$ is a semidirect product of $N := \mathrm{Aut}_L(L(\sqrt[n]{U}))$ by G. Then N is isomorphic to U^* (the dual of U) as $(\mathbb{Z}/n\mathbb{Z})G$-module.*

The whole construction of the generic extension for $A \rtimes G$ is motivated by this corollary.

3. Generic extension

3.1. Definitions and notations

Let G be a finite group and K a field.

Definition 5 (Saltman (1982, Definition 1.1))**.** A Galois extension S/R of commutative K-algebras with group G is called a *generic G-extension* over K, if

1. R is of the form $K[\mathbf{t}, 1/t]$ for some number d of indeterminates $\mathbf{t} = (t_1, \ldots, t_d)$ and an element $0 \neq t \in K[\mathbf{t}]$, and

2. whenever $\mathcal{K}$ is an extension field of K and $\mathcal{L}/\mathcal{K}$ is a Galois algebra with group G, there is a K-algebra homomorphism $\varphi\colon R \to \mathcal{K}$, such that $S \otimes_\varphi \mathcal{K}/\mathcal{K}$ and $\mathcal{L}/\mathcal{K}$ are isomorphic as Galois extensions. The map φ is called a *specialization*.

Since a lot of arguments involve extending the scalars of K-algebras to $K(\zeta_n)$, we adopt the following notation.

Notation. Let $n \in \mathbb{N}$ and K a field of characteristic coprime to n. Whenever X is a K-algebra, we set $X_n := K(\zeta_n) \otimes_K X$, where ζ_n is a primitive nth root of unity.

3.2. Construction of generic extensions

We have the following analogue to Corollary 4 for Galois algebras.

Lemma 6. *Let $n \in \mathbb{N}$, and let K be a field of characteristic coprime to n. Let $A = (\mathbb{Z}/n\mathbb{Z})^k$ for some $k \in \mathbb{N}$ and let G be a finite group acting faithfully on A. Define $C := \mathrm{Aut}_K(K_n)$. Let T/K be a Galois algebra with group $A \rtimes G$ and $S := T^A$.*

Then there exist $\alpha_1, \dots, \alpha_k \in T_n^*$ with $\alpha_i^n \in S_n^*$ such that $T_n = S_n[\alpha_1, \dots, \alpha_k]$. The group $\langle \alpha_1 S_n^*, \dots, \alpha_k S_n^* \rangle \leq T_n^*/S_n^*$ is isomorphic to A^* as $(\mathbb{Z}/n\mathbb{Z})G$-modules, and for any $\alpha S_n^* \in \langle \alpha_1 S_n^*, \dots, \alpha_k S_n^* \rangle$ of order n, the group $\langle \alpha S_n^* \rangle$ is isomorphic to $\langle \zeta_n \rangle$ as $(\mathbb{Z}/n\mathbb{Z})C$-module.

Proof. Let A_i be the ith component of $(\mathbb{Z}/n\mathbb{Z})^k$, and let $\overline{A_i}$ be the canonical complement $(i = 1, \dots, k)$. Then $T^{\overline{A_i}}/S$ and hence $T_n^{\overline{A_i}}/S_n$ is Galois with group $A_i \cong \mathrm{C}_n$. Since S_n is a direct sum of isomorphic fields, by Hilbert 90 for Galois algebras there exists $\alpha_i \in T_n^{\overline{A_i}}$ with $T_n^{\overline{A_i}} = S_n[\alpha_i]$ and $\alpha_i^n \in S_n^*$. Furthermore, A_i acts on $S_n[\alpha_i]$ by multiplying α_i with roots of unity. Since T_n is generated by the subalgebras $T_n^{\overline{A_i}}$, we have $T_n = S_n[\alpha_1, \dots, \alpha_k]$.

For the last statement consider the non-degenerate pairing

$$\langle \cdot, \cdot \rangle\colon A \times \langle \alpha_1 S_n^*, \dots, \alpha_k S_n^* \rangle \to \langle \zeta_n \rangle\colon (\sigma, \alpha S_n^*) \mapsto \frac{\sigma(\alpha)}{\alpha}.$$

We have

$$\langle {}^\gamma\sigma, \alpha S_n^* \rangle = \frac{\gamma\sigma\gamma^{-1}(\alpha)}{\alpha} = \gamma\left(\frac{\sigma\gamma^{-1}(\alpha)}{\gamma^{-1}(\alpha)}\right) = \gamma(\langle \sigma, \gamma^{-1}(\alpha) S_n^* \rangle),$$

for any $\gamma \in C \times G$. Since $\langle \zeta_n \rangle \subseteq K_n = S_n^G$ we see $\langle {}^g\sigma, \alpha S_n^* \rangle = \langle \sigma, g^{-1}(\alpha) S_n^* \rangle$ for all $g \in G$, which proves that $\langle \alpha_1 S_n^*, \dots, \alpha_k S_n^* \rangle$ is isomorphic to A^* as $(\mathbb{Z}/n\mathbb{Z})G$-modules. Now let $\kappa \in C$ and $e \in \mathbb{N}$ with $\kappa(\zeta_n) = \zeta_n^e$. Then we have $\langle \sigma, \kappa(\alpha) S_n^* \rangle = \langle {}^\kappa\sigma, \kappa(\alpha) S_n^* \rangle = \langle \sigma, \alpha S_n^* \rangle^e$, and since the pairing is bi-multiplicative and non-degenerate, we have $\kappa(\alpha) S_n^* = \alpha^e S_n^*$, which concludes the proof. □

Our next goal is to describe the action of G on T_n more precisely: we know the images of the α_i only up to elements in S_n^*; we will therefore choose new generators $\beta_1, \dots, \beta_k$ of T_n where we can describe the action explicitly. To do this, we make the following assumption: we let $n = q$ for a prime power q and assume that $A = (\mathbb{Z}/q\mathbb{Z})^k$ is *cyclic* as $(\mathbb{Z}/q\mathbb{Z})G$-module. For any submodule $M \leq (\mathbb{Z}/q\mathbb{Z})G$ isomorphic to A^* we then have $MA^* = A^*$. More precisely, for any $x \in A^*$ with $(\mathbb{Z}/q\mathbb{Z})x = A^*$ we have $Mx = A^*$. Fix such an M and let $(m_1, \dots, m_k)$ be a basis of M such that m_1 is a cyclic generator of M; then $m_1 \cdot x$ is again a cyclic generator of A^*.

The passage from T_q^* to T_q^*/S_q^* corresponds to the passage from $\mathbb{Z}$ to $\mathbb{Z}/q\mathbb{Z}$. The idea is therefore to choose preimages of $\mathbb{Z}/q\mathbb{Z}$ in $\mathbb{Z}$ for M and transfer the resulting relations onto T_q^*: Let $\Lambda\colon G \to (\mathbb{Z}/q\mathbb{Z})^{k\times k}\colon g \mapsto \Lambda^g$ be the representation induced by M with respect to the basis $(m_1,\dots,m_k)$. Furthermore, let $\Gamma_i^g \in \mathbb{Z}/q\mathbb{Z}$ with $m_i = \sum_{g\in G} \Gamma_i^g g$ for all $g \in G$ and $i \in \{1,\dots,k\}$. Choose $\lambda^g \in \mathbb{Z}^{k\times k}$ and $\gamma_i^g \in \mathbb{Z}$ such that $\Lambda^g = \lambda^g \mod q$ and $\Gamma_i^g = \gamma_i^g \mod q$ for all $g \in G$ and $i \in \{1,\dots,k\}$.

Then we have on the one hand

$$gm_i = \sum_{h\in G} \gamma_i^h gh = \sum_{h\in G} \gamma_i^{g^{-1}h} h \mod q,$$

on the other hand

$$gm_i = \sum_{j=1}^{k} \lambda_{ji}^g m_j = \sum_{j=1}^{k} \lambda_{ji}^g \sum_{h\in G} \gamma_j^h h \mod q,$$

thus $\gamma_i^{g^{-1}h} = \sum_{j=1}^k \gamma_j^h \lambda_{ji}^g + t(i,g,h)q$ for some $t(i,g,h) \in \mathbb{Z}$.

Finally, let $(\sigma_1,\dots,\sigma_k) \in A^k$ be the dual basis of $(m_1,\dots,m_k)$ and $C := \mathrm{Aut}_K(K_q)$.

Lemma 7. *With the assumptions and notations above, let T/K be a Galois algebra with group $A \rtimes G$ and set $S := T^A$. Choose a generator αS_q^* of $\langle \alpha_1 S_q^*,\dots,\alpha_k S_q^*\rangle$ as $(\mathbb{Z}/q\mathbb{Z})G$-module and set $a := \alpha^q \in S_q^*$. For $\kappa \in C$ with $\kappa(\zeta_q) = \zeta_q^e$ let $y^\kappa \in S_q^*$ with $\kappa(\alpha) = \alpha^e y^\kappa$. Then there exist roots $\beta_i \in T_q$ of $t^q - \prod_{h\in G} h(a^{\gamma_i^h})$ such that $T_q = S_q[\beta_1,\dots,\beta_k]$, and C, G, and A act on T_q by*

$$\kappa(\beta_i) = \beta_i^e \prod_{h\in G} h((y^\kappa)^{\gamma_i^h}), \qquad g(\beta_i) = \prod_{j=1}^{k} \beta_j^{\lambda_{ji}^g} z_i^g, \qquad \sigma_j(\beta_i) = \zeta_q^{\delta_{ij}} \beta_i,$$

where $\kappa \in C$, $g \in G$, $z_i^g = \prod_{h\in G} h(a^{t(i,g,h)})$, and δ_{ij} is the Kronecker delta.

Proof. Let $\beta_i' := \prod_{h\in G} h(\alpha^{\gamma_i^h})$ for $i = 1,\dots,k$; then $\beta_i' S_q^* = m_i(\alpha S_q^*)$, i.e.

$$\langle \alpha_1 S_q^*,\dots,\alpha_k S_q^*\rangle = M\alpha(S_q^*) = \langle \beta_1' S_q^*,\dots,\beta_k' S_q^*\rangle$$

and hence $T_q = S_q[\beta_1',\dots,\beta_k']$.

Since β_i' is a root of $t^q - \prod_{h\in G} h(a^{\gamma_i^h})$, its image under g must be a root of

$$t^q - \prod_{h\in G} h(a^{\gamma_i^{g^{-1}h}}) = t^q - \prod_{j=1}^{k} \left(\prod_{h\in G} h(a^{\gamma_j^h})\right)^{\lambda_{ji}^g} \cdot \left(\prod_{h\in G} h(a^{t(i,g,h)})\right)^q.$$

These roots are $\zeta_q^\ell \prod_{j=1}^k (\beta_j')^{\lambda_{ji}^g} z_i^g$ for $\ell = 0,\dots,q-1$, so for every $g \in G$ and every $i \in \{1,\dots,k\}$ there exists ℓ_i^g such that $g(\beta_i') = \zeta_q^{\ell_i^g} \prod_{j=1}^k (\beta_j')^{\lambda_{ji}^g} z_i^g$.

Consider the $(\mathbb{Z}/q\mathbb{Z})G$-module $(\mathbb{Z}/q\mathbb{Z})^k \oplus \mathbb{Z}/q\mathbb{Z}$ with basis $(\xi_1,\dots,\xi_{k+1})$, where G acts by $g\xi_i = \sum_{j=1}^k \lambda_{ji}^g \xi_j + \ell_i^g \xi_{k+1}$ for $i = 1,\dots,k$, and $g\xi_{k+1} = \xi_{k+1}$ (i.e. ξ_i corresponds to β_i' for $i = 1,\dots,k$, and ξ_{k+1} corresponds to ζ_q). Then $\left((\mathbb{Z}/q\mathbb{Z})^k \oplus \mathbb{Z}/q\mathbb{Z}\right)/\langle \xi_{k+1}\rangle \cong A^*$, i.e. there exist $\mu_1,\dots,\mu_k \in \mathbb{Z}$ such that $\langle \xi_1 + \mu_1\xi_{k+1},\dots,\xi_k + \mu_k\xi_{k+1}\rangle$ is a submodule isomorphic to A^*. Setting $\beta_i := \zeta_q^{\mu_i}\beta_i'$ yields the desired result for the action of G. For the action of C just note that $\kappa(\beta_i') = \prod_{h\in G} h(\kappa(\alpha)^{\gamma_i^h}) = (\beta_i')^e \prod_{h\in G} h((y^\kappa)^{\gamma_i^h})$. □

The last lemma gives us the formulae to construct Galois extensions with group $A \rtimes G$, given a G-extension and a C_q-extension.

Lemma 8. *Let $\mathcal{R} \subseteq \mathcal{S} \subseteq \mathcal{U}$ be K-algebras, such that $\mathcal{S}/\mathcal{R}$ is a G-extension and $\mathcal{U}/\mathcal{S}$ is a C_q-extension. Assume that $\mathcal{U}_q = \mathcal{S}_q[\theta]$ with $\theta \in \mathcal{U}_q$ such that $v := \theta^q \in \mathcal{S}_q$; for $\kappa \in C$ with $\kappa(\zeta_q) = \zeta_q^e$ let $y^\kappa \in \mathcal{S}_q$ with $\kappa(\theta) = \theta^e y^\kappa$.*

Set $\mathcal{T}_q := \mathcal{S}_q[\theta_1, \ldots, \theta_k]$, where $\theta_i^q = \prod_{h\in G} h(v^{\gamma_i^h})$; define the action of C, G, and A on $\mathcal{T}_q$ by

$$\kappa(\theta_i) = \theta_i^e \prod_{h\in G} h((y^\kappa)^{\gamma_i^h}), \qquad g(\theta_i) = \prod_{j=1}^k \theta_j^{\lambda_{ji}^g} z_i^g, \qquad \sigma_j(\theta_i) = \zeta^{\delta_{ij}}\theta_i,$$

where $\kappa \in C$, $g \in G$, $z_i^g = \prod_{h\in G} h(v^{t(i,g,h)})$, and δ_{ij} is the Kronecker delta.

Then $\mathcal{T}_q/\mathcal{R}$ is a $C \times (A \rtimes G)$-extension.

Proof. Let $s := \sum_{\ell\in(\mathbb{Z}_{\geq 0})^k} s_\ell \theta^\ell$ be an arbitrary element in $\mathcal{T}_q$, where $s_\ell \in \mathcal{S}_q$ and $\theta^\ell := \prod_{i=1}^k \theta_i^{\ell_i}$, for all $\ell \in (\mathbb{Z}_{\geq 0})^k$. Define $g(s) := \sum_{\ell\in(\mathbb{Z}_{\geq 0})^k} g(s_\ell)g(\theta)^\ell$, where $g(\theta) := \prod_{i=1}^k g(\theta_i)$. By the definition of z_i^g we have $g(\theta_i)^q = g(\theta_i^q)$, so $g(s)$ is well defined. We show that this defines an action of G on $\mathcal{T}_q$: let $g, h \in G$ and $i \in \{1, \ldots, k\}$. Since Λ is a representation, we have $\sum_{j=1}^k \lambda_{\ell j}^g \lambda_{ji}^h = \lambda_{\ell i}^{gh} + s(i,\ell,g,h)q$ for some $s(i,\ell,g,h) \in \mathbb{Z}$. We have to prove $g(h(\theta_i)) = (gh)(\theta_i)$. Set $b_i := \theta_i^q = \prod_{h\in G} h(v^{\gamma_i^h})$. On the one hand we have

$$g(h(\theta_i)) = \prod_{j=1}^k \left[\prod_{\ell=1}^k \theta_\ell^{\lambda_{\ell j}^g \lambda_{ji}^h} (z_j^g)^{\lambda_{ji}^h}\right] g(z_i^h) = \prod_{\ell=1}^k \theta_\ell^{\lambda_{\ell i}^{gh}} \prod_{\ell=1}^k b_\ell^{s(i,\ell,g,h)} \prod_{j=1}^k (z_j^g)^{\lambda_{ji}^h} g(z_i^h),$$

on the other hand we have $(gh)(\theta_j) = \prod_{\ell=1}^k \theta_\ell^{\lambda_{\ell i}^{gh}} z_i^{gh}$, hence we have to show

$$\prod_{j=1}^k (b_j^{s(i,j,g,h)} (z_j^g)^{\lambda_{ji}^h}) g(z_i^h) = z_i^{gh}.$$

This amounts to show

$$\sum_{j=1}^k (\gamma_j^\alpha s(i,j,g,h) + t(j,g,\alpha)\lambda_{ji}^h) + t(i,h,g^{-1}\alpha) = t(i,gh,\alpha) \qquad (*)$$

for all $\alpha \in G$. But

$$\sum_{j=1}^k t(j,g,\alpha)\lambda_{ji}^h = \frac{\sum_{j=1}^k \gamma_j^{g^{-1}\alpha}\lambda_{ji}^h - \sum_{\ell=1}^k \gamma_\ell^\alpha \lambda_{\ell i}^{gh}}{q} - \sum_{j=1}^k \gamma_j^\alpha s(i,j,g,h)$$

and

$$t(i,h,g^{-1}\alpha) = \frac{\gamma_i^{(gh)^{-1}\alpha} - \sum_{j=1}^k \gamma_j^{g^{-1}\alpha}\lambda_{ji}^h}{q} = t(i,gh,\alpha) + \frac{\sum_{j=1}^k (\gamma_j^\alpha \lambda_{ji}^{gh} - \gamma_j^{g^{-1}\alpha}\lambda_{ji}^h)}{q},$$

which proves $(*)$. We show that the actions of A and G on $\mathcal{T}_q$ result in an $A \rtimes G$-extension $\mathcal{T}_q/\mathcal{R}_q$. For $i, j \in \{1, \ldots, k\}$ and $g \in G$ choose $\mu_{ji}^g \in \mathbb{Z}$ such that $g^{-1}\sigma_i g = \sum_{j=1}^k \mu_{ji}^g \sigma_j$; since A acts trivially on $\mathcal{S}_q$, it is enough to prove that $\sigma_i g$ and $g \sum_{j=1}^k \mu_{ji}^g \sigma_j$ act in the same way on θ_ℓ for $\ell \in \{1, \ldots, k\}$. We have on the one hand

$$\sigma_i g(\theta_\ell) = \zeta^{\lambda_{i\ell}^g} \prod_{j=1}^k \theta_j^{\lambda_{j\ell}^g} z_\ell^g,$$

on the other hand

$$g\left(\left(\sum_{j=1}^k \mu_{ji}^g \sigma_j\right)(\theta_\ell)\right) = g(\zeta^{\mu_{\ell i}^g}\theta_\ell) = \zeta^{\mu_{\ell i}^g} \prod_{j=1}^k \theta_j^{\lambda_{j\ell}^g} z_\ell^g.$$

Since $(\sigma_1, \ldots, \sigma_k)$ is the dual basis of $(m_1, \ldots, m_k)$, we have $\lambda_{\ell i}^g \equiv \mu_{i\ell}^g \mod q$.

Finally, it is easy to verify that our definition gives an action of C on $\mathcal{T}_q$ and that the actions of C and $A \rtimes G$ commute, which finishes the proof of the lemma. □

Remark. Whenever there exists a generic C_q-extension over K, we can choose one of the form $\mathcal{U}/\mathcal{S}$ such that $\mathcal{U}_q = \mathcal{S}_q[\theta]$ for some $\theta \in \mathcal{U}_q$ with $\theta^q \in \mathcal{S}_q$, as in the last lemma. The proof is almost identical to the proof that a generic extension can be chosen to have a normal basis, using the equivalence of the existence of generic G-extensions over K and the retract-rationality of the extension $K(t_1, \ldots, t_n)/K(t_1, \ldots, t_n)^G$, where G acts faithfully and transitively on $\{t_1, \ldots, t_n\}$ (cf. (Jensen et al., 2002, Remark, p. 100) and (Saltman, 1982, Corollary 5.4)).

Note that the generic C_q-extensions constructed by Saltman (1982) already are of this form.

Now let A be any finite abelian group. For every prime p let A_p be the p-Sylow subgroup of A. Then $A \cong \bigoplus_{p \text{ prime}} A_p$ and $\mathrm{Aut}(A) \cong \bigoplus_{p \text{ prime}} \mathrm{Aut}(A_p)$, so if a group G is acting on A, this action induces actions on the groups A_p. We can get a finer decomposition of A: For each prime p, the group A_p is a $\mathbb{Z}_p G$-module, where $\mathbb{Z}_p G$ is the group ring of G over the ring of p-adic integers $\mathbb{Z}_p$. We assume $p \nmid G$; then $\mathbb{Z}_p G$ is a direct sum of full matrix rings of unramified extensions of $\mathbb{Z}_p$ (cf. (Jacobinski, 1981, Satz 11.1), (Holt and Plesken, 1989, Proposition 2.2.28)), i.e.

$$\mathbb{Z}_p G \cong \bigoplus_{i=1}^{\ell} R_i^{n(i)\times n(i)},$$

where $n(i) \in \mathbb{N}$, and R_i is an unramified extension of $\mathbb{Z}_p$, for $i = 1, \ldots, \ell$. By multiplying A_p with the corresponding central idempotents, it suffices to analyze finite $R^{n\times n}$-modules, where R is an unramified extension of $\mathbb{Z}_p$ and $n \in \mathbb{N}$. Using Morita equivalence and the Fundamental Theorem of finitely generated modules over PIDs we conclude

$$A_p \cong \bigoplus_{i=1}^{m} (\mathbb{Z}/p^{e_i}\mathbb{Z})^{k_i},$$

for some $m, n_i, k_i \in \mathbb{N}$, where each $(\mathbb{Z}/p^{e_i}\mathbb{Z})^{k_i}$ is an irreducible $\mathbb{Z}_p G$-module.

We are now able to prove Theorem 1.

Proof of Theorem 1. Let $\mathcal{S}/\mathcal{R}$ be a generic G-extension over K. We can assume that $\mathcal{S}/\mathcal{R}$ has a normal basis (cf. Jensen et al., 2002, p. 105), and thus $\mathcal{S}^N/\mathcal{R}$ has a normal basis for any normal subgroup $N \trianglelefteq G$.

We assume first that A is of the form $A \cong (\mathbb{Z}/q\mathbb{Z})^k$ for some prime power q and some $k \in \mathbb{N}$, such that A is cyclic as $(\mathbb{Z}/q\mathbb{Z})G$-module. Let $N \trianglelefteq G$ be the kernel of the action of G on A. Let $\mathcal{V}/\mathcal{U}$ be a generic C_q-extension over K; by the previous remark we can assume that $\mathcal{V}_q = \mathcal{U}_q[\theta]$ for some $\theta \in \mathcal{V}_q$ with $\theta^q \in \mathcal{U}_q$.

By the definition of generic extensions, $\mathcal{R}$ is of the form $\mathcal{R} = K[r_1, \ldots, r_m, 1/r]$ and $\mathcal{U}$ is of the form $\mathcal{U} = K[u_1, \ldots, u_n, 1/u]$. Let $u = f(u_1, \ldots, u_n)$ for some polynomial f. Let $(s_1, \ldots, s_\ell)$ be a free basis of $\mathcal{S}^N/\mathcal{R}$; choose $n \cdot \ell$ indeterminates $\mathbf{y} = (y_{11}, \ldots, y_{n\ell})$ over $\mathcal{S}$ and set $\rho' := f(\sum_{j=1}^{\ell} y_{1j}s_j, \ldots \sum_{j=1}^{\ell} y_{nj}s_j) \in \mathcal{S}^N[\mathbf{y}]$. Then $\rho := \prod_{g \in G/N} g(\rho') \in R[\mathbf{y}] = K[\mathbf{r}, \mathbf{y}, 1/r]$, where $\mathbf{r} = (r_1, \ldots, r_m)$. Set $\mathcal{R}' := \mathcal{R}[\mathbf{y}, 1/\rho]$ and $\mathcal{S}' := \mathcal{S}[\mathbf{y}, 1/\rho]$, and define a homomorphism $\varphi\colon \mathcal{U} \to (\mathcal{S}')^N\colon u_i \mapsto \sum_{j=1}^{\ell} y_{ij}s_j$; we denote the extension of φ to $\mathcal{U}_q \to (\mathcal{S}')_q^N$ again by φ. Set $\mathcal{V}' := \mathcal{V} \otimes_\varphi (\mathcal{S}')^N$; then $\mathcal{V}'/\mathcal{S}'$ is a C_q-extension, and $\mathcal{V}'_q = (\mathcal{S}')_q^N[\widetilde{\theta}]$, where $\widetilde{\theta}^q = \varphi(\theta^q)$. Set $v := \varphi(\theta^q)$, and define $\theta_1, \ldots, \theta_k$ as in Lemma 8 to get a $C \times (A \rtimes G/N)$-extension $(\mathcal{S}')_q^N[\theta_1, \ldots, \theta_k]/\mathcal{R}'$. Then $\mathcal{T}_q := \mathcal{S}'_q[\theta_1, \ldots, \theta_k]/\mathcal{R}'$ is a $C \times (A \rtimes G)$-extension, where N acts trivially on the θ_i. Set $\mathcal{T} := \mathcal{S}'_q[\theta_1, \ldots, \theta_k]^C$. We claim that $\mathcal{T}/\mathcal{R}'$ is a generic $A \rtimes G$-extension.

Let T/K be an $A \rtimes G$-extension (by Jensen et al. (2002, Proposition 1.1.5) it suffices to consider $A \rtimes G$-extensions of K instead of extension fields $L \supseteq K$); set $S := T^A$. There exists a specialization $\psi\colon \mathcal{R} \to K$ such that $\mathcal{S} \otimes_\psi K/\mathcal{R} \otimes_\psi K \cong S/K$, and $\psi(s_1), \ldots, \psi(s_\ell)$ is a K-basis of S^N.

Choose $\alpha \in (T_q^N)^*$ as in Lemma 7 and let $L := S_q^N[\alpha]^C$. Then L/S^N is a C_q-extension, so there exists a specialization $\chi\colon \mathcal{U} \to S^N$ such that $\mathcal{V} \otimes_\chi S^N/S^N \cong L/S^N$. There exist $z_{ij} \in K$ with $\chi(u_i) = \sum_{j=1}^{\ell} z_{ij}\psi(s_j)$, and extending the map ψ to $\mathcal{R}'$ by $y_{ij} \mapsto z_{ij}$ we get an isomorphism $\mathcal{T}_q \otimes_\psi K/K \cong T_q/K$ which maps θ_i to β_i, i.e. an isomorphism of $C \times (A \rtimes G)$-extensions. Restricting to the fixed algebras, we get $\mathcal{T} \otimes_\psi K/K \cong T/K$ as $A \rtimes G$-extensions.

Now let A be arbitrary; we have $A \cong \bigoplus_{p \text{ prime}} A_p$ as G-module. Let p be a prime and $N \trianglelefteq G$ the kernel of the action of G on A_p. Then there exist $n_1, \ldots, n_m \in \mathbb{N}$ and $k_1, \ldots, k_m \in \mathbb{N}$ such that $A_p \cong \bigoplus_{i=1}^{m} (\mathbb{Z}/p^{n_i}\mathbb{Z})^{k_i}$ as G/N-module and such that $(\mathbb{Z}/p^{n_i}\mathbb{Z})^{k_i}$ is cyclic as $(\mathbb{Z}/p^{n_i}\mathbb{Z})G/N$-module. The process above can be carried out for each of those cyclic submodules to give a generic $A \rtimes G$-extension. □

3.3. Generic polynomials and generic dimension

The generic dimension of a group G over a field K, denoted by $\mathrm{gd}_K G$, is the minimal number of parameters in a generic G-polynomial over K, or ∞ if no generic polynomial exists (cf. Jensen et al., 2002, Section 8.5). The following bounds can be derived from Saltman's results about generic extensions for semidirect products $A \rtimes G$: If G is a finite group acting on the finite abelian group A by automorphisms with kernel $N \trianglelefteq G$, and if K is an infinite field and $|G|$ and $|A|$ are coprime, then $\mathrm{gd}_K(A \rtimes G) \leq \mathrm{gd}_K(G) + [G : N]\,\mathrm{gd}_K(A)$ (cf. Jensen et al., 2002, Proposition 8.5.6). Using the construction in Theorem 1, these bounds can be considerably improved:

Let A be a finite abelian group and G a group acting on A, such that for every prime p the image of G in $\mathrm{Aut}(A_p)$ has order coprime to p. Let p^{ℓ_p} be the exponent

of A_p and $N_p \trianglelefteq G$ the kernel of the action on A_p; then there exist $k_1, \ldots, k_{\ell_p}$ such that $A_p \cong \bigoplus_{i=1}^{\ell_p} (\mathbb{Z}/p^i\mathbb{Z})^{k_i}$ as $\mathbb{Z}_p(G/N_p)$-modules. For every i, let $\gamma(p,i)$ denote the minimal number of generators of $(\mathbb{Z}/p^i\mathbb{Z})^{k_i}$ as $(\mathbb{Z}/p^i\mathbb{Z})(G/N_p)$-modules.

Corollary 9. *Let A be a finite abelian group and G a group acting on A, such that for every prime p the image of G in $\mathrm{Aut}(A_p)$ has order coprime to p. For every prime p, define N_p, ℓ_p, and $\gamma(p,i)$ as above. Then*

$$\mathrm{gd}_K(A \rtimes G) \leq \mathrm{gd}_K(G) + \sum_{p \text{ prime}} [G : N_p] \sum_{i=1}^{\ell_p} \gamma(p,i)\, \mathrm{gd}_K(\mathrm{C}_{p^i}).$$

Saltman gives an explicit construction of generic C_q-extensions for prime powers q with $8 \nmid q$ (cf. Saltman, 1982, Proposition 2.6), and Jensen, Ledet, and Yui use these extensions to construct generic polynomials in $\varphi(q)/2$ parameters for odd q (cf. Jensen et al., 2002, Proposition 5.3.4). This allows us to construct generic $A \rtimes G$-polynomials over $\mathbb{Q}$:

Corollary 10. *Let A be a finite abelian group with $8 \nmid \exp(A)$. Let G be a group acting on A, such that for every prime p the image of G in $\mathrm{Aut}(A_p)$ has order coprime to p. For every prime p, define N_p, ℓ_p, and $\gamma(p,i)$ as above. Let $\mathcal{R} = K[r_1, \ldots, r_m, 1/r]$ and let $\mathcal{S}/\mathcal{R}$ be a generic G-extension with a normal basis. Then a generic $(A \rtimes G)$-polynomial over $\mathbb{Q}$ with*

$$m + [G : N_2] \sum_{i=1}^{\ell_2} \gamma(2,i)\varphi(2^i) + \sum_{\substack{p \text{ prime} \\ p \geq 3}} [G : N_p] \sum_{i=1}^{\ell_p} \gamma(p,i) \frac{\varphi(p^i)}{2}$$

parameters can be effectively constructed.

Proof. It suffices to consider the case where A is of the form $A \cong (\mathbb{Z}/q\mathbb{Z})^k$ for some prime power q and some $k \in \mathbb{N}$, such that A is cyclic as $(\mathbb{Z}/q\mathbb{Z})G$-module. In the general case we can take a product of the generic polynomials. Let $N \trianglelefteq G$ be the kernel of the action of G on A. Let T/K be a Galois algebra with group $A \rtimes G$. Choose α and β_i in T_q^N as in Lemma 7. Then $(S_q^N[\beta_1])^C/S^N$ is Galois with group C_q. Following the argument in Jensen et al. (2002, p. 103) we see that there exists $j \in \{1, \ldots, q-1\}$ with $(j,q) = 1$ and a specialization $\varphi\colon \mathcal{T} \to K$ such that θ_1 maps to β_1^j and $\mathrm{Tr}_{\mathcal{T}_q/\mathcal{T}}(\theta_1)$ maps to a primitive element of $(S_q^N[\beta_1])^C/S^N$. Using the pairing in Lemma 6, we see that the Galois closure of $(S_q^N[\beta_1])^C/K$ is T/K, since $\beta_1 S_q^* = m_1 \alpha S_q^*$, and we chose m_1 as cyclic generator. Thus the product of the minimal polynomial of $\mathrm{Tr}_{\mathcal{T}_q/\mathcal{T}}(\theta_1)$ and a (suitable) generic polynomial for G is a generic polynomial for $A \rtimes G$. □

Remark. The generic polynomials can be simplified in special cases.

1. Assume that G acts faithfully on the cyclic $(\mathbb{Z}/q\mathbb{Z})G$-module $A \cong (\mathbb{Z}/q\mathbb{Z})^k$, where q is a prime power and $k \in \mathbb{N}$. By replacing α by α^j and β_1 by β_1^j in the situation above we can assume that $j = 1$, i.e. $\mathrm{Tr}(\beta_1)$ is a primitive element of $(S_q[\beta_1])^C/S$, where $S := T^A$. We claim that the Galois closure of $K[\mathrm{Tr}(\beta_1)]/K$ is T, i.e. the minimal polynomial of $\mathrm{Tr}_{\mathcal{T}_q/\mathcal{T}}(\theta_1)$ is generic (i.e. there is no need for the additional generic polynomial for G in the proof above):

Let $\overline{A} \leq A$ be the orthogonal complement of $\langle \beta_1 S_q^* \rangle$ under the pairing in Lemma 6, then $S_q[\beta_1] = T_q^{\overline{A}}$ and hence $S[\mathrm{Tr}(\beta_1)] = T^{\overline{A}}$. Thus $K[\mathrm{Tr}(\beta_1)] = T^B$ for some $\overline{A} \leq B \leq A \rtimes G$, and since $q \big| [K[\mathrm{Tr}(\beta_1)] : K]$ we have $B \cap A = \overline{A}$. The Galois closure of T^B is $T^{B'}$, where B' is the core of B in $A \rtimes G$, i.e. $B' = \bigcap_{x \in A \rtimes G} B^x$; we show that B' is trivial. Since $\beta_1 S_q^* = m_1 \alpha S_q^*$ and we chose m_1 as cyclic generator, we see that the normal closure of $\langle \beta_1 S_q^* \rangle$ in $A^* \rtimes G$ is A^*. Since the pairing respects the G-action, we get that the normal core of $\overline{A}$ is trivial, hence B' intersects A trivially. The group AB' splits over A, so B' is a subgroup of G. But G acts faithfully on A, i.e. $B' = 1$.

2. Now assume $A = \mathbb{Z}/q\mathbb{Z}$ for an odd prime power $q = p^n$ and G acts faithfully on A. In (1) above we saw that we can get an irreducible generic polynomial of degree $|G| \cdot q$; now, we make some further reductions which will give a generic polynomial of degree q.
   Since G is isomorphic to a subgroup of $\mathrm{Aut}(\mathrm{C}_q)$, it is cyclic of order ℓ, generated by an element $g \in G$. We can choose the γ_i^h such that $\theta_1^q = v^{k^{\ell-1}} g(v^{k^{\ell-2}}) \cdots g^{\ell-1}(v) =: \Psi(v)$ in Lemma 8 for some $k \in \mathbb{N}$. Furthermore, we can choose $\mathcal{V}/\mathcal{U}$ as the generic C_q-extension constructed by Saltman: Let $d = \varphi(q)$, let $e \in \mathbb{N}$ be of order pd modulo pq and choose a generator κ of $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_q))$. Set $x := u_1 + u_2(\zeta_q + 1/\zeta_q) + \cdots + u_{d/2}(\zeta_q + 1/\zeta_q)^{d/2} + (\zeta_q - 1/\zeta_q)$ and $u := \prod_{i=0}^{d-1} \kappa(x)$. Now let $\mathcal{U} := \mathbb{Q}[u_1, \ldots, u_{d/2}, 1/u]$ and $\mathcal{V}_q := \mathcal{U}_q[\theta]$ with $\theta^q = x^{e^{d-1}} \kappa(x^{e^{d-2}}) \cdots \kappa^{d-1}(x) =: \Phi(x)$. Then $\mathcal{V}_q^{\langle \kappa \rangle} / \mathcal{U}$ is a generic C_q-extension (cf. Jensen et al., 2002, Section 5.3). Next, let $\mathcal{S} / \mathcal{R}$ be a generic G-extension with free basis $(s_1, \ldots, s_\ell)$, and replace each u_i by $\sum_j y_{ij} s_j$, so from x we get $X := (\sum_j y_{1j} s_j) + \cdots + (\sum_j y_{d/2,j} s_j)(\zeta_q + 1/\zeta_q)^{d/2} + (\zeta_q - 1/\zeta_q)$. Set $\rho := \prod_{i=0}^{\ell-1} \prod_{j=0}^{d-1} g^i(\kappa^j(X))$, $\mathcal{R}' := \mathcal{R}[\mathbf{y}, 1/\rho]$, and $\mathcal{S}' := \mathcal{S}[\mathbf{y}, 1/\rho]$, and let $\mathcal{T}_q := \mathcal{S}'_q[\theta_1]$, where $\theta_1^q = \Psi(\Phi(X))$. Then $\mathcal{T}_q^{\langle \kappa \rangle} / \mathcal{R}'$ is a generic $\mathrm{C}_q \rtimes G$-extension. Let $s \in \mathcal{S}'$ be a generator for a normal basis of $\mathcal{S}'/\mathcal{R}'$. Then the minimal polynomial of $\mathrm{Tr}_{\mathcal{T}_q/\mathcal{T}^G}(\theta_1 s)$ is generic:
   The argument is analogous to the proof of Jensen et al. (2002, Proposition 5.3.4): The extension $\mathcal{T}_q/\mathcal{R}'$ is generated by $\{\zeta^i \theta_1^j g^m(s) \,|\, 0 \leq i < \varphi(q), 0 \leq j < q, 0 \leq m < \ell\}$, so $\mathcal{T}/\mathcal{R}'$ is generated by their traces. We only have to consider the cases $i = 0$ and $(q, j) = 1$, since the other traces are either conjugate to one of those or lie in a subextension. If T/K is a $\mathrm{C}_q \rtimes G$-extension and $S := T^G$, then $T_q = S_q[\beta_1]$ with $\beta_1^q = \Psi(\Phi(b))$ for some $b \in S$, and some element $\mathrm{Tr}_{T_q/T^G}(\theta_1^j g^m(s)) = \mathrm{Tr}_{T_q/T^G}(g^{-m}(\theta_1^j)s)$ specializes to a primitive element. We have $g^{-m}(\Psi(\Phi(b))^j) = \Psi(\Phi(g^{-m}(b^j)))$, so by sending X to $g^{-m}(b^j)$ we get the desired result.

Remark. The theory developed here gives an interpretation for the element $M_\tau(b)$ in Saltman (1982, Theorem 2.3) or $\Phi(b)$ in Jensen et al. (2002, Section 5.3), which is used to characterize cyclic extensions of prime power degree q: it is an image of an element in $(\mathbb{Z}/q\mathbb{Z})C$ which generates a submodule isomorphic to the $(\mathbb{Z}/q\mathbb{Z})C$-module $\langle \zeta_q \rangle$ (where $C := \mathrm{Aut}_K(K(\zeta_q))$, and K is the base field).

4. Examples

Example 11 ($S_3 = D_6 = C_3 \rtimes C_2$)**.** A generic C_2-extension is given by $\mathcal{R}' = K[r, 1/r]$ and $\mathcal{S}' := \mathcal{R}'[\alpha]$ with $\alpha^2 = r$, where C_2 acts by changing the sign, and $s := 1-\alpha$ generates a free basis. We have $X := y_1+y_2\alpha+\zeta-\zeta^2$ and $\theta_1^3 = \Psi(\Phi(X)) = X^4\kappa(X^2)g(X^2)\kappa(g(X))$. We replace θ_1 by θ_1/X to remove the fourth power, and get the trace t of $s\theta$ as

$$t = \theta s + \frac{\theta^2 g(s)}{g(x_1)\kappa(x_1)} + \frac{\theta^2 s}{g(x_1)\kappa(x_1)} + \theta g(s).$$

The generator σ of C_3 simply acts on the summands by multiplication with roots of unity, and we can calculate the minimal polynomial of t as

$$\mu := X^3 - 12(A^2 + 12y_1^2)X + 16(A-6)(A^2 + 12y_1^2),$$

where $A := ry_2^2 - y_1^2 + 3$.

The easy example of the generic S_3-polynomial allows us to construct generic polynomials for groups of order 24.

Example 12 (Groups of order 24)**.** There are 15 groups of order 24, and it is known for all of them whether generic polynomials over $\mathbb{Q}$ exist (cf. Jensen et al., 2002, Exercise 7.3). We are now able to actually compute generic polynomials for those groups.

For $C_3 \times C_8 \cong C_{24}$ and $C_3 \rtimes C_8$ there are no generic polynomials over $\mathbb{Q}$. For $\mathrm{SL}(2,3)$, Rikuna (2004) proved that the invariant field of a four-dimensional representation is purely transcendental, so a generic polynomial can be constructed, e.g using the methods of Kemper and Mattig (2000).

If the group is a direct product (i.e. $D_8 \times C_3$, $Q_8 \times C_3$, $C_4 \times C_6$, $V_4 \times C_6$, $S_3 \times C_4$, $S_3 \times V_4 \cong D_{12} \times C_2$, $(C_3 \rtimes C_4) \times C_2$, and $C_2 \wr C_3 \cong A_4 \times C_2$), a generic polynomial can be constructed by taking a product of generic polynomials for each factor. Generic polynomials for S_4 are well known, so we are left to deal with the groups $C_3 \rtimes Q_8$, $G_1 := C_3 \rtimes D_8$, where the kernel of the action is C_4, and $G_2 := C_3 \rtimes D_8$, where the kernel of the action is V_4.

We start with $C_3 \rtimes Q_8$. Let

$$\begin{aligned} F(r_1, r_2, r_3, X) :=& (X^2-1)^4 - 2(1 - r_1r_2r_3)^2 \frac{A+B+C}{ABC}(X^2-1)^2 \\ &- 8\frac{(1-r_1r_2r_3)^3}{ABC}(X^2-1) \\ &+ (1-r_1r_2r_3)^4 \frac{A^2+B^2+C^2-2AB-2AC-2BC}{A^2B^2C^2}, \end{aligned}$$

where $A := 1 + r_1^2 + r_1^2r_2^2$, $B := 1 + r_2^2 + r_2^2r_3^2$, and $C := 1 + r_3^2 + r_1^2r_3^2$, and set $\mu_1 := r_4^4 F(r_1, r_2, r_3, r_4^{-1/2}X)$. Then μ_1 is a generic Q_8-polynomial (Jensen et al., 2002, Theorem 6.1.12), and a quadratic subextension is parametrized by the polynomial $X^2 - (1 + r_1^2 + r_1^2r_2^2)(1 + r_2^2 + r_2^2r_3^2)$. By Example 11,

$$\mu_2 := X^3 - 12(A^2 + 12y_1^2)X + 16(A-6)(A^2 + 12y_1^2)$$

with $A := (1 + r_1^2 + r_1^2 r_2^2)(1 + r_2^2 + r_2^2 r_3^2) y_2^2 - y_1^2 + 3$ is a 'generic polynomial' for the S_3-subextension. Thus $\mu_1\mu_2$ is a generic $C_3 \rtimes Q_8$-polynomial.

Now we consider the semidirect products $C_3 \rtimes D_8$. Let

$$\mu_1 := X^4 - 2r_1 r_2 X^2 + r_1^2 r_2 (r_2 - 1) \in \mathbb{Q}(r_1, r_2, X).$$

Then μ_1 is a generic D_8-polynomial; furthermore, if $F/\mathbb{Q}(r_1, r_2)$ is the splitting field, then $F/\mathbb{Q}(\sqrt{r_2})$ is a V_4-extension, and $F/\mathbb{Q}(\sqrt{r_2 - 1})$ is a C_4-extension (cf. Jensen et al., 2002, Theorem 2.2.7 and Corollary 2.2.8). Set

$$\mu_2 := X^3 - 12(A^2 + 12y_1^2)X + 16(A - 6)(A^2 + 12y_1^2),$$
$$\mu_3 := X^3 - 12(B^2 + 12y_1^2)X + 16(B - 6)(B^2 + 12y_1^2),$$

where $A := r_2 y_2^2 - y_1^2 + 3$ and $B := (r_2 - 1)y_2^2 - y_1^2 + 3$, then $\mu_1\mu_2$ is generic for G_2-extensions, and $\mu_1\mu_3$ is generic for G_1-extensions.

As mentioned in the introduction, it is now quite simple to describe an algorithm to compute generic polynomials over $\mathbb{Q}$ for Frobenius groups $C_p \rtimes C_\ell$, where C_ℓ acts faithfully on C_p and $8 \nmid \ell$. However, the actual computation of the polynomials is practically infeasible, as there is no computer algebra system known to the author with an efficient method for computations in the rational function field $\mathbb{Q}(z_1, \ldots, z_k)$ and algebraic extensions thereof.

Instead, we will use the theory developed here to construct single polynomials having a prescribed semidirect product as Galois group.

Example 13 (Polynomials with prescribed Galois groups)**.** 1. First, we set $G := C_4$ and construct polynomials with Galois group $\mathbb{F}_5^k \rtimes C_4$ for several $k \in \mathbb{N}$. Let $L/\mathbb{Q} := \mathbb{Q}(\zeta_5)/\mathbb{Q}$ and let g be the generator of the Galois group C_4 which maps ζ_5 to ζ_5^2.

The subgroup $\langle \zeta_5 L^{*5} \rangle \leq L^*/L^{*5}$ is invariant under C_4, so any root of $t^5 - \zeta_5$ generates a field extension $E/\mathbb{Q}$ with Galois group C_{20}. In fact, $E = \mathbb{Q}(\zeta_{25})$.

The $\mathbb{F}_5 C_4$-submodule of L^*/L^{*5} generated by $(1+\zeta_5)L^{*5}$ is $\langle (1+\zeta_5)L^{*5}, (1+\zeta_5^2)L^{*5} \rangle$, and g acts with the matrix $\left(\begin{smallmatrix} 0 & 2 \\ 1 & 1 \end{smallmatrix}\right)$. Thus the Galois group of

$$\prod_{i=0}^{3} (t^5 - g^i(1 + \zeta_5)) = t^{20} - 3t^{15} + 4t^{10} - 2t^5 + 1$$

is $\mathbb{F}_5^2 \rtimes C_4$, where g acts on $\mathbb{F}_5^2$ via $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 3 \end{smallmatrix}\right)$, by Proposition 3.

Similarly, the $\mathbb{F}_5 C_4$-submodule of L^*/L^{*5} generated by $(1 - \zeta_5)L^{*5}$ is

$$\langle (1 - \zeta_5)L^{*5}, (1 - \zeta_5^2)L^{*5}, (1 - \zeta_5^4)L^{*5} \rangle,$$

and g acts with the matrix $\left(\begin{smallmatrix} 0 & 0 & 3 \\ 1 & 0 & 1 \\ 0 & 1 & 2 \end{smallmatrix}\right)$, so we know the Galois group of $t^{20} - 5t^{15} + 10t^{10} - 10t^5 + 5$, namely the semidirect product $\mathbb{F}_5^3 \rtimes C_4$, where g acts by $\left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{smallmatrix}\right)$.

Last, consider the element $x := (1 + \zeta_5 - \zeta_5^2)$; then xL^{*5} generates a submodule isomorphic to the regular module. The element $1 - g^2 \in \mathbb{F}_5 C_4$ is a cyclic generator of the two-dimensional self-dual faithful $\mathbb{F}_5 C_4$-module, so any root of $t^5 - x/g^2(x)$ generates a field extension $E/\mathbb{Q}$ whose Galois closure has Galois group $\mathbb{F}_5^2 \rtimes C_4$, where g acts on $\mathbb{F}_5^2$ by $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 4 \end{smallmatrix}\right)$; the minimal polynomial of the roots of $t^5 - x/g^2(x)$ over $\mathbb{Q}$ is $t^{20} + \frac{1}{11}t^{15} - \frac{19}{11}t^{10} + \frac{1}{11}t^5 + 1$.

2. As a second example, we construct a polynomial with Galois group $\mathbb{F}_3^4 \rtimes \mathrm{D}_8$, where $\mathrm{D}_8 := \langle a, b \mid a^4, b^2, (ab)^2 \rangle$ is the dihedral group of order 8, and the action of D_8 on $M := \mathbb{F}_3^4$ is defined by

$$a \mapsto \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 \end{pmatrix}, \quad b \mapsto \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Let $S := \mathbb{Q}(\sqrt[4]{-2}, i)$ be the splitting field of $t^4 + 2$ over $\mathbb{Q}$; its Galois group is generated by the elements $\alpha = (\sqrt[4]{-2} \mapsto i\sqrt[4]{-2}, i \mapsto i)$ and $\beta = (\sqrt[4]{-2} \mapsto \sqrt[4]{-2}, i \mapsto -i)$, and it is isomorphic to D_8.
Now let ζ_3 be a primitive third root of unity and consider the element $x := \sqrt[4]{-2} + i + \zeta_3 \in S(\zeta_3)^*$. Then $xS(\zeta_3)^{*3}$ generates an eight-dimensional submodule of the $\mathbb{F}_3\,\mathrm{D}_8$-module $S(\zeta_3)^*/S(\zeta_3)^{*3}$. The element $1 + 2ba \in \mathbb{F}_3\,\mathrm{D}_8$ generates a submodule of $\mathbb{F}_3\,\mathrm{D}_8$ isomorphic to M, thus $y := x\beta(\alpha(x^2))S(\zeta_3)^{*3}$ generates a submodule of $S(\zeta_3)^*/S(\zeta_3)^{*3}$ isomorphic to M.
Set $z := y^2\kappa(y)$, where κ is a generator of $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_3))$ and let θ be a root of $t^3 - z$. Then $S(\mathrm{Tr}_{S(\zeta_3,\theta)/S(\zeta_3,\theta)^{\langle\kappa\rangle}}(\theta))/S$ is a C_3-extension (cf. Jensen et al., 2002, Section 5.3). The Galois closure $U/\mathbb{Q}(\zeta_3)$ of $S(\zeta_3, \theta)/\mathbb{Q}(\zeta_3)$ has Galois group $M \rtimes \mathrm{D}_8$, since M is self-dual, thus the Galois closure $T/\mathbb{Q}$ of $S(\mathrm{Tr}_{S(\zeta_3,\theta)/S(\zeta_3,\theta)^{\langle\kappa\rangle}}(\theta))/\mathbb{Q}$ has Galois group $M \rtimes \mathrm{D}_8$. Since we know the action of the Galois group on $U/\mathbb{Q}$, we can compute the minimal polynomial of $\mathrm{Tr}_{S(\zeta_3,\theta)/S(\zeta_3,\theta)^{\langle\kappa\rangle}}(\theta)$ as

$$\begin{aligned} & t^{24} - 144t^{22} + 472t^{21} + 7524t^{20} - 30456t^{19} - 266608t^{18} - 981864t^{17} + 30277458t^{16} \\ & \quad + 9496600t^{15} - 1093991688t^{14} - 1140063288t^{13} + 30808510272t^{12} \\ & \quad + 31632046632t^{11} - 495311379648t^{10} - 865959612792t^9 + 5149493226585t^8 \\ & \quad + 14478424454376t^7 - 28713293762728t^6 - 144781282966176t^5 \\ & \quad - 41870309411988t^4 + 619972209753552t^3 + 1309616138896848t^2 \\ & \quad + 1104816334207968t + 352192366019556. \end{aligned}$$

Acknowledgments

I would like to express my gratitude to Professor Wilhelm Plesken for many invaluable discussions and helpful comments. Furthermore, I would like to thank the anonymous referee for pointing out additional references (especially concerning the existence of generic $\mathrm{SL}(2, 3)$-polynomials over $\mathbb{Q}$) and a wrong citation in the proof of the theorem.

References

Holt, D. F., Plesken, W., 1989. Perfect groups. Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, with an appendix by W. Hanrath, Oxford Science Publications.

Jacobinski, H., 1981. Maximalordnungen und erbliche Ordnungen. Vol. 6 of Vorlesungen aus dem Fachbereich Mathematik der Universität Essen [Lecture Notes in Mathematics at the University of Essen]. Universität Essen Fachbereich Mathematik, Essen.

Jensen, C. U., Ledet, A., Yui, N., 2002. Generic polynomials. Vol. 45 of Mathematical Sciences Research Institute Publications. Cambridge University Press, Cambridge, constructive aspects of the inverse Galois problem.

Kemper, G., 2001. Generic polynomials are descent-generic. Manuscripta Math. 105 (1), 139–141.

Kemper, G., Mattig, E., 2000. Generic polynomials with few parameters. J. Symbolic Comput. 30 (6), 843–857, algorithmic methods in Galois theory.

Lang, S., 2002. Algebra, 3rd Edition. Vol. 211 of Graduate Texts in Mathematics. Springer-Verlag, New York.

Ledet, A., 2000. Generic extensions and generic polynomials. J. Symbolic Comput. 30 (6), 867–872, algorithmic methods in Galois theory.

Malle, G., Matzat, B. H., 1999. Inverse Galois theory. Springer Monographs in Mathematics. Springer-Verlag, Berlin.

Rikuna, Y., 2004. The existence of a generic polynomial for $\mathrm{SL}(2,3)$ over $\mathbf{Q}$Preprint.

Saltman, D. J., 1982. Generic Galois extensions and problems in field theory. Adv. in Math. 43 (3), 250–283.