Computing Galois Groups of Ehrhart Polynomials in OSCAR

Claus Fieker[1], Tommy Hofmann[*2], and Michael Joswig[3,4]

[1]*Technische Universität Kaiserslautern*
[2]*Universität Siegen*
[3]*Technische Universität Berlin, Chair of Discrete Mathematics/Geometry*
[4]*Max-Planck Institute for Mathematics in the Sciences, Leipzig*

Abstract. We report on an implementation of Galois groups in the new computer algebra system `OSCAR`. As an application we compute Galois groups of Ehrhart polynomials of lattice polytopes.

Keywords: lattice polytopes, smooth Fano polytopes, computer algebra

1 Introduction

OSCAR is an acronym for "Open Source Computer Algebra Resource" [13, 25]. This is a new computer algebra system, written in JULIA, which combines and extends the full feature set of ANTIC [17], GAP [19], POLYMAKE [20] and SINGULAR [11]. The implementation is an ongoing major collaborative effort lead by the transregional collaborative research center (SFB-TRR) 195 "Symbolic Tools in Mathematics and their Application", which is funded by the German Research Foundation (DFG). At the current version 0.8.2 the system is still in its infancy; yet it offers a wide range of functions already. As a showcase here we give an account of computations in OSCAR which require methods from algebra, number theory, group theory and polyhedral geometry. OSCAR is registered as a JULIA package, which makes the installation of a released version via JULIA's package manager trivial. Additionally, the entire source code and its ongoing development can be followed at https://github.com/oscar-system. This also includes documentation, unit tests and continuous integration. The specific computations shown here are documented at https://github.com/micjoswig/oscar-notebooks.

A *lattice polytope*, P, is the convex hull of finitely many points in $\mathbb{R}^n$ with integral coordinates. The function $L_P(t)$, for $t \in \mathbb{N}$, counts the lattice points in the dilations $t \cdot P$. Ehrhart's Theorem says that $L_P(t)$ is a rational univariate polynomial of degree $d = \dim P$ in the parameter t; see, *e.g.*, [6, Section 3.4]. Research on Ehrhart polynomials abounds for their connections to combinatorics, algebraic geometry and beyond. Here

---

[*]tommy.hofmann@uni-siegen.de

we use OSCAR to study the Galois groups of Ehrhart polynomials. To the best of our knowledge this is a new idea.

2   Computing Galois Groups

The computation of Galois groups of rational polynomials is among the fundamental problems of algorithmic algebraic number theory as formulated by Zassenhaus in [30]. In the following we will give a brief overview about the standard algorithm for solving this task as well as the state of current implementations.

We will first explain what is meant by computing the Galois group of a rational polynomial. To this end let $f \in \mathbb{Q}[t]$ be a polynomial of degree n. Recall that the Galois group $\mathrm{Gal}(f)$ of f is defined as the group of automorphisms of $\mathrm{Gal}(N/\mathbb{Q})$, where N denotes a splitting field of f, *i.e.*, a minimal field extension of $\mathbb{Q}$ such that f decomposes over N into linear factors. Denote by $S = \{\alpha_1, \ldots, \alpha_n\}$ the set of roots of f in any field containing $\mathbb{Q}$. After choosing an ordering on the roots S, via its action on S the Galois group $\mathrm{Gal}(f)$ gives rise to a faithful permutation representation $G \to S_n$. The equivalence class of this representation is independent of the chosen set S or its ordering. Thus when speaking of computing $\mathrm{Gal}(f)$, we mean the computation of a permutation group $G \subseteq S_n$ such that the action of $\mathrm{Gal}(f)$ on a set of roots in any splitting field is permutation equivalent to the natural action of G. Note that this implies $\mathrm{Gal}(f) \cong G$ as groups, but permutation equivalence is in general stronger.

We now sketch an algorithm of Stauduhar [28] and its improvements by Fieker and Klüners [18] for finding the Galois group $\mathrm{Gal}(f) \leq S_n$, where $f \in \mathbb{Q}[t]$ has degree n.

1. Determine approximations $\widehat{S} = \{\widehat{\alpha}_1, \ldots, \widehat{\alpha}_n\} \subseteq L$ of the roots of f in a suitable field extension $\mathbb{Q} \subseteq L$. One may take $L = \mathbb{C}$ and employ well-known methods to approximate roots of univariate polynomials, but it is also possible to use algebraic closures of p-adic fields $\mathbb{Q}_p$.

2. Assume that we know a subgroup $G \leq S_n$ for which the inclusion $\mathrm{Gal}(f) \leq G$ holds (at the beginning $G = S_n$). To test whether $\mathrm{Gal}(f)$ is equal to G, it is sufficient to test whether $\mathrm{Gal}(f) \leq H$ for any of the finitely many maximal subgroups $H \leq G$. Thus let $H \leq G$ be a subgroup. Denote by $F \in \mathbb{Z}[x_1, \ldots, x_n]$ a G-relative H-invariant polynomial, that is, F equals $F^\sigma := F(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ for all $\sigma \in H$ and the stabilizer of F in G equals H. Now after certain technical properties are checked, the main result of Stauduhar states that $\mathrm{Gal}(f) \leq H$ if and only if $F(\alpha_1, \ldots, \alpha_n)$ is an element of $\mathbb{Z}$. As this latter task can be performed by evaluating $F(\widehat{\alpha}_1, \ldots, \widehat{\alpha}_n)$ to a high enough precision, we can decide whether $\mathrm{Gal}(f) \leq H$ rigorously. By performing this task iteratively, the algorithm traverses down the lattice of subgroups of S_n until the Galois group $\mathrm{Gal}(f) \leq S_n$ is determined.

Remark 1. While the algorithm described above yields a procedure to compute Galois groups that works well in practice for input of small size, we want to point out several improvements, which are necessary to render this algorithm practical.

1. While we formulated the algorithm for arbitrary polynomials, it is advisable to first determine a factorization of f into irreducible polynomials and compute the Galois group for each of these polynomials first. This yields two advantages: For irreducible polynomials, the Galois group is automatically transitive, hence fewer candidates have to be checked and secondly, for pairs of transitive groups more sophisticated methods for finding invariants are available than in the generic case.

2. Instead of testing $\mathrm{Gal}(f) \leq H$ for all maximal subgroups H of G, one can restrict to representatives of conjugacy classes of maximal subgroups of G. Given such a representative H, one then tests for a set of coset representatives τ of H in G whether $F^\tau(\alpha_1, \ldots, \alpha_n)$ is an integer, which is equivalent to $\mathrm{Gal}(f) \leq H^\tau$. Determining the conjugacy classes of maximal subgroups and coset representatives of permutation groups are well-studied problems in algorithmic group theory, with efficient solutions.

3. One bottleneck of the algorithm is finding the G-relative H-invariant polynomial F. Generic methods described in [18] yield a polynomial whose number of terms grows linearly in the index $[G : H]$, making this step quite costly for groups with maximal subgroups of large index. More advanced techniques have been introduced by Elsenhans [15].

4. To deal with large index subgroups, the idea of short cosets has been introduced, where additional information is used to reduce the set of coset representatives that need to be considered. For example, if f has a pair of complex conjugate roots, the complex conjugation has to be an element of the Galois group of f, and hence only σ such that H^σ contains the complex conjugation need to be tested.

5. To make use of highly optimized algorithms for finding subfields of number fields, instead of starting with the full symmetric group, one can start with the intersection of suitable wreath products: If f is irreducible, each subfield of the stem field $\mathbb{Q}[t]/(f)$ of f yields a block system for the unknown Galois group, hence a maximal subgroup supporting this.

An implementation of the algorithm, which performs quite well in practice, is available in OSCAR (Version 0.8.2). The implementation exploits the tight integration between the group theoretic component built upon GAP and the number theoretic functionality provided by ANTIC. Section 3 below comprises concrete computations in the context of Ehrhart polynomials.

We end with comparisons to other computer algebra packages with the functionality to compute Galois groups of (a restricted set of) polynomials in $\mathbb{Q}[t]$. As is apparent from the description of the algorithm, critical steps require the use of sophisticated techniques from both algorithmic group and number theory. This requirement already narrows down possible computer algebra software able to handle this scenario.

1. Computing Galois groups of rational polynomials has been available in the closed source system MAGMA [8] for quite some time. In comparison to OSCAR, due to various optimizations, for increasing parameters MAGMA will outperform the current implementation in OSCAR. Yet, for parameter ranges of practical relevance, the performance profiles are similar.

2. Based on the work of Eichenlaub [14], the number theory package PARI (Version 2.13.1) provides an implementation to determine Galois groups for polynomials f with degree $\deg(f) \leq 11$, which in addition need to be irreducible. Neither assumption is met in our application: Ehrhart polynomials may be reducible, and they may have arbitrarily high degrees.

3. Implementations of algorithms of Soicher–McKay [27] and Hulpke [23] in GAP allow to determine Galois groups of irreducible polynomials of degree up to 15.

4. The computer algebra system SAGEMATH [29] (Version 9.5) includes interfaces to PARI and GAP, which are subject to the same restrictions (f needs to be irreducible with $\deg(f) \leq 11$ or $\deg(f) \leq 15$, depending on which interface is used).

Thus, for the first time, Galois groups of arbitrary rational polynomials can be determined using a freely available open source computer algebra package. For example, the Galois group of the Ehrhart polynomial (of degree 16) of the 16-dimensional Fano simplex of order $2^8 \cdot 8!$ (see Section 3) can be determined using OSCAR within 10 minutes, a computation which was previously impossible without MAGMA.

3   Ehrhart Polynomials of Lattice Polytopes

Let $P \in \mathbb{R}^d$ be a d-dimensional lattice polytope. Then the function $L_P(t) = |tP \cap \mathbb{Z}^d|$ is a polynomial in t of degree d; this is called the *Ehrhart polynomial* of P. Numerous facts are known about Ehrhart polynomials: *e.g.*, the leading coefficient is the volume of P, the constant term equals one, and the polynomial $d! \cdot L_P(t)$ has integral coefficients. Yet many questions remain open. For instance, it is unclear which polynomials arise as Ehrhart polynomials [6, Open Problem 3.43]. We refer to the monographs of Beck and Robins [6] and Ewald [16] for the general background.

Computing Ehrhart polynomials is a subtle task, which may involve triangulating the input and computing lattice points; see, *e.g.*, [6, Section 3.4] and [4]. Note that even computing the leading coefficient, which is the volume, is #*P*-hard [12]. Standard implementations include LATTE [3] and NORMALIZ [9]; both are available through interfaces in POLYMAKE and thus also in OSCAR. For comparisons and further implementations see [1].

Galois groups. Here we propose to investigate the Galois groups of Ehrhart polynomials, considered as polynomials over some algebraically closed extension of $\mathbb{Q}$, such as $\mathbb{C}$ or the algebraic closure of the *p*-adics. This extends ongoing research on the zeros of Ehrhart polynomials; see, *e.g.*, [5, 7] and their references as well as [6, Open Problem 3.44]. We start with a first example, which is straightforward. Its purpose is to exhibit that Ehrhart polynomials may be reducible.

Example 2. Let C be the *d*-dimensional cube $[-1,1]^d$. Its Ehrhart polynomial reads $L_C(t) = (2t+1)^d$, whose Galois group is trivial.

The next example is more interesting.

Example 3. Consider the *d*-simplex $S = \text{conv}\{e_1, e_2, \ldots, e_d, -e_1 - e_2 - \cdots - e_d\}$, whose normalized volume equals $d + 1$. Here the Ehrhart polynomial is

$$L_S(t) \ = \ \binom{t+d+1}{d+1} - \binom{t}{d+1} \ .$$

Its roots are determined in [7, Theorem 1.7].

The polytope S in the example above is sometimes called the *Fano simplex*. Employing the results of [7] one can prove the following.

Theorem 4. *The Galois group* $\text{Gal}(L_S(t))$ *over* $\mathbb{Q}$ *of the d-dimensional Fano simplex S is isomorphic to the wreath product* $C_2 \wr S_k$, *where* $k = \lfloor d/2 \rfloor$. *Its order is* $2^k k!$.

We show how to compute the Ehrhart polynomial and its Galois group for $d = 14$. This requires an installation of JULIA (Version ≥ 1.6), with OSCAR installed via `using Pkg; Pkg.add("Oscar")`. Timings are taken on an Apple M1, 16 GB and macOS version 11.6.

```
julia> using Oscar;

julia> S = fano_simplex(14)
A polyhedron in ambient dimension 14

julia> @time G = galois_group(ehrhart_polynomial(S))
```

```
 0.840115 seconds (3.59 M allocations: 280.822 MiB, 6.75% gc time)
(<permutation group of size 645120 with 9 generators>, Galois Context for
↪   15*t^14 + 105*t^13 + 24115*t^12 + 143325*t^11 + 7724717*t^10 +
↪   37312275*t^9 + 725938785*t^8 + 2681453775*t^7 + 21964438496*t^6 +
↪   56663366760*t^5 + 201186840400*t^4 + 310989260400*t^3 + 429952217472*t^2
↪   + 283465647360*t + 87178291200 and prime 59)


julia> describe(G[1])
"C2 x ((C2 x C2 x C2 x C2 x C2 x C2) : S7)"
```

Smooth Fano polytopes.   We conclude this note with an analysis of a particularly interesting class of lattice polytopes. Let $P \subset \mathbb{R}^d$ be a d-dimensional lattice polytope with the origin in the interior. Its *polar* is $P^\circ = \{y \in \mathbb{R}^d \mid \langle x, y \rangle \le 1 \text{ for all } x \in P\}$, which is again a d-dimensional polytope. The lattice polytope P is *reflexive* if P° is a lattice polytope [10, Section 2.4]. Further, the lattice polytope is said to be *smooth* if the primitive facet normal vectors in each normal cone form a $\mathbb{Z}$-basis of the ambient lattice $\mathbb{Z}^d$; see, *e.g.*, [10, Section 2.4]. In particular, smooth polytopes are necessarily simple. A *smooth Fano polytope* is a smooth and reflexive lattice polytope. Examples include the cube (Example 2) and the polar of the Fano simplex (Example 3). Notice that sometimes in the literature smoothness is associated with the face fan of P rather than the normal fan; see, *e.g.*, [2, 21, 22]. In that case our definition applies to the polar P°. Interest in reflexive polytopes comes from toric algebraic geometry and its applications to mathematical physics.

Example 5. The reflexive polytope $\mathrm{DP}(d) = \mathrm{conv}\{\pm e_1, \pm e_2, \dots, \pm e_d, \pm\mathbf{1}\}$ is the *del Pezzo polytope* of dimension d. Its polar $\mathrm{DP}(d)^\circ$ is smooth Fano if and only if d is even.

   The Ehrhart polynomials of the polars of the smooth Fano polytopes and their zeros have been investigated a lot; see, *e.g.*, [7, 21, 22] and references therein. Hegedüs and Kasprzyk [22, Theorem 1.5] proved that for P a smooth Fano polytope of dimension $d \le 5$ the roots of the Ehrhart polynomial $L_{P^\circ}(t)$ of the polar lie on the "critical line" of those points in $\mathbb{C}$ whose real part equals $-\frac{1}{2}$. Moreover, Hegedüs and Kasprzyk also showed that, up to lattice equivalence, there are precisely four smooth Fano 6-polytopes P such that the roots of $L_{P^\circ}(t)$ do *not* lie on the critical line. In [22, Example 1.7] these four polytopes are identified via the IDs 1895, 1930, 4853, and 5817 in the Graded Ring Database [31, 32], which stores the polars of all smooth Fano polytopes of dimension ≤ 6. The second but last example, which is the free sum $\mathrm{DP}(2) \oplus \mathrm{DP}(4)$, is special; see [2, Theorem 7(iii)]. An OSCAR computation reveals that the Galois group of its Ehrhart polynomial is isomorphic to S_3. In fact, $\mathrm{DP}(2) \oplus \mathrm{DP}(4)$ is the only polar of a smooth Fano 6-polytope such that the Ehrhart polynomial has Galois group of order six.

   OSCAR provides direct access to the database POLYDB [26] which extends the classification from [32] to dimension ≤ 8. The respective POLYDB IDs of (the polars of) the four

polytopes from [22, Example 1.7] read: F.6D.0803, F.6D.0720, F.6D.3154, and F.6D.2616. We can query POLYDB to obtain a tally of the orders of the Galois groups of the Ehrhart polynomials of the polars of all 7622 smooth Fano 6-polytopes:

```
julia> db = Polymake.Polydb.get_db();

julia> collection = db["Polytopes.Lattice.SmoothReflexive"];

julia> query = Dict("DIM"=>6);

julia> res = Polymake.Polydb.find(collection, query);

julia> E6 = [ ehrhart_polynomial(polarize(Polyhedron(P))) for P in res ];

julia> sort(MSet(order(galois_group(e)[1]) for e = E6).Dict)
OrderedCollections.OrderedDict{Int64, Int64} with 6 entries:
  4  => 623
  6  => 1
  8  => 22
  12 => 44
  16 => 310
  48 => 6622
```

4 Conclusion

The following question is immediate:

Question 6. *Which groups arise as Galois groups of Ehrhart polynomials?*

It is a deep open question whether each finite group occurs as some Galois group of a rational polynomial; see, *e.g.*, [24]. While it seems to be difficult to characterize all Ehrhart polynomials it may still be the case that the above question is simpler. For instance, it is known that each finite cyclic group occurs as the Galois group of some rational polynomial. Can these be chosen as Ehrhart polynomials?

Acknowledgments

References

[1] B. Assarf, E. Gawrilow, K. Herr, M. Joswig, B. Lorenz, A. Paffenholz, and T. Rehn. "Computing convex hulls and counting integer points with POLYMAKE". *Math. Program. Comput.* **9**.1 (2017), pp. 1–38. DOI.

[2] B. Assarf, M. Joswig, and A. Paffenholz. "Smooth Fano polytopes with many vertices". *Discrete Comput. Geom.* **52**.2 (2014), pp. 153–194. DOI.

[3] V. Baldoni, N. Berline, J. De Loera, B. Dutra, M. Kãűppe, S. Moreinis, G. Pinto, M. Vergne, and J. Wu. "A userâĂŹs guide for LATTE INTEGRALE (Version 1.7.2)". 2013. Link.

[4] A. Barvinok. *Integer points in polyhedra*. Zurich Lectures in Advanced Mathematics. European Mathematical Society (EMS), Zürich, 2008, pp. viii+191. DOI.

[5] M. Beck, J. A. De Loera, M. Develin, J. Pfeifle, and R. P. Stanley. "Coefficients and roots of Ehrhart polynomials". *Integer points in polyhedra—geometry, number theory, algebra, optimization*. Vol. 374. Contemp. Math. Amer. Math. Soc., Providence, RI, 2005, pp. 15–36. DOI.

[6] M. Beck and S. Robins. *Computing the continuous discretely. Integer-Point Enumeration in Polyhedra*. Second Edition. Undergraduate Texts in Mathematics. With illustrations by David Austin. Springer, New York, 2015. DOI.

[7] C. Bey, M. Henk, and J. M. Wills. "Notes on the roots of Ehrhart polynomials". *Discrete Comput. Geom.* **38**.1 (2007), pp. 81–98. DOI.

[8] W. Bosma, J. Cannon, and C. Playoust. "The Magma algebra system. I. The user language". *J. Symbolic Comput.* **24**.3-4 (1997). Computational algebra and number theory (London, 1993), pp. 235–265. DOI.

[9] W. Bruns and C. Söger. "The computation of generalized Ehrhart series in NORMALIZ". *J. Symbolic Comput.* **68**.part 2 (2015), pp. 75–86. DOI.

[10] D. A. Cox, J. B. Little, and H. K. Schenck. *Toric varieties*. Vol. 124. Graduate Studies in Mathematics. American Mathematical Society, Providence, RI, 2011, pp. xxiv+841. DOI.

[11] W. Decker, G.-M. Greuel, G. Pfister, and H. Schönemann. "SINGULAR 4-3-0 — A computer algebra system for polynomial computations". 2022. Link.

[12] M. E. Dyer and A. M. Frieze. "On the complexity of computing the volume of a polyhedron". *SIAM J. Comput.* **17**.5 (1988), pp. 967–974. DOI.

[13] C. Eder, W. Decker, C. Fieker, M. Horn, and M. Joswig, eds. *The OSCAR book*. 2024.

[14] Y. Eichenlaub. "ProblÃĺmes effectifs de thÃ©orie de Galois en degrÃ©s 8 Ãă 11". ThÃĺse. UniversitÃ© Bordeaux, 1996.

[15] A.-S. Elsenhans. "Improved methods for the construction of relative invariants for permutation groups". *J. Symbolic Comput.* **79**.part 2 (2017), pp. 211–231. DOI.

[16] G. Ewald. *Combinatorial convexity and algebraic geometry*. Vol. 168. Graduate Texts in Mathematics. Springer-Verlag, New York, 1996. DOI.

[17] C. Fieker, W. Hart, T. Hofmann, and F. Johansson. "Nemo/Hecke: Computer algebra and number theory packages for the Julia programming language". *Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation*. ISSAC '17. New York, NY, USA: ACM, 2017, pp. 157–164. DOI.

[18] C. Fieker and J. Klüners. "Computation of Galois groups of rational polynomials". *LMS J. Comput. Math.* **17**.1 (2014), pp. 141–158. DOI.

[19] *GAP – Groups, Algorithms, and Programming (Version 4.11.1)*. The GAP Group. 2021. Link.

[20] E. Gawrilow and M. Joswig. "POLYMAKE: a framework for analyzing convex polytopes". *Polytopes — Combinatorics and Computation (Oberwolfach, 1997)*. Vol. 29. DMV Sem. Basel: Birkhäuser, 2000, pp. 43–73. Link.

[21] G. Hegedüs, A. Higashitani, and A. Kasprzyk. "Ehrhart polynomial roots of reflexive polytopes". *Electron. J. Combin.* **26**.1 (2019), Paper No. 1.38, 27. DOI.

[22] G. Hegedüs and A. Kasprzyk. "Roots of Ehrhart polynomials of smooth Fano polytopes". *Discrete Comput. Geom.* **46**.3 (2011), pp. 488–499. DOI.

[23] A. Hulpke. "Galois groups through invariant relations". *Groups St. Andrews 1997 in Bath, II*. Vol. 261. London Math. Soc. Lecture Note Ser. Cambridge Univ. Press, Cambridge, 1999, pp. 379–393. DOI.

[24] G. Malle and B. H. Matzat. *Inverse Galois theory*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 1999. DOI.

[25] "OSCAR – Open Source Computer Algebra Research system, (Version 0.8.2-DEV)". The OSCAR Team, 2022. Link.

[26] A. Paffenholz. "POLYDB: a database for polytopes and related objects". *Algorithmic and Experimental Methods in Algebra, Geometry, and Number Theory*. Springer, Cham, 2017, pp. 533–547.

[27] L. Soicher and J. McKay. "Computing Galois groups over the rationals". *J. Number Theory* **20**.3 (1985), pp. 273–281. DOI.

[28] R. P. Stauduhar. "The determination of Galois groups". *Math. Comp.* **27** (1973), pp. 981–996. DOI.

[29] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.4.0)*. 2022. Link.

[30] H. J. Zassenhaus. "Über die konstruktive Behandlung mathematischer Probleme". *Lectures at the Rhine–Westphalia Academy of Sciences, No. 307*. Westdeutscher Verlag, Opladen, 1982, pp. 7–52.

[31] M. Ã¥bro. "Smooth toric Fano varieties online database". http://www.grdb.co.uk/forms/toricsmooth.

[32] M. Ã¥bro. "An algorithm for the classification of smooth Fano polytopes". 2007. arXiv: 0704.0049.