INVARIANTS FOR THE COMPUTATION OF INTRANSITIVE AND TRANSITIVE GALOIS GROUPS

ANDREAS-STEPHAN ELSENHANS*

Abstract. One hard step in the computation of Galois groups by Stauduhar's method is the construction of relative invariants. In this note, a representation-theoretic approach is given for the construction in the case of an intransitive group.

In the second part of the article, it is shown that the construction can be used for groups that have a suitable intransitive subgroup. The construction solves an open question of Fieker and Klüners.

1. Introduction

Computing the Galois group of a polynomial is an interesting problem in algorithmic number theory. Nowadays, methods ([Ge], [FK]) are based on Stauduhar's [Sta] approach. The idea of this is as follows.

We start with a polynomial f of degree n over $\mathbb{Z}$. First, we compute the roots $r_1, \ldots, r_n$ of f as complex or p-adic numbers. Then, we choose a permutation group G that is known to contain the Galois group (e. g. S_n).

Now, one computes all conjugacy classes of maximal subgroups of G. For a representative U of such a class, one takes a so called *relative invariant* polynomial $I(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$. This is a polynomial such that the stabilizer of I in G is U. Then, one chooses a list of coset-representatives of G/U. For each representative g, one computes $I^g(r_1, \ldots, r_n)$. We assume that the values are pairwise distinct. In this case, one can prove that the value $I^{g_0}(r_1, \ldots, r_n)$ is rational if and only if the Galois group is contained in U^{g_0}. If this is the case then one replaces G by U^{g_0} and repeats the step.

Many difficulties are hidden in the details of the method. See [Ge] or [GK] for details and several optimizations.

Such a relative invariant is by no means unique and in many cases its evaluation takes most of the running time. What properties of the invariant determine the evaluation time?

First, there is the degree of the invariant. It has a direct influence on the computation time. The point is that the numerical precision that is needed in Stauduhar's algorithm is approximately proportional to the degree of the invariant. Thus, the degree should be moderate, but we are not forced to minimize it.

An other point is the number of operations that is needed to evaluate the invariant. If one expresses the invariant as a sum of monomials then this is impractical in

Key words and phrases. Galois group, invariant, representation, algorithm.

*The author was supported in part by the Deutsche Forschungsgemeinschaft (DFG) through a funded research project.

many cases. If one can express the invariant as a sum of products of simpler polynomials then the number of operations for the evaluation can decrease dramatically. Thus, the invariants are given by straight-line programs [BCS, 4.1].

Classically, people focused on invariants for transitive groups. They listed several *special* invariants. This means they produced a table with one invariant for each pair of groups $U \subset G \subset S_n$ ($n \leq 23$ [Ge]). Each of the *special* invariants needs only very few operations for the evaluation, but in many cases they are not of minimal degree. Some of the special invariants extend to families of subgroups.

Further, there is the construction of *generic* invariants. Generic invariants are given by summing an U-orbit of a monomial. If one has a good strategy to choose the monomial then this approach leads to an invariant of minimal degree. This was done in [Gi] for the case of transitive maximal subgroups in S_n and A_n and the case of a solvable transitive subgroup in S_p (p prime). The costs for the evaluation are given by the length of the orbit. In the worst case, this is just the group order.

The intransitive case can be reduced to the transitive case. After a determination of the Galois action on each orbit one proceeds as follows. First, one forms the cartesian product of all orbits. This gives a new permutation representation of the initial group, which is still not transitive. To get a transitive group, one restricts to the action on an orbit. Now, one can apply the known constructions for special invariants.

From a practical point of view, the situation is as follows. The special invariants for transitive groups are practical as long as they are known. Frequently, the reduction from the intransitive case to special invariants of transitive groups leads to invariants of a degree that is far too big. In many cases, the use of generic invariants leads to large computation times and huge memory usage.

The aim of this note is to show that the intransitive case can be handled directly. In many cases, the construction will lead to an invariant that is given as a product (one factor for each orbit). This factorization will reduce the number of operations for the evaluation.

The article is arranged as follows:

- First, we will review subdirect products. This is the group theory that is involved in the construction.
- Then, we will construct invariants in the case that the base field contains enough roots of unity.
- Next, we will explain that avoiding roots of unity is only a formal problem.
- Finally, we will show that this approach can be used for some transitive groups that have a suitable intransitive subgroup.

Motivation. This investigation was motivated by computations in arithmetic geometry. For example, given a smooth cubic surface or a special quartic surface then this surface contains a finite number of lines. The Galois group that acts on the lines is automatically a subgroup of the automorphism group of the intersection configuration of the lines.

The lines can be detected explicitly by a Gröbner basis computation. If the coordinates are chosen sufficiently general then the Gröbner basis will contain an univariate polynomial such that its zeros correspond 1-1 to the lines. The Galois action on the roots of this polynomial is exactly the action on the lines.

Knowing the Galois group, one can derive arithmetic invariants of the surface. The calculations done by Jahnel and the author in [EJ1] and [EJ2] drew interest on algorithms for Galois groups.

2. Subdirect products

Recall 2.1. Let $G = G_1 \times G_2$ be the cartesian product of two groups. A subgroup U of G is called a subdirect product if the projections to G_1 and G_2 are surjective.

The simplest construction for subdirect products is the following. Let H be a third group and $\phi_i \colon G_i \to H$ be two surjective homomorphisms. Then

$$\{(g_1, g_2) \in G_1 \times G_2 \mid \phi_1(g_1) = \phi_2(g_2)\}$$

is a subdirect product of G_1 and G_2.

Let us show that each subdirect product U arises in this way. For this, we denote the identity element of G_i by e_i. Then, we can construct normal subgroups K_i of G_i by $K_1 := \{g_1 \in G_1 \mid (g_1, e_2) \in U\}$ and $K_2 := \{g_2 \in G_2 \mid (e_1, g_2) \in U\}$.

As $K := K_1 \times K_2 \subset U$ one can pass to the quotient $U/K \subset G_1/K_1 \times G_2/K_2$. Note that the projections of U/K to G_1/K_1 and G_2/K_2 are still surjective. Counting elements, we get $\#U/K = \#G_1/K_1 = \#G_2/K_2$. Thus, U/K, G_1/K_1, and G_2/K_2 must be isomorphic groups. Calling this group H, we get surjective morphisms $\phi_i \colon G_i \to H$. Now, $U = \{(g_1, g_2) \in G_1 \times G_2 \mid \phi_1(g_1) = \phi_2(g_2)\}$ results.

Remark 2.2. Subdirect products are exactly the groups we have to deal with when we compute the Galois group of a reducible polynomial. For example, let the product $f_1 \cdot f_2$ be given. First, one may compute the Galois groups G_1, G_2 of the factors. The result will be a subdirect product of these groups.

Thus, the algorithm of Stauduhar will built up a descent-chain starting at the cartesian product of G_1 and G_2 to smaller and smaller subdirect products.

Proposition 2.3. *Let $U \subset U_0 \subset G_1 \times G_2$ be two subdirect products. Assume U to be maximal in U_0. Then, there exist irreducible representations ϕ_1, ϕ_2 of G_1, G_2 such that $U = \{(g_1, g_2) \in U_0 \mid \phi_1(g_1) = \phi_2(g_2)\}$.*

Proof. As U is a subdirect product, there exist representations ψ_1, ψ_2 such that $U = \{(g_1, g_2) \in U_0 \mid \psi_1(g_1) = \psi_2(g_2)\}$. Just take a faithful representation of the group H considered above.

We express the representations as direct sums of irreducible representations $\psi_{1,j}, \psi_{2,j}$ for $j = 1, \ldots, k$. This leads to

$$U = \{(g_1, g_2) \in U_0 \mid \psi_{1,j}(g_1) = \psi_{2,j}(g_2), j = 1, \ldots, k\}\,.$$

Now, we define

$$U_j := \{(g_1, g_2) \in U_0 \mid \psi_{1,j}(g_1) = \psi_{2,j}(g_2)\}\,.$$

We get $U = \bigcap_{j=1}^{k} U_j$. As U is maximal in U_0, there must be a j such that $U = U_j$. □

3. Relative invariants for subdirect products

Recall 3.1 (Basic representation theory in characteristic zero)**.** Let G be a finite group and V be a vector space over a subfield of $\mathbb{C}$.

i) A homomorphism $\phi \colon G \to \mathrm{Gl}(V)$ is called a *representation*.

ii) There exists a G-invariant scalar product on V. Thus, without restriction, the image of ϕ is already contained in the unitary group.

iii) Given two representations $\phi_i \colon G \to \mathrm{Gl}(V_i)$, we can form the tensor product with the G-action $g \circ (v_1 \otimes v_2) := \phi_1(g)v_1 \otimes \phi_2(g)v_2$.

iv) For a representation ϕ, its composition $\mathrm{Tr} \circ \phi$ with the trace map is called the *character* of ϕ.

v) A character is a class function. I.e., it is constant on each conjugacy class.

vi) The character of the tensor product of two representations is given by pointwise multiplication of the characters of the factors.

vii) The space of all class functions is equipped with the scalar product

$$\langle \chi_1 \mid \chi_2 \rangle := \frac{1}{\#G} \sum_{g \in G} \chi_1(g)\overline{\chi_2(g)}\,.$$

viii) The characters of all absolutely irreducible representations form an orthonormal base of the space of all class functions.

ix) Two representations are isomorphic if and only if they have the same character.

Recall 3.2 (Link between representations and invariants)**.** Let $G \subset S_n$ be a permutation group. The canonical action of G on the polynomial ring $\mathbb{C}[X_1, \ldots, X_n]$ is a linear representation of G. Each homogeneous component of the polynomial ring gives us a finite-dimensional subrepresentation. Usually, these representations split further into components. For example, the G-action on the linear span of the G-orbit of $X_1^0 X_2^1 \cdots X_n^{n-1}$ is the regular representation of G. Thus, we can find all irreducible representations of G in it.

From now on, we will use the language of representations. The reader might think of them as subrepresentations of the polynomial ring. Thus, we switch from relative invariant polynomials for the subgroup $U \subset G$ to relative invariant vectors. More precisely, let V be a representation of G. Then, a vector $v \in V$ is a relative invariant if and only if $\mathrm{Stab}_G(v) = U$. Thus, a non-trivial irreducible representation of G gives us a relative invariant if and only if its restriction to U contains trivial components.

Proposition 3.3. i) *Let ϕ_1, ϕ_2 be irreducible representations of a finite group G. Then, $\phi_1 \otimes \phi_2$ contains a trivial component if and only if ϕ_1 and $\overline{\phi_2}$ are isomorphic.*

ii) *Let the unitary group $U_n(\mathbb{C})$ act on the tensor product $\mathbb{C}^n \otimes \mathbb{C}^n$ by*

$$M \circ (u \otimes v) = (Mu) \otimes (\overline{M}v)\,.$$

Then, the only trivial component of the representation is spanned by $e_1 \otimes e_1 + \cdots + e_n \otimes e_n$.

Proof.
i) Denote by χ_1, χ_2 the characters of ϕ_1, ϕ_2 and the trivial character by χ_0. Using [JL, Exercise 19.1] we get $\langle \chi_1 \otimes \chi_2 \mid \chi_0 \rangle = \langle \chi_1 \mid \overline{\chi_2} \rangle$. Now the orthogonality relations of irreducible characters imply the claim.

ii) This is a straightforward computation. □

Remark 3.4. Let ϕ_1, ϕ_2 be the representations considered in Proposition 2.3. Then, the last proposition shows that a relative invariant for $U \subset U_0$ is somewhere in the tensor product $\phi_1 \otimes \overline{\phi_2}$. If the representations are explicitly given in the standard unitary group then we can write down the relative invariant.

Examples 3.5. Let us explain in a few examples how this representation-theoretic approach leads to relative invariant polynomials in product form.

i) Let

$$G := S_n \times S_m \quad \text{and} \quad U := \{(g_1, g_2) \in G \mid \operatorname{sgn}(g_1) = \operatorname{sgn}(g_2)\}.$$

The action of S_k on

$$\Delta_k(X) \quad := \quad \prod_{1 \le i < j \le k} (X_i - X_j)$$

is given by the sign homomorphism. Thus, the action on $\Delta_n(X)\Delta_m(Y)$ is exactly the tensor product of the two representations. We have a relative invariant for U.

ii) Let $D_4 = \langle (1,2,3,4), (1,3) \rangle \subset S_4$ be the symmetry group of the square. The abelian quotient of D_4 is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$. The action on the polynomials

$$\begin{aligned} r_1(X) &:= (X_1 - X_3)(X_2 - X_4) \\ r_2(X) &:= (X_1 + X_2 - X_3 - X_4)(X_2 + X_3 - X_1 - X_4) \end{aligned}$$

leads to two different 1-dimensional representations. Note that these two representations differ by the only non-trivial outer automorphism of D_4, which roughly interchanges the action on edges and vertices.

Invariants for all index 2 subgroups of $D_4 \times D_4$ are given by products of $r_1(X)$, $r_2(X)$, $r_1(Y)$, $r_2(Y)$. Even simpler (but less systematically), one could use

$$r_3(X) := X_1 + X_3 - (X_2 + X_4)$$

instead of r_2.

iii) More generally, we can inspect $G := D_4^n$, the n-fold cartesian product of the dihedral group. For any pair of groups $[G, G] \subset U_2 \subset U_1 \subset G$ (U_2 maximal in U_1), we get a relative invariant as the product of a subset of

$$\{r_1(X^{(k)}), r_2(X^{(k)}) \mid k = 1, \ldots, n\}\,.$$

iv) The only subdirect products in $D_4 \times D_4$, for which we have not yet constructed a relative invariant, is the diagonally embedded D_4.

This can be done as follows. First, note that the action of D_4 on the vector space, spanned by $\{X_1 - X_3, X_2 - X_4\}$, is exactly the usual 2-dimensional representation. The tensor product of two such representations gives us the relative invariant

$$(X_1 - X_3)(X_5 - X_7) + (X_2 - X_4)(X_6 - X_8)$$

for the diagonal in $D_4 \times D_4$. A relative invariant for the skew diagonally embedded D_4 is given by

$$(X_1 + X_2 - X_3 - X_4)(X_5 - X_7) + (X_1 + X_4 - X_2 - X_3)(X_6 - X_8)\,.$$

v) Let $C_n \subset S_n$ be the cyclic group of order n. All irreducible representations of C_n are given by the action on polynomials of the form

$$r_n(X) := X_1 + \zeta_n X_2 + \zeta_n^2 X_3 + \cdots + \zeta_n^{n-1} X_n\,.$$

Here, ζ_n denotes an n-th root of unity.

Thus, relative invariants for all subdirect products in $C_{n_1} \times \cdots \times C_{n_k}$ are given by products of $r_{n_i}(X^{(i)})$ and the correct choice of the roots of unity.

Remark 3.6. The last example used roots of unity as coefficients of the invariant. This is typical as, in general, all representations are defined over cyclotomic extensions. See [Fi1] for the computation of extensions of minimal degree that allow the construction of a representation.

Unfortunately, the computation of Galois groups needs invariants with rational coefficients.

4. Invariants with integer coefficients

4.1. Let $R := \mathbb{Z}[T]/p(T)$ be an integral extension of the integers and $d := \deg(p)$. Further, let $R[X_1, \ldots, X_n]$ be the multivariate polynomial ring. An element $f \in R[X_1, \ldots, X_n]$ can uniquely be written in the form

$$f = \sum_{i=0}^{d-1} T^i f_i$$

with $f_i \in \mathbb{Z}[X_1, \ldots, X_n]$. We call the f_i the *components* of f. For $\sigma \in S_n$, we have

$$f^\sigma = \sum_{i=0}^{d-1} T^i f_i^\sigma \,.$$

If f is a relative invariant for the maximal subgroup $U \subset U_0$ then one of its components is also a relative invariant. To see this, first note that the intersection of all stabilizers of the f_i in U_0 is U. As U is maximal, we are done.

Example 4.2. Let $C_4 \subset S_4$ be the cyclic group of order 4. A relative invariant for the diagonal of $C_4 \times C_4$ is given by

$$p(X,Y) = (X_1 + TX_2 + T^2X_3 + T^3X_4)(Y_1 + T^3Y_2 + T^2Y_3 + TY_4)$$

in $\left(\mathbb{Z}[T]/(T^2+1)\right)[X,Y]$. Splitting this into components, we get the two polynomials

$$\begin{aligned} p_0(X,Y) &= (X_1 - X_3)(Y_1 - Y_3) + (X_2 - X_4)(-Y_2 + Y_4) \\ p_1(X,Y) &= (X_1 - X_3)(Y_2 - Y_4) + (X_2 - X_4)(Y_1 - Y_3)\,. \end{aligned}$$

Note that the stabilizer of p in $S_4 \times S_4$ is exactly the diagonally embedded C_4. The stabilizers of p_0 and p_1 are larger. Further, $p_0 + 2p_1$ has the same stabilizer as p in $S_4 \times S_4$.

Remark 4.3. The last example suggests that the use of the extension $\mathbb{Z}[T]/(T^2+1)$ instead of $\mathbb{Z}$ is purely formal. But this is not the case.

First, the approach gives us an invariant vector instead of an invariant. When running Stauduhar's algorithm, we have to check that the values of the invariant polynomial are distinct. Thus, working with the entire vector solves some degenerated cases. A second advantage becomes visible when we work with more factors.

Example 4.4. Let ρ be an isomorphism $C_4 \to \mathbb{Z}/4\mathbb{Z}$. Then, we can write down the group

$$U_k := \{(a_1, \ldots, a_k) \in C_4^k \mid \rho(a_1) + \cdots + \rho(a_k) = 0\}\,.$$

A relative invariant for $U_k \subset C_4^k$ is given by

$$\prod_{i=1}^{k}(X_1^{(i)} + TX_2^{(i)} + T^2X_3^{(i)} + T^3X_4^{(i)})\,.$$

This polynomial can be evaluated by $(k-1)$ multiplications in $\mathbb{Z}[T]/(T^2+1)$. The components of this invariant do not have a nice product representation.

Remark 4.5. When we perform Stauduhar's algorithm, we suggest to evaluate the invariant in the étale [Bo, V 6.3 Def. 1] algebra $K[T]/p(T)$ and then split the result into components. Here, K denotes the field in which the roots are given. This gives us a vector of values of invariant polynomials with integral coefficients.

For simplicity, we write all invariants as polynomials with coefficients in cyclotomic extensions of $\mathbb{Z}$. It is a formal process to convert them to polynomials with coefficients in $\mathbb{Z}[T]/p(T)$.

5. The trace construction

Recall 5.1 (Induced representations)**.** Let $U \subset G$ be finite groups and $\phi : U \to \mathrm{Gl}(V)$ be a representation. Then, there is a representation ϕ^G called the induced representation of ϕ. If χ is the character of ϕ then we denote by χ^G the character of ϕ^G. Induced representations and characters have the following properties.

i) The dimension of ϕ^G is the product of the dimension of ϕ and the index $[G : U]$.

ii) If $\phi : U \to \{1\}$ is the trivial representation then the induced representation is just the permutation representation of the action of G on the cosets G/U.

iii) Let ϕ be a representation of U and ψ be a representation of G. Denote the characters by χ and ρ. The identity

$$\langle \chi^G \mid \rho \rangle = \langle \chi \mid \rho_U \rangle$$

is called Frobenius reciprocity. Here, ρ_U is the character of the representation ψ restricted to U.

Proposition 5.2. *Let $G, U_0 \subset G_0$ be finite groups. We define $U := G \cap U_0$ and assume that G is maximal in G_0. In addition, we assume $[G_0 : G] = [U_0 : U]$. Further, let ϕ be a representation of U_0 such that ϕ_U contains trivial components, but ϕ does not contain a trivial component.*

Then, the induced representation ϕ^{G_0} does not contain trivial components, but its restriction $(\phi^{G_0})_G = (\phi_U)^G$ contains trivial components. (I.e., the induced representation gives us a relative invariant.)

Proof. Denote the character of ϕ by χ and the trivial character by χ_0. Using Frobenius reciprocity, we compute

$$\langle \chi_0 \mid \chi^{G_0} \rangle = \langle \chi_0 \mid \chi \rangle = 0$$

as ϕ does not contain trivial components. Doing the same with $(\chi^{G_0})_G = (\chi_U)^G$ instead of χ^{G_0}, we see that $(\phi^{G_0})_G$ contains as many trivial components as ϕ_U. □

Remark 5.3 (The trace construction)**.** Let $f_0 \in \mathbb{C}[X_1, \ldots, X_n]$ be a polynomial such that the group $U_0 \subset S_n$ acts on $\mathrm{span}(f_0)$ by a non-trivial 1-dimensional representation, but the restriction to the subgroup $U \subset U_0$ is trivial.

Let G, G_0 be groups containing U, U_0 such that $G \cap U_0 = U$, G maximal in G_0, and $[G_0 : G] = [U_0 : U]$. Assume that the vector space

$$V := \mathrm{span}\{f_0^\sigma \mid \sigma \in G/U\} = \mathrm{span}\{f_0^\sigma \mid \sigma \in G_0/U_0\}$$

is of dimension $[G : U]$.

Then, the action of G_0 on V is the induced representation ϕ^{G_0} in explicit form. The polynomial

$$f := \sum_{\sigma \in G/U} f_0^\sigma$$

is a relative invariant for $G \subset G_0$. We say that f is obtained from f_0 by the *trace construction*. Up to a scalar, this is the *Reynolds operator* studied in invariant theory [Stu, Chap. 2.1].

Remarks 5.4. i) It can easily be checked that V has the expected dimension. For this, one computes the rank of the matrix $(f_0^{\sigma_i}(P_j))$. Here, the P_j are randomly chosen points.

ii) To prove that the dimension is strictly less is far more expensive. It requires to present all f_0^σ as linear combinations of monomials. If one wants to attack this by evaluation then a huge number of points has to be used.

iii) If the assumption on the dimension of V can not be verified then one can modify f_0 in several ways. First, some (but not all) powers of f_0 will give representations with the same properties. Further, we can multiply f_0 with any U_0-invariant function. If, for example, U_0 stabilizes $\{X_1, \ldots, X_k\} \subset \{X_1, \ldots, X_n\}$ then any symmetric function of $X_1, \ldots, X_k$ can be used.

iv) If we are only interested in an invariant and not in the entire induced representation then f can be used as long as it is not an invariant for G_0. This is the case as long as $f \neq 0$.

v) In an extremal situation V is 1-dimensional and f is still a relative invariant. In this case, f is a scalar multiple of f_0. Thus, f_0 itself is a cheap relative invariant. An example for this is $s_1(d_1, \ldots, d_m)$ in [Ge, Satz 6.8].

Example 5.5. Let $G := A_n$, $U = A_{n-1}$, $G_0 = S_n$, and $U_0 = S_{n-1}$. Then, the polynomial

$$\Delta_{n-1}(X_1, \ldots, X_{n-1}) := \prod_{1 \leq i \leq j < n} (X_i - X_j)$$

gives us an initial representation. At a first glace, the trace construction would lead to the sum

$$f := \sum_{i=1}^{n} (-1)^{(n-1)(n-i)} \Delta_{n-1}(X_1, \ldots, \widehat{X_i}, \ldots, X_n)\,.$$

But this is not a relative invariant for $A_n \subset S_n$. Note that the polynomials $\Delta_{n-1}(X_1, \ldots, \widehat{X_i}, \ldots, X_n)$ are linearly dependent. Replacing Δ_{n-1} by Δ_{n-1}^3 or $\Delta_{n-1} X_n^n$ will work. Note that Δ_{n-1}^2 is not suitable.

Example 5.6 (Cf. [Fi2])**.** Denote by $G_0 \subset S_{128}$ the group generated by

$(1, 17, 9, 86, 84, 116, 85, 27, 12, 88, 102, 33, 96, 79, 60, 26, 109, 99, 41, 45, 68, 100,$
$94, 40, 31, 13, 121, 105, 54, 117, 61, 112, 22, 6, 14, 65, 67, 35, 66, 124, 11, 63, 49,$
$118, 55, 72, 91, 125, 42, 52, 110, 106, 83, 51, 57, 111, 120, 10, 30, 46, 97, 34, 90, 39)$
$(2, 78, 62, 44, 59, 101, 119, 108, 36, 71, 29, 123, 58, 38, 24, 25, 56, 15, 7, 23, 69, 81,$
$74, 103, 5, 98, 4, 104, 87, 3, 75, 37, 21, 73, 89, 107, 92, 50, 32, 43, 115, 80, 122, 28,$
$93, 113, 127, 126, 95, 8, 16, 128, 82, 70, 77, 48, 18, 53, 19, 47, 64, 20, 76, 114),$
$(1, 106, 28, 82, 55, 125, 37, 18, 120, 46, 44, 87, 84, 40, 108, 56, 42, 65, 104, 59,$
$54, 39, 126, 36, 12, 118, 128, 58, 68, 124, 48, 21, 22, 45, 123, 69, 96, 26, 114, 5,$
$31, 105, 107, 64, 67, 111, 43, 95, 109, 86, 47, 92, 97, 112, 25, 115, 11, 33, 23, 93,$
$83, 27, 103, 2)(3, 122, 30, 35, 38, 4, 49, 51, 20, 29, 121, 116, 113, 19, 102, 100)$
$(6, 98, 75, 90, 13, 15, 74, 66, 99, 80, 24, 91, 88, 78, 32, 57, 17, 53, 76, 61, 10, 8,$
$77, 85, 52, 71, 127, 60, 63, 73, 119, 94)(7, 110, 72, 70, 16, 41, 79, 81)$
$(9, 34, 101, 89)(14, 117, 50, 62),$
$(1, 77, 123, 72, 54, 89, 25, 88, 31, 24, 44, 100, 68, 19, 103, 52, 42, 119, 104, 117,$
$55, 7, 37, 13, 12, 76, 128, 35, 67, 29, 43, 6, 22, 74, 28, 79, 97, 62, 126, 63, 120,$
$127, 107, 51, 83, 4, 48, 99, 109, 32, 47, 34, 96, 16, 114, 10, 11, 75, 23, 116, 84,$
$122, 108, 17)(2, 98, 33, 30, 18, 73, 45, 41, 21, 53, 118, 121, 5, 78, 106, 110)$
$(3, 26, 61, 59, 38, 39, 91, 82)(8, 65, 9, 95, 80, 46, 49, 36)(14, 56, 71, 105, 102,$
$115, 15, 86)(20, 125, 90, 92, 113, 112, 60, 69)(27, 66, 93, 101, 111, 94, 87, 70)$
$(40, 57, 64, 81, 124, 85, 58, 50)$

of order $193428131138340667952988 16 = 2^{84}$. G_0 is not a wreath product and not a direct product of subgroups. The group is not primitive, it has block systems of sizes 2, 4, 8, 16, 32, and 64. Further, G_0 has 7 maximal subgroups, all of index 2. One can check that 4 of them are transitive and have no further block structure. Invariants for these 4 subgroups can not be constructed by [Ge, Satz 6.14], as the difference between G_0 and the subgroups vanishes, when we pass to a permutation representation on a block system. Thus, we get 4 interesting subgroups without obvious invariants. We denote them by G_i $(i = 1, \dots, 4)$.

Following our general strategy, we need a subgroup of small index that does not act transitively. We pick the kernel of the action on the 8 blocks of length 16. We denote the kernel in G_j by U_j. Surprisingly, all the U_i for $i \geq 1$ coincide. Thus, we have one group of order 2^{79} and one of order 2^{78}. Restricting the action of U_0 to one orbit, we get the group H generated by

$$(1, 96, 31, 68, 42, 97, 11, 84, 22, 55, 120, 83, 109, 54, 12, 67),$$
$$(1, 12, 109, 31, 22, 11, 42, 120)(55, 96)(67, 83, 84, 68)$$

with support $\{1, 11, 12, 22, 31, 42, 54, 55, 67, 68, 83, 84, 96, 97, 109, 120\}$ of order 4096. The groups U_0 and U_1 are subdirect products of H^8.

The abelian quotient of H is $(\mathbb{Z}/4\mathbb{Z})^2$. Thus, we have maps from U_0, U_1 to $(\mathbb{Z}/4\mathbb{Z})^{16}$. It turns out that the images are isomorphic to $(\mathbb{Z}/4\mathbb{Z})^6 \times (\mathbb{Z}/2\mathbb{Z})^3$ and $(\mathbb{Z}/4\mathbb{Z})^6 \times (\mathbb{Z}/2\mathbb{Z})^2$. This shows that we can use tensor products of 1-dimensional representations of H to construct a representation of U_0 that is trivial on U_1.

Analyzing permutation characters, we get that the H-actions on the orbits of X_1X_{11} and $X_1X_{42}X_{54}X_{55}$ contain 1-dimensional representations that generate the

abelian quotient of H. As H is sufficiently small, we can take

$$\begin{aligned} f_1 &:= \sum_{\sigma \in H/\operatorname{Stab}(\{1,11\})} \overline{\chi_1(\sigma)}(X_1X_{11})^\sigma \\ f_2 &:= \sum_{\sigma \in H/\operatorname{Stab}(\{1,42,54,55\})} \overline{\chi_2(\sigma)}(X_1X_{42}X_{54}X_{55})^\sigma \end{aligned}$$

as polynomials, on which H acts via these representations. Here, χ_1, χ_2 denote characters of the representations.

Using a transversal of the block-stabilizer in G_0, we can translate these two polynomials and get analogous representations for the action on the 8 other orbits of U_0.

All products of these polynomials are representations of U_0. We take four factors f_1^σ and two factors f_2^τ. The factors f_1^σ correspond to the U_0-orbits of 2, 3, 4, and 23. The factors f_2^τ correspond to the U_0-orbits of 1 and 3.

The idea behind this is as follows. First, one computes the images of U_0, U_1 in $\{\pm 1, \pm\zeta_4\}^{16} \cong (\mathbb{Z}/4\mathbb{Z})^{16}$. (The maps are given by the 16 representations corresponding to the translations of f_1 and f_2.) Then, we search for a linear form $(\mathbb{Z}/4\mathbb{Z})^{16} \to \mathbb{Z}/4\mathbb{Z}$ with a minimal number of non-zero coefficients, the kernel of which contains the image of U_1 but not the image of U_0.

The constructed product gives us a non-trivial representation of U_0 with kernel U_1. Let us call this polynomial f_0. It has degree 16 and its evaluation needs 709 multiplications.

Now we try to induce invariants for the 4 interesting maximal subgroups G_i of G_0. It turns out that the G_i-orbit of f_0 does not contain $32 = [G_1 : U_1] = [G_0 : U_0]$ linear independent polynomials. Thus, the naive construction degenerates.

Multiplying f_0 with the block-sum

$$\sum_{i \in \{4,7,16,19,24,29,32,62,74,75,76,77,89,119,122,127\}} X_i$$

gives us a degree 17 polynomial such that the G_i-orbits consist of 32 linear independent polynomials each. Each sum of such an orbit of 32 polynomials gives us a relative invariant of degree 17. The evaluation costs are 22720 multiplications.

Remark 5.7. It is possible to reduce the number of multiplications by finding better presentations of f_1, f_2. For example

$$\begin{aligned} f_1 &= \zeta_4(X_{67} - X_{68} + X_{84} - X_{83})(X_{54} - X_{55} + X_{97} - X_{96}) \\ &\quad + (X_{12} + X_{11} - X_{120} - X_{31})(X_{22} + X_1 - X_{109} - X_{42}) \\ f_2 &= ((X_{42} - X_{109})(X_1 - X_{22}) - \zeta_4(X_{31} - X_{120})(X_{11} - X_{12})) \\ &\quad \cdot ((X_{55} - X_{96})(X_{54} - X_{97}) + \zeta_4(X_{68} - X_{83})(X_{67} - X_{84})) \end{aligned}$$

gives a representation of the f_i involving only 3 respectively 7 multiplications. Thus, the costs for the entire invariant are reduced to $32 \cdot (1 + 4 \cdot 3 + 2 \cdot 7) = 864$ multiplications.

It is not surprising that such a simplification is in principle possible. To explain this, note that H has a block system with two blocks of size 8. Thus, every representation of H is a component of a representation induced from one of the block stabilizer. Further, every representation of the block stabilizer is contained in a tensor product of representations of the two groups that act on the orbits. Now,

one can continue recursively by using block systems of the groups that act on one orbits. However it is not clear, why this is so efficient.

6. A general strategy

6.1. Example 5.6 suggests the following strategy for the construction of invariants.

Algorithm 6.2. Let transitive subgroups $U \subset G \subset S_n$, U maximal in G, be given.

i) Compute all block systems of G and all transitive maximal subgroups of G.

ii) For each block system, compute its stabilizer S in G.

iii) Embed S and $S \cap U$ into the direct product P of the groups that act on the orbits of S.

iv) Compute the images of S and $S \cap U$ in the abelian quotient $P/[P, P]$.

v) If the images differ then construct a 1-dimensional representation of P that is trivial on $S \cap U$, but not on S. This representation is automatically a tensor product of 1-dimensional representations of the factors of P.

vi) Try to find nice presentations of each factor by recursively expressing it as a component of an induced representation of a tensor product of representations of smaller subgroups. (Compare Remark 5.7.)

vii) Use the trace-construction to get a relative invariant for $U \subset G$.

Remark 6.3. In the case that several relative invariants were found, one can optimize the computations by taking the cheapest one.

Experiment 6.4. It is hard to do a fair comparison between this and other methods. Let us try the following. We start with all transitive subgroups $G \subset S_n$ for $n = 24$ $(27, 30)$. These groups have been classified in [Hul].

Using the algorithm of [CH1], we computed for each G a list of all conjugacy classes of transitive, maximal subgroups. Then, we asked `magma` for special invariants. It turned out that, for 24274 (1894, 5468) out of 25000 (2392, 5712) possibilities for G, special invariants for all maximal subgroups were found.

The remaining 726 (498, 244) possibilities for G give rise to 5234 (4848, 1144) pairs $U \subset G$ of groups. For 2191 (2148, 462) of them, no special invariant was found.

Then, we checked whether Algorithm 6.2 could construct an invariant. This worked for 2140 (2012, 298) pairs of groups. Surprisingly, Algorithm 6.2 failed only in cases when the subgroup U was not normal. Table 1 gives an overview of the distribution of the indices of the subgroups we treated and the ones that remain.

		$[G:U]$											
n		2	3	4	5	8	9	16	25	27	64	81	≥ 100
24	total	1020	20	922		15	2	80			82	32	18
	rem.		7				2				10	32	
27	total		2020				123			5			
	rem.		110				24			2			
30	total	99	99		18		2	40	26		6	109	63
	rem.		32		10		2		26			57	37

Table 1. Frequency of $[G : U]$ for pairs without special invariants

The costs for the invariants are proportional to the number of summands used in the trace construction. Table 2 give an overview.

	Number of summands						
n	$2-9$	$12-20$	$24-42$	$48-96$	$108-192$	$216-432$	≥ 576
24	440	312	480	513	193	52	150
27	1097	393	145	249	105	19	4
30	10	39	3	60	32	46	108

TABLE 2. Distribution of the costs of the new invariants

Summarizing, we get cheap replacements for generic invariants in a large number of cases with small index. When we work in S_{24} or S_{30}, special invariants for most pairs of subgroups are known.

Remark 6.5. We restricted to $n = 24$ (27, 30) for two reasons. First, invariants for $n \leq 23$ were optimized by [Ge]. Further, a database of all transitive groups for larger n is not yet available. Note that for $n = 32$ such a database would consist of 2 801 324 groups [CH2].

Example 6.6. Let us inspect an example of a pair of groups without a known special invariant such that Algorithm 6.2 does not work. As it worked for all normal subgroups there is no example with index 2. Thus we pick one with index 3. We take G as the transitive group nr. 5421 of degree 30. As an abstract group, G is $(A_3 \wr S_{10}) \rtimes \pm 1$. The group has only one block system. It has 10 blocks of size 3. The block-stabilizer in G is

$$\{(\sigma_1, \ldots, \sigma_{10}) \in S_3^{10} \mid \operatorname{sgn}(\sigma_1) = \cdots = \operatorname{sgn}(\sigma_{10})\}.$$

Let U be the subgroup

$$\left(\{(\sigma_1, \ldots, \sigma_{10}) \in A_3^{10} \mid \sigma_1 \cdots \sigma_{10} = \mathrm{id}\} \rtimes S_{10}\right) \rtimes \pm 1$$

of G. An inspection of the Molien series shows that there is no relative invariant of degree less than 10. `magma` needs 50 hours and 9 GB of memory to find a generic invariant with 456275848 multiplications for this pair of groups. An evaluation of the invariant in $[1, \ldots, 1]$ results in 2976069600. This evaluation needs 31 seconds of CPU-time.

Algorithm 6.2 does not work as there is no 3-torsion in the inspected quotients $P/[P, P]$.

Remark 6.7. There are several possibilities to extend Algorithm 6.2.

i) One could use higher-dimensional representations of the factors of P. But in the case of more than two factors, this will result in a large tensor product. Thus, one needs a strategy to extract a subrepresentation of S as soon as possible. This modification can no longer use the abelian quotient $P/[P, P]$ for simplification.

ii) One could replace step 2 by any other strategy of selecting intransitive subgroups.

iii) The relative invariant for $S \cap U \subset S$ constructed in step 5 may have a larger stabilizer than $S \cap U$ in G. In this case, we can start the trace-construction with $S \cap U$ replaced by the stabilizer. This will lead to a final invariant with less summands.

iv) As Algorithm 6.2 works well for normal subgroups, one could attack non-normal index 3 subgroups by computing an index 2 subgroup $G_1 \subset G$ such that $U \cap G_1 \subset G_1$ is normal. Then one could try to derive a relative invariant f for $U \subset G$ from a relative invariant f_1 of $U \cap G_1 \subset G_1$ with the Reynoulds operator. Thus, one takes $f := f_1 + f_1^\sigma$ with an arbitrary $\sigma \in U \setminus G_1$.

Example 6.8. i) Using these generalizations, we can inspect the groups of Example 6.6 once more. We set $f(u,v,w) := u + \zeta_3 v + \zeta_3^2 w$. Then we can write down the relative invariant

$$\begin{aligned} & f(x_1,x_2,x_3)f(x_4,x_6,x_5)f(x_7,x_8,x_9)f(x_{10},x_{11},x_{12})f(x_{13},x_{14},x_{15}) \\ & f(x_{16},x_{18},x_{17})f(x_{19},x_{20},x_{21})f(x_{22},x_{24},x_{23})f(x_{25},x_{27},x_{26})f(x_{28},x_{30},x_{29}) \\ + \quad & f(x_1,x_3,x_2)f(x_5,x_6,x_4)f(x_7,x_9,x_8)f(x_{11},x_{10},x_{12})f(x_{15},x_{14},x_{13}) \\ & f(x_{17},x_{18},x_{16})f(x_{19},x_{21},x_{20})f(x_{22},x_{23},x_{24})f(x_{26},x_{27},x_{25})f(x_{30},x_{28},x_{29}) \end{aligned}$$

of minimal degree for $U \subset G$.

The invariant is constructed as follows. First, we pass to the subgroup $G_1 := A_3 \wr S_{10}$. Now $U \cap G_1 \subset G_1$ is normal. Then, we pick the intransitive subgroup $S := A_3^{10}$. The first product in the invariant for $U \cap S \subset S$. When we apply the trace construction, we observe that the product is not changed by the action of S_{10}. Thus, the first product is in fact an invariant for $U \cap G_1 \subset G_1$. We get the final result by applying the Reynolds operator to this.

ii) An example that uses an other kind of intransitive subgroup is the following. Denote by $M_{24} \subset A_{24}$ the Mathieu group of order 244823040. When we apply Algorithm 6.2 to these groups, we do not get anything useful.

Let us use the intransitive subgroup $S \subset M_{24}$ of index 759 instead of a block stabilizer. S has orbits of size 8 and 16. We denote the orbit of length 8 by O_8. Then we can form the relative invariant

$$\sum_{g \in M_{24}/S} \left(\sum_{i \in O_8^g} X_i \right)^6$$

for $M_{24} \subset A_{24}$. It uses 6071 additions and 759 powers. Note that M_{24} is 5-transitive, so there is no chance to construct a relative invariant of degree ≤ 5.

This strategy primarily applies to subgroups of huge index. This is the typical situation for primitive groups in A_n or S_n [DM].

References

[BCP] Bosma, W., Cannon, J., and Playoust, C.: *The Magma algebra system I: The user language,* J. Symbolic Comput. 24 (1997), no. 3-4, 235–265.

[Bo] Bourbaki, N.: *Algebra II, Chapters 4-7,* Springer-Verlag, Berlin, 1990.

[BCS] Bürgisser, P., Clausen, M., and Shikrollahi, M.A.: *Algebraic Complexity Theory,* Springer-Verlag, Berlin, Heidelberg, New York, 1996.

[CH1] Cannon, J. and Holt, D.: *Computing maximal subgroups of finite groups,* J. Symbolic Comput. 37 (2004), no. 5, 589–609.

[CH2] Cannon, J. and Holt, D.: *The transitive permutation groups of degree 32,* Experimental Mathematics 17 (2008), no. 3, 307–314.

[DM] Dixon, J. D. and Mortimer, B.: *Permutation groups,* Springer-Verlag, Berlin, Heidelberg, New York, 1996.

[EJ1] Elsenhans, A.-S. and Jahnel, J.: *On the Brauer-Manin obstruction for cubic surfaces,* Journal of Combinatorics and Number Theory 2 (2010), 107–128.

[EJ2] Elsenhans, A.-S. and Jahnel, J.: *Cubic surfaces with a Galois invariant pair of Steiner trihedra,* International Journal of Number Theory 7 (2011), 947–970.
[Fi1] Fieker, C.: *Minimizing representations over number fields II: Computations in the Brauer group,* J. Algebra 322 (2009), no. 3, 752–765.
[Fi2] Fieker, C.: *Personal communication,* Sydney, 2011.
[FK] Fieker, C. and Klüners, J.: *Galoisgruppen in Magma,* Computeralgebra Rundbrief 43 (2008), 19–20.
[Ge] Geißler, K.: *Berechnung von Galoisgruppen über Zahl- und Funktionenkörpern,* Dissertation, Berlin, 2003.
[GK] Geißler, K. and Klüners, J.: *Galois group computation for rational polynomials,* Algorithmic methods in Galois theory. J. Symbolic Comput. 30 (2000), no. 6, 653–674.
[Gi] Girstmair, K.: *On invariant polynomials and their application in field theory,* Math. Comp. 48 (1987), no. 178, 781–797.
[Hul] Hulpke, A.: *Constructing transitive permutation groups,* J. Symbolic Comput. 39 (2005), no. 1, 1–30.
[Hup] Huppert, B.: *Endliche Gruppen I,* Springer-Verlag, Berlin, Heidelberg, New York, 1967.
[JL] James, G. and Liebeck, M.: *Representations and characters of groups,* Cambridge University Press, Cambridge, 1993.
[Sta] Stauduhar, R. P.: *The determination of Galois groups,* Math. Comp. 27 (1973), 981–996.
[Stu] Sturmfels, B.: *Algorithms in Invariant Theory*, Springer-Verlag, Wien, New York, 1993.

Universität Bayreuth, Mathematisches Institut, Universitätsstrasse 30, D-95447 Bayreuth, Germany
E-mail address: stephan.elsenhans@uni-bayreuth.de