Using Buchbergers algorithm in invariant theory

Manfred Göbel

Universität Tübingen, FRG

December 4, 1993

Abstract

This paper shows how Groebner bases theory could be used in invariant theory. It presents algorithms for representation, basis-construction and -test for the ring $\mathrm{Inv}_{G_n}^K$ of G_n-invariant polynomials over the field K for any given group G_n of permutations.

1 Introduction

Bases for rings of G_n-invariant polynomials for any given group G_n of permutations could be easly computed using the results of E. Noether [Noether16] or [Göbel92].

Moreover, the theorem of E. Noether as well as the results of [Göbel92] provides an algorithm to find a representation of a polynomial $f \in \mathrm{Inv}_{G_n}^K$ as a polynomial in a subset of the G_n-invariant polynomials of a basis. Both algorithms have been implemented in a computer algebra system and have proven to perform well. Their only lack is, that they do not use the knowledge of the basis, i.e. they find the needed subset of basis polynomials for the representation of a polynomial $f \in \mathrm{Inv}_{G_n}^K$ in every computation once again. This note presents an algorithm to find the representation of a given polynomial $f \in \mathrm{Inv}_{G_n}^K$ by using the explicit given basis polynomials through Gröbner bases theory [Becker93].

The plan of the paper is as follow: Section 2 presents the basic definitions and gives a short overview over the above mentioned reduction methods. Section 3 contains the details of the representation algorithm and algorithms for basis-construction and -test. Finally, section 4 illustrates the methods by a few examples obtained by an implementation of the algorithms in the computer algebra system MAS [Kredel91].

A part of the results of this note were obtained during the authors time at the university of Passau. The author would like to thank Prof. Dr. Weispfenning (Passau) and Prof. Dr. Küchlin (Tübingen) for the support of this work.

2 Basics

N is the set of all natural numbers including zero, R is a commutative ring with 1, K is field, $K[X_1, \ldots, X_n]$ is the commutative polynomial ring over K in the indeterminantes X_i, T_n is the sets of terms (= power-products of the X_i) in $K[X_1, \ldots, X_n]$, $M_n = \{at \mid a \in K, t \in T_n\}$ is the set of monomials in $K[X_1, \ldots, X_n]$, and $T_n(f)$, $M_n(f)$ is the set of terms and monomials in $f \in K[X_1, \ldots, X_n]$ with non-zero coefficients, respectively. $deg(t)$ ($deg(f)$) is the total degree of $t \in T_n$ ($f \in K[X_1, \ldots, X_n]$).

An admissible order on T_n is a linear order $<$ on T_n which turns $(T_n, 1, \cdot, <)$ into an ordered multiplicative monoid with smallest element 1. $AO(T_n)$ is the set of all admissible orders on T_n. Any admissible order on T_n extends the divisibility relation on T_n; moreover, it induces in a natural way a linear quasiorder $<$ on $K[X_1, \ldots, X_n]$: $f < g$ iff there exists $t \in T_n(g) \setminus T_n(f)$ such that for all $\hat{t} > t$, $\hat{t} \in T_n(f)$ iff $\hat{t} \in T_n(g)$. Both the admissible order on T_n and the induced quasiorder on $K[X_1, \ldots, X_n]$ are well-founded (Noetherian), i.e. admit no infinite, strictly decreasing chain. This is a consequence of the fundamental lemma that is due to Dickson (1913) [Becker93].

For a fixed admissible order $<$ on T_n and $f \in K[X_1, \ldots, X_n]$, we let $HT(f)$, $HC(f)$, $HM(f)$ (the highest monomial, highest term, highest coefficient of f) denote the highest term t w.r.t. $<$ in $T_n(f)$, the coefficient a of t in f and the monimal at of f, respectively. $desc(X_1^{f_1} \ldots X_n^{f_n}) = X_1^{e_1} \ldots X_n^{e_n}$ with $\{f_1, \ldots, f_n\} = \{e_1, \ldots, e_n\}$ and $e_1 \geq \ldots \geq e_n$.

G_n is any finite permutation group operating on n indeterminates. The order of G_n is denoted by $| G_n |$. S_n, A_n, D_n and Z_n are the symmetric, alternating, dieder and cyclic permutation groups. $f \in K[X_1, \ldots, X_n]$ is G_n-invariant, if $f = \pi(f) := f(\pi(X_1), \pi(X_2), \ldots, \pi(X_n))$ for all $\pi \in G_n$. Then $\pi(a) = a$, $\pi(-f) = -\pi(f)$, $\pi(f_1 + f_2) = \pi(f_1) + \pi(f_2)$ and $\pi(f_1 \cdot f_2) = \pi(f_1) \cdot \pi(f_2)$ for f, $f_1, f_2 \in K[X_1, \ldots, X_n]$, $a \in K$ and $\pi \in G_n$.

$orbit_{G_n}(t) = \sum_{s \in \{\pi(t) | \pi \in G_n\}} s$ is the G_n-invariant orbit of $t \in T_n$. Then $orbit_{G_n}(t)$ is G_n-invariant, $deg(orbit_{G_n}(t)) = deg(t)$, and if $f \in \mathrm{Inv}_{G_n}^K$ and $at \in M_n(f)$, then $M_n(a \cdot orbit_{G_n}(t)) \subseteq M_n(f)$. $f \in \mathrm{Inv}_{G_n}^K$ iff f is a finite K-linearcombination of G_n-invariant orbits.

Ω_{G_n} is the symmetry operator for the group G_n with $\Omega_{G_n}(f) = \frac{1}{|G_n|} \sum_{\pi \in G_n} \pi(f)$. Then $\Omega_{G_n}(f_1 + f_2) = \Omega_{G_n}(f_1) + \Omega_{G_n}(f_2)$ and $\Omega_{G_n}(af) = a\Omega_{G_n}(f)$, for f, $f_1, f_2 \in K[X_1, \ldots, X_n]$ and $a \in K$. It is obvious, that $f \in \mathrm{Inv}_{G_n}^K \iff f = \Omega_{G_n}(f)$ and that $deg(f) = deg(\Omega_{G_n}(f))$.
$\mathrm{Inv}_{G_n}^K$ is the commutative ring with 1 of G_n-invariant polynomials in $K[X_1, \ldots, X_n]$. A finite subset $\{\psi_1, \ldots, \psi_k\}$ of G_n-invariant orbits of $\mathrm{Inv}_{G_n}^K \setminus K$ is a finite basis of $\mathrm{Inv}_{G_n}^K$, if $\mathrm{Inv}_{G_n}^K = \{f(\psi_1, \ldots, \psi_k) \mid f \in K[X_1, \ldots, X_k]\}$. $\mathrm{Inv}_{G_n}^K$ is finitely generated, if $\mathrm{Inv}_{G_n}^K$ has a finite basis.

The theorem of E. Noether shows, that $\mathrm{Inv}_{G_n}^K$ has a finite basis, if $char(K) = 0$. This basis is the set of all G_n-invariant orbits with total degree $\leq |G_n|$. The proof of the theorem is constructive and provides therefore a method based on comparsion of coefficients for the computation of a represention of any G_n-invariant orbit in $\mathrm{Inv}_{G_n}^K$. The theorem does not hold for polynomial rings over fields with $char(K) \neq 0$ and even more, it is wrong over an arbitrary ground ring R.

The work reported in [Göbel92] presents a top-down-reduction method and shows, that $\mathrm{Inv}_{G_n}^K$ has a finite basis. This basis is the set of all special G_n-invariant orbits with maximal variable degree $\leq max\{1, n-1\}$ and total degree $\leq max\{n, n(n-1)/2\}$. The standard algorithm reduces every non special orbit, and furthermore, the method works for arbitrary ground rings R. Special G_n-invariant orbits are defined as follow: Let $t = X_1^{e_1} \ldots X_n^{e_n} \in T_n$ and let $I \subseteq \{1, \ldots, n\}$ a set of indices. Then t is k-connected w.r.t. I, if the following conditions are satisfied:

1. $|I| = k$ and $max\{e_1, \ldots, e_n\} = max\{e_i \mid i \in I\}$
2. The absolute difference between the decreasing ordered elements of the set $\{e_i \mid i \in I\}$

is less than one.

t is maximal k-connected, if t is not $(k+1)$-connected or $k = n$. $f \in K[X_1, \ldots, X_n]$ is (maximal) k-connected, if t is (maximal) k-connected for all $t \in T_n(f)$. Let $t = X_1^{e_1} \ldots X_n^{e_n} \in T_n$ maximal n-connected and let $e_i = 0$ for a $1 \le i \le n$ or $e_1 = \ldots = e_n = 1$. Then t is a special term and $orbit_{G_n}(t)$ is a special G_n-invariant orbit. It is obvious, that every special G_n-invariant orbit has a maximal variable degree $\le max\{1, n-1\}$ and total degree $\le max\{n, n(n-1)/2\}$ and that there exists only a finite number of special G_n-invariant orbits.

$RGB(.)$ $(ERGB(.))$ is the (extended) Buchberger algorithm. Then for any finite $C = \{f_1, \ldots, f_l\} \subset K[X_1, \ldots, X_n]$ $\{p_1, \ldots, p_r\} = RGB(C)$ $(\{p_1 = \sum g_{1i} f_i, \ldots, p_r = \sum g_{ri} f_i\} = ERGB(C))$ is the (extended) reduced Groebner basis of the finitely generated ideal $Id(C)$ w.r.t. a given term order $< \in AO(T_n)$.

3 Representation, basis-construction and -test

Lemma 3.1 Let $B = \{\psi_1, \ldots, \psi_l\}$ a finite basis of $\mathrm{Inv}_{G_n}^K$ and $P = RGB(B)$. Then $f \in \mathrm{Inv}_{G_n}^K \Longrightarrow f \in Id(B)$ and $f \in \mathrm{Inv}_{G_n}^K \Longrightarrow f \xrightarrow[P]{} 0$.

Proof $f \in \mathrm{Inv}_{G_n}^K \Longrightarrow f = p(\psi_1, \ldots, \psi_l), p \in K[X_1, \ldots, X_l] \Longrightarrow f \in Id(B) \Longrightarrow f \xrightarrow[P]{} 0$. □

Lemma 3.2 Let $B_1 = \{\psi_1, \ldots, \psi_{l_1}\}$, $B_2 = \{\gamma_1, \ldots, \gamma_{l_2}\}$ finite bases of $\mathrm{Inv}_{G_n}^K$. Then $Id(B_1) = Id(B_2)$.

Proof

1. $Id(B_1) \subseteq Id(B_2)$: $f \in Id(B_1) \Longrightarrow f = \sum_{i=1}^{l_1} g_i \psi_i = \sum_{i=1}^{l_1} g_i p_i(\gamma_1, \ldots, \gamma_{l_2}) = \sum_{i=1}^{l_2} h_i \gamma_i$ $\Longrightarrow f \in Id(B_2)$.
2. $Id(B_2) \subseteq Id(B_1)$: $f \in Id(B_2) \Longrightarrow f = \sum_{i=1}^{l_2} \hat{g}_i \gamma_i = \sum_{i=1}^{l_2} \hat{g}_i \hat{p}_i(\psi_1, \ldots, \psi_{l_1}) = \sum_{i=1}^{l_1} \hat{h}_i \psi_i$ $\Longrightarrow f \in Id(B_1)$. □

Lemma 3.3 There exists an algorithm for every finite basis B of $\mathrm{Inv}_{G_n}^K$, which represents any $f \in \mathrm{Inv}_{G_n}^K$ as a polynomial over the field K in the polynomials of the finite basis B.

Proof We present such an algorithm:

Algorithm 3.4

1. INPUT $f \in \mathrm{Inv}_{G_n}^K$; finite basis $B = \{\psi_1, \ldots, \psi_l\}$ of $\mathrm{Inv}_{G_n}^K$; $\{p_1 = \sum_{i=1}^l g_{1i} \psi_i, \ldots, p_r = \sum_{i=1}^l g_{ri} \psi_i\} = ERGB(B))$; term order $< \in AO(T_n)$;
2. IF $f \in K$ THEN $q := f$; RETURN; ENDIF;
3. $f := \sum_{i=1}^r g_i p_i = \sum_{i=1}^l \hat{g}_i \psi_i$;
4. $f := \Omega_{G_n}(f) = \sum_{i=1}^l \Omega(\hat{g}_i) \psi_i$;

5. FOR $i = 1$ TO l DO Recursive call for $\Omega_{G_n}(\hat{g}_i)$ $\left[\begin{array}{rcl} q_i & \in & K[X_1, \ldots, X_l] \\ \Omega_{G_n}(\hat{g}_i) & = & q_i(\psi_1, \ldots, \psi_l) \end{array} \right]$;
6. $q := \sum_{i=1}^{l} q_i X_i$;
7. OUTPUT $q \in K[X_1, \ldots, X_l]$ with $f = q(\psi_1, \ldots, \psi_l)$;

Termination & correctness Termination is obvious, because $deg(\Omega_{G_n}(\hat{g}_i)) < deg(f)$ for $1 \leq i \leq l$. The algorithm is correct, because every $f \in \mathrm{Inv}_{G_n}^K$ has a representation as a polynomial over the field K in the G_n-invariant orbits of the finite basis B.
This proves lemma 3.3. □

Corollary 3.5 Let B a finite basis of $\mathrm{Inv}_{G_n}^K$ and $\hat{B} \subseteq \mathrm{Inv}_{G_n}^K \setminus K$ finite with $RGB(\hat{B}) = RGB(B)$ w.r.t. $< \in AO(T_n)$. Then $\hat{B}$ is a finite basis of $\mathrm{Inv}_{G_n}^K$.

Proof This is a direct consequence of lemma 3.3 and algorithm 3.4. □
Corollary 3.5 enables us to decide

- if any arbitrary finite subset of $\mathrm{Inv}_{G_n}^K \setminus K$ is a basis of $\mathrm{Inv}_{G_n}^K$, and furthermore,
- if a subset of a finite basis of $\mathrm{Inv}_{G_n}^K$ is a finite basis of $\mathrm{Inv}_{G_n}^K$.

Lemma 3.6 There exists an algorithm to decide, if a finite subset $B \subseteq \mathrm{Inv}_{G_n}^K \setminus K$ is a basis of $\mathrm{Inv}_{G_n}^K$.

Proof We present such an algorithm:

Algorithm 3.7

1. INPUT $B = \{\psi_1, \ldots, \psi_l\} \subseteq \mathrm{Inv}_{G_n}^K \setminus K$; term order $< \in AO(T_n)$;
2. $ISorNOT := RGB(B) = RGB(\{orbit_{G_n}(t) \mid t \in T_n \text{ special}\})$;
3. OUTPUT $ISorNOT :=$ true (false), if B is (not) a finite basis of $\mathrm{Inv}_{G_n}^K$;

Termination & correctness Termination is obvious. Correctness is a consequence of corollary 3.5, because $\{orbit_{G_n}(t) \mid t \in T_n \text{ special}\}$ is a basis of $\mathrm{Inv}_{G_n}^K$.
This proves lemma 3.6. □

Definition 3.8

1. Let $B = \{\psi_1, \ldots, \psi_l\}$ a finite basis of $\mathrm{Inv}_{G_n}^K$. Then B is called reduced, if $B \setminus \{\psi_i\}$ is not a finite basis of $\mathrm{Inv}_{G_n}^K$ for $1 \leq i \leq l$.
2. Let $< \in AO(T_n)$ and $B = \{f_1, \ldots, f_l\}$ with $f_i \in K[X_1, \ldots, X_n]$, $1 \leq i \leq l$. Then C $= (g_1, g_2, \ldots, g_l) := ord(B, <)$, if $\{g_1, \ldots, g_l\} = B$ and $g_1 \leq \ldots \leq g_l$, $g_1 := first(C)$ and $(g_2, \ldots, g_l) := red(C)$.
3. Let $< \in AO(T_n)$ and $B_1 = (f_{11}, \ldots, f_{1l_1})$, $B_2 = (f_{21}, \ldots, f_{2l_2})$ with $f_{ij} \in K[X_1, \ldots, X_n]$, $1 \leq i \leq 2$, $1 \leq j \leq l_1, l_2$. Then $B_1 <_M B_2$, if ($f_{1i} = f_{2i}$ for $1 \leq i < j$ and $f_{1j} < f_{2j}$ for a $j \in \{1, \ldots, \min\{l_1, l_2\}\}$) or ($f_{1i} = f_{2i}$ for $1 \leq i \leq l_1$ and $l_1 < l_2$).

Lemma 3.9 Let $< \in AO(T_n)$ and B a finite basis of $\mathrm{Inv}_{G_n}^K$. Then there exists an algorithm, which computes a finite basis $\hat{B} \subseteq B$, such that $ord(\hat{B},<) <_M ord(C,<)$ for every reduced finite basis $C \subseteq B$ of $\mathrm{Inv}_{G_n}^K$ with $C \neq B$.

Furthermore, the finite basis $\hat{B}$ is reduced, if $(\gamma_1,\ldots,\gamma_l) = ord(B,<)$ and $deg(\gamma_{k_1}) \leq deg(\gamma_{k_2})$ for all $1 \leq k_1 \leq k_2 \leq l$.

Proof We present such an algorithm:

Algorithm 3.10

1. INPUT $B = \{\psi_1,\ldots,\psi_l\}$ finite basis of $\mathrm{Inv}_{G_n}^K$; term order $< \in AO(T_n)$;
2. $\hat{B} := \emptyset$; $P := \emptyset$;
3. $L := ord(B,<)$;
4. WHILE $L \neq ()$ DO
5. $\quad\gamma := first(L)$; $L := red(L)$;
6. $\quad\gamma \xrightarrow[P]{} h$;
7. $\quad$IF $h \neq 0$ THEN $\hat{B} := \hat{B} \cup \{\gamma\}$; $P := RGB(P \cup \{h\})$; ENDIF;
8. $\quad$ENDWHILE;
9. OUTPUT finite basis $\hat{B}$ with $ord(\hat{B},<) <_M ord(C,<)$ for every reduced finite basis $C \subseteq B$ of $\mathrm{Inv}_{G_n}^K$ with $C \neq \hat{B}$;

Termination & correctness The algorithm terminates, because B is a finite set of G_n-invariant orbits. For the correctness assume, that there exists a reduced finite basis $C \subseteq B$ with $C \neq \hat{B}$ such that $(\gamma_1,\ldots,\gamma_{l_1}) = ord(C,<) <_M ord(\hat{B},<) = (\hat{\psi}_1,\ldots\hat{\psi}_{l_2})$. Then there exists a $1 \leq j \leq l_2$ with $\gamma_i = \hat{\psi}_i$ for $1 \leq i < j$ and $\gamma_j < \hat{\psi}_j$. Then $\gamma_j \xrightarrow[P]{} 0$ with $P = RGB(\{\gamma_1,\ldots,\gamma_{j-1}\}) = RGB(\{\hat{\psi}_1,\ldots\hat{\psi}_{j-1}\})$. $\Longrightarrow C \setminus \{\gamma_j\}$ is a finite basis (contradiction).

Assume now, that $(\gamma_1,\ldots,\gamma_l) = ord(B,<)$ such that $deg(\gamma_{k_1}) \leq deg(\gamma_{k_2})$ for all $1 \leq k_1 \leq k_2 \leq l$ and $\hat{B}$ with $(\hat{\psi}_1,\ldots\hat{\psi}_{l_2}) = ord(\hat{B},<)$ is not reduced. Then there exists a max. $j < l_2$ such that $\hat{B} \setminus \{\hat{\psi}_j\}$ is a basis of $\mathrm{Inv}_{G_n}^K$.

$$\Longrightarrow \hat{\psi}_j \notin Id(\hat{\psi}_1,\ldots,\hat{\psi}_{j-1}),\ \hat{\psi}_j \in Id(\hat{\psi}_1,\ldots,\hat{\psi}_{j-1},\hat{\psi}_{j+1},\ldots,\hat{\psi}_{l_2})$$
$$\Longrightarrow \hat{\psi}_j = \textstyle\sum_{i<j} h_i\hat{\psi}_i + \sum_{i>j} h_i\hat{\psi}_i$$
$$\Longrightarrow h_i \in K \text{ for } i > j \text{ and } deg(\hat{\psi}_i) = deg(\hat{\psi}_j)$$
$$\Longrightarrow h_i = 0 \text{ for } i > j \text{ and } deg(\hat{\psi}_i) > deg(\hat{\psi}_j)$$
$$\Longrightarrow \exists\, k > j \text{ with } \hat{\psi}_k = \textstyle\sum_{i<k} g_i\hat{\psi}_i$$
$$\Longrightarrow \hat{\psi}_k \in Id(\hat{\psi}_1,\ldots,\hat{\psi}_{k-1}) \Longrightarrow \hat{\psi}_k \notin \hat{B} \text{ (contradiction)}$$

This proves lemma 3.9. $\square$

4 Examples

Definition 4.1 Let $t_1, t_2 \in T_n$. Then $orbit_{G_n}(t_1) <^*_{lex} orbit_{G_n}(t_2)$, if $(desc(t_1) <_{lex} desc(t_2))$ or $(desc(t_1) =_{lex} desc(t_2)$ and $orbit_{G_n}(t_1) <_{lex} orbit_{G_n}(t_2))$.

Remark 4.2 Algorithm 3.10 computes for every n with $<_{lex}$ as term order a smallest finite basis B of $\mathrm{Inv}^Q_{S_n}$ ($\mathrm{Inv}^Q_{A_n}$) for $B = \{orbit_{S_n}(t) \mid t \in T_n \text{ special}\}$ ($B = \{orbit_{A_n}(t) \mid t \in T_n \text{ special}\}$) and $L := ord(B, <^*_{lex})$. The polynomials in B are the elementary symmetric polynomials (and $orbit_{A_n}(X_1^{n-1}X_2^{n-2}\dots X_{n-2}^2X_n)$).

Examples 4.3 The following complete lists of highest terms of G_n-invariant orbits of a finite basis of $\mathrm{Inv}^Q_{G_n}$ as well as the numbers of G_n-invariant orbits in the tables below where obtained by using algorithm 3.10 with $<_{lex}$ as term order, $B = \{orbit_{G_n}(t) \mid t \in T_n \text{ special}\}$ and $L := ord(B, <^*_{lex})$.

- $\mathrm{Inv}^Q_{Z_1}$, $\mathrm{Inv}^Q_{D_1}$: X_1
- $\mathrm{Inv}^Q_{Z_2}$, $\mathrm{Inv}^Q_{D_2}$: X_1, X_1X_2
- $\mathrm{Inv}^Q_{Z_3}$: X_1, X_1X_2, $X_1X_2X_3$, $X_1^2X_3$
- $\mathrm{Inv}^Q_{Z_4}$: X_1, X_1X_3, X_1X_2, $X_1X_2X_3$, $X_1X_2X_3X_4$, $X_1^2X_4$, $X_1^2X_3X_4$
- $\mathrm{Inv}^Q_{Z_5}$: X_1, X_1X_3, X_1X_2, $X_1X_2X_4$, $X_1X_2X_3$, $X_1X_2X_3X_4$, $X_1X_2X_3X_4X_5$, $X_1^2X_5$, $X_1^2X_4$, $X_1^2X_4X_5$, $X_1^2X_3X_5$, $X_1^2X_3X_4$, $X_1^2X_3X_4X_5$, $X_1^2X_2X_4X_5$, $X_1^2X_2X_3X_5$
- $\mathrm{Inv}^Q_{D_3}$: X_1, X_1X_2, $X_1X_2X_3$
- $\mathrm{Inv}^Q_{D_4}$: X_1, X_1X_3, X_1X_2, $X_1X_2X_3$, $X_1X_2X_3X_4$
- $\mathrm{Inv}^Q_{D_5}$: X_1, X_1X_3, X_1X_2, $X_1X_2X_4$, $X_1X_2X_3$, $X_1X_2X_3X_4$, $X_1X_2X_3X_4X_5$, $X_1^2X_3X_4$, $X_1^2X_2X_3X_5$

References

[Becker93] Becker, T., Weispfenning, V.: In cooperation with H. Kredel: Groebner Bases: a computational approach to commutative algebra, Springer, New York, 1993

[Göbel92] Göbel, M.: Reduktion G-symmetrischer Polynome für beliebige Permutationsgruppe G, Diploma thesis, Universität Passau, WS 1991/92

[Kredel91] Kredel, H.: MAS, Modula-2 Algebra System, Interactive Usage, Definition Modules, Indexes, Computer Algebra Group, University of Passau, MAS Version 0.6, 1991

[Noether16] Noether, E.: Der Endlichkeitssatz der Invarianten endlicher Gruppen, Mathe. Ann. 77, 1916, S. 89-92

	Number of S_n-invariant orbits over Q			
n	special	total degree $\leq \lvert S_n \rvert$	special/total degree $\leq \lvert S_n \rvert$	basis
1	1	1	1	1
2	2	3	2	2
3	4	22	4	3
4	8	1291	8	4
5	16	...	16	5
6	32	...	32	6

	Number of A_n-invariant orbits over Q			
n	special	total degree $\leq \lvert A_n \rvert$	special/total degree $\leq \lvert A_n \rvert$	basis
1	1	1	1	1
2	3	2	2	2
3	5	7	5	4
4	9	181	9	5
5	17	...	17	6
6	33	...	33	7

	Number of D_n-invariant orbits over Q			
n	special	total degree $\leq \lvert D_n \rvert$	special/total degree $\leq \lvert D_n \rvert$	basis
1	1	1	1	1
2	2	3	2	2
3	4	22	4	3
4	14	91	14	5
5	61	346	61	9
6	414	1724	294	12
7	3416	8576	1481	26

	Number of Z_n-invariant orbits over Q			
n	special	total degree $\leq \lvert Z_n \rvert$	special/total degree $\leq \lvert Z_n \rvert$	basis
1	1	1	1	1
2	2	3	2	2
3	5	7	5	4
4	20	19	11	7
5	109	51	27	15
6	784	159	89	20
7	6757	491	266	49