Invariant Theory of Finite Groups

University of Leicester, March 2004

Jürgen Müller

Abstract

This introductory lecture will be concerned with polynomial invariants of finite groups which come from a linear group action. We will introduce the basic notions of invariant theory, discuss the structural properties of invariant rings, comment on computational aspects, and finally present two applications from function theory and number theory.

Keywords are: polynomial rings, graded commutative algebras, Hilbert series, Noether normalization, Cohen-Macaulay property, primary and secondary invariants, symmetric groups, reflection groups, ...

Contents

1 Symmetric polynomials

In Section 1 we introduce the most basic example of group invariants, namely the symmetric polynomials. As a reference see [10, Ch.4.6].

(1.1) Remark. Let F be a field, let $X := \{X_1, \ldots, X_n\}$, for $n \in \mathbb{N}_0$, be a finite set of algebraically independent indeterminates over F, and let $F[X] := F[X_1, \ldots, X_n]$ be the corresponding polynomial ring. Note that $F[X]$ is the free commutative F-algebra with free generators X.

Let $\mathcal{S}_n \cong \mathcal{S}_X$ denote the symmetric group on X, acting from the right on X. As $\pi \in \mathcal{S}_X$ permutes X, this induces an F-algebra automorphism $\pi\colon F[X] \to F[X]$, and hence a right action of $\mathcal{S}_X$ on $F[X]$.

Note that, if $f \in F[X]$ is homogeneous of degree $\deg_X(f) = d \in \mathbb{N}_0$, then $f\pi \in F[X]$ also is homogeneous and we have $\deg_X(f\pi) = d$.

(1.2) Definition. A polynomial $f \in F[X]$ is called **symmetric**, if $f\pi = f$ for all $\pi \in \mathcal{S}_X$.

Let $F[X]^{\mathcal{S}_X} := \{f \in F[X]; f \text{ symmetric}\} \subseteq F[X]$. As $\mathcal{S}_X$ acts by F-algebra automorphisms of $F[X]$, the subset $F[X]^{\mathcal{S}_X}$ is a subring of $F[X]$, containing the constant polynomials $1 \cdot F \cong F$, thus $F[X]^{\mathcal{S}_X}$ an F-subalgebra of $F[X]$, called the corresponding **invariant ring**.

We describe the structure of the invariant ring $F[X]^{\mathcal{S}_X}$.

(1.3) Definition. a) Let Y be an indeterminate over $F[X]$. Then we have

$$\prod_{i=1}^{n}(Y - X_i) = Y^n + \sum_{i=1}^{n}(-1)^i e_i Y^{n-i} \in F[X][Y],$$

where the $e_i \in F[X]$, for $i \in \{1, \ldots, n\}$, are the **elementary symmetric polynomials** $e_i := \sum_{1 \le j_1 < j_2 < \cdots < j_i \le n}(\prod_{k=1}^{i} X_{j_k}) \in F[X]$.

Hence $e_i \in F[X]$ is symmetric and homogeneous, and we have $\deg_X(e_i) = i$. Note that in particular we have $e_1 = \sum_{i=1}^{n} X_i$ and $e_n = \prod_{i=1}^{n} X_i$.

b) For a monomial $X^\alpha := \prod_{i=1}^{n} X_i^{\alpha_i} \in F[X]$, for $\alpha = [\alpha_1, \ldots, \alpha_n] \in \mathbb{N}_0^n$, let $\mathrm{wt}_X(X^\alpha) := \sum_{i=1}^{n} i\alpha_i \in \mathbb{N}_0$ be its **weight**. For $f \in F[X]$ let the weight $\mathrm{wt}_X(f) \in \mathbb{N}_0$ be defined as the maximum of the weights of the monomials occurring in f.

(1.4) Theorem. Let $f \in F[X]$ be symmetric such that $\deg_X(f) = d$. Then there is $g \in F[X]$ such that $\mathrm{wt}_X(g) \le d$ and $f = g(e_1, \ldots, e_n)$.

Proof. Induction on n, the case $n = 1$ is clear, hence let $n > 1$. Induction on d, the case $d = 0$ is clear, hence let $d > 0$.

Substituting $X_i \mapsto X_i$ for $i \in \{1, \ldots, n-1\}$, while $X_n \mapsto 0$ and $Y \mapsto Y$ in Definition (1.3) yields $Y \cdot \prod_{i=1}^{n-1}(Y - X_i) = Y^n + \sum_{i=1}^{n-1}(-1)^i e'_i Y^{n-i} \in F[X][Y]$, where the $e'_i := e_i(X_1, \ldots, X_{n-1}, 0) \in F[X]$, for $i \in \{1, \ldots, n-1\}$, are the elementary symmetric polynomials in the indeterminates $\{X_1, \ldots, X_{n-1}\}$.

By induction there is $g' \in F[X]$ such that $\mathrm{wt}_X(g') \leq d$ and $f(X_1, \ldots, X_{n-1}, 0) = g'(e'_1, \ldots, e'_{n-1})$. As the e_i are homogeneous and $\deg_X(e_i) = i$, we conclude that $\deg_X(g'(e_1, \ldots, e_{n-1})) \leq d$. Let $f' := f - g'(e_1, \ldots, e_{n-1}) \in F[X]$, hence $\deg_X(f') \leq d$ as well. As $f'(X_1, \ldots, X_{n-1}, 0) = 0$, we conclude that $f' \in F[X_1, \ldots, X_{n-1}][X_n]$ is divisible by X_n. As $f' \in F[X]$ is symmetric, and the $X_i \in F[X]$ are pairwise non-associate primes, we have $f' = f'' \cdot e_n \in F[X]$.

Hence $f'' \in F[X]$ is symmetric and we have $\deg_X(f'') \leq d - n < d$. Thus by induction there is $g'' \in F[X]$ such that $\mathrm{wt}_X(g'') \leq d - n$ and $f'' = g''(e_1, \ldots, e_n)$. Thus $f = g'(e_1, \ldots, e_{n-1}) + e_n \cdot g''(e_1, \ldots, e_n)$, where $\mathrm{wt}_X(g' + X_n g'') \leq d$. ♯

Note that the Proof of Theorem (1.4) is constructive: A given $f \in F[X]$ is written algorithmically as a polynomial g in the elementary symmetric polynomials; see Exercise (8.1). Corollary (1.7) shows that g is uniquely determined.

(1.5) Corollary. The invariant ring $F[X]^{\mathcal{S}_X}$ is as an F-algebra generated by the elementary symmetric polynomials $\{e_1, \ldots, e_n\}$.

(1.6) Theorem. The set $\{e_1, \ldots, e_n\} \subseteq F[X]$ is algebraically independent.

Proof. Induction on n, the case $n = 1$ is clear, hence let $n > 1$. Assume to the contrary, that there is $0 \neq f \in F[X]$ of minimal degree, such that $f(e_1, \ldots, e_n) = 0$. Let $f = \sum_{i=0}^{d} f_i(X_1, \ldots, X_{n-1}) X_n^i \in F[X_1, \ldots, X_{n-1}][X_n]$.

If $f_0 = 0$, then we have $f = X_n \cdot f'$ and hence $f'(e_1, \ldots, e_n) = 0$, where $f' \neq 0$ and $\deg_X(f') < \deg_X(f)$, a contradiction. Thus we have $f_0 \neq 0$. Substituting $X_n \mapsto 0$ as in the Proof of Theorem (1.4), we from the above expression for f obtain $0 = f(e'_1, \ldots, e'_{n-1}, 0) = f_0(e'_1, \ldots, e'_{n-1})$. By induction this contradicts to the algebraic independence of $\{e_1, \ldots, e_{n-1}\}$. ♯

(1.7) Corollary. The invariant ring $F[X]^{\mathcal{S}_X}$ is a polynomial ring in the indeterminates $\{e_1, \ldots, e_n\}$, i. e. we have $F[X]^{\mathcal{S}_X} \cong F[e_1, \ldots, e_n]$.

This leads to the following questions:
The invariant ring $F[X]^{\mathcal{S}_X} \subseteq F[X]$ is a finitely generated commutative F-algebra. Is this also true for subgroups of $\mathcal{S}_X$, or even more generally for linear actions of finite groups, as are considered from Section 2 on? How can we find generators, and which degrees do they have?
The invariant ring $F[X]^{\mathcal{S}_X} \subseteq F[X]$ even is a polynomial ring. By Exercise (8.2)

this is not always the case. What can be said in general about the structure of invariant rings? When are they polynomial rings? Is there always a 'large' polynomial subring of the invariant ring, as in the case of Exercise (8.2)?

2 Invariant rings

We introduce our basic objects of study. References, albeit using slightly different formalisms, are [1, Ch.1] or [12, Ch.1]. We assume the reader familiar with the basic notions of group representation theory. To make the objects of study precise we need some formalism; informally we are just forming the polynomial ring whose indeterminates are the elements of a basis of a vector space, see Proposition (2.2). The notation fixed in Definition (2.1) will be in force throughout.

(2.1) Definition and Remark. Let F be a field, let V be an F-vector space such that $n = \dim_F(V) \in \mathbb{N}_0$.

a) For $d \in \mathbb{N}$ the d-th **symmetric power** $S[V]_d := V^{\otimes d}/V'_d$ of V is defined as the quotient F-space of the d-th tensor power space $V^{\otimes d}$, where tensor products are taken over F, with respect to the F-subspace

$$V'_d := \langle v_1 \otimes \cdots \otimes v_d - v_{1\pi^{-1}} \otimes \cdots \otimes v_{d\pi^{-1}}; v_i \in V, \pi \in \mathcal{S}_d \rangle_F \leq V^{\otimes d}.$$

The **symmetric algebra** $S[V]$ over V is defined as $S[V] := \bigoplus_{d\in\mathbb{N}_0} S[V]_d$, where we let $S[V]_0 := 1 \cdot F \cong F$. It becomes a finitely generated commutative F-algebra, where multiplication is inherited from concatenation of tensor products, and where e. g. an F-basis $\{b_1, \ldots, b_n\} \subseteq V = S[V]_1$ of V is an F-algebra generating set of $S[V]$.

b) Let G be a group and let $D_V \colon G \to GL(V) \cong GL_n(F)$ be an F-representation of G. Hence the F-vector space V becomes an FG-module, where FG denotes the group algebra of G over the field F.

By diagonal G-action, $V^{\otimes d}$, for $d \in \mathbb{N}$, becomes an FG-module. As the $\mathcal{S}_d$-action and the G-action on $V^{\otimes d}$ commute, we conclude that $V'_d \leq V^{\otimes d}$ is an FG-submodule, and hence the quotient F-space $S[V]_d = V^{\otimes d}/V'_d$ is an FG-module as well. Let G act trivially on $S[V]_0 = 1 \cdot F$.

Moreover, G acts by F-algebra automorphisms on $S[V]$. Again, the corresponding **invariant ring** is defined as $S[V]^G := \{f \in S[V]; f\pi = f \text{ for all } \pi \in G\}$.

(2.2) Proposition. Let $S[V]$ be as in Definition (2.1). Then we have $S[V] \cong F[X]$ as F-algebras, where $F[X]$ is as in Remark (1.1).

Proof. Let $\{b_1, \ldots, b_n\} \subseteq V$ be an F-basis of V. As $F[X]$ is the free F-algebra on X, there is an F-algebra homomorphism $\alpha \colon F[X] \to S[V] \colon X_i \mapsto b_i$, for $i \in \{1, \ldots, n\}$. Conversely, by the defining property of tensor products, for $d \in \mathbb{N}_0$

there is an F-linear map $\beta_d\colon V^{\otimes d} \to F[X]\colon b_{i_1} \otimes b_{i_2} \otimes \cdots \otimes b_{i_d} \mapsto \prod_{k=1}^{d} X_{i_k}$, for $i_k \in \{1, \ldots, n\}$. Since $F[X]$ is commutative, we have $V_d' \leq \ker(\beta_d)$, and hence there is an F-linear map $\beta := \sum_{d \geq 0} \beta_d\colon S[V] \to F[X]$. Moreover, β is a ring homomorphism. Finally, we have $\alpha\beta = \mathrm{id}_{F[X]}$ and $\beta\alpha = \mathrm{id}_{S[V]}$. ♯

(2.3) Remark. Let $F[X]$ be given as in Remark (1.1), and let $V := F[X]_1 := \{f \in F[X]; \deg_X(f) = 1\} \cup \{0\}$. By Proposition (2.2) we get $S[V] \cong F[X]$ as F-algebras. Moreover, as $V = F[X]_1$ is an $F\mathcal{S}_X$-module, by Definition (2.1) we have an $\mathcal{S}_X$-action on $S[V]$, which indeed coincides with the $\mathcal{S}_X$-action on $F[X]$ given in Remark (1.1).

We introduce some important structural notions for commutative rings. Actually, although these notions are applicable to general commutative rings, they have originally been introduced by Hilbert and Noether for the examination of invariant rings. This leads to the first basic structure Theorem (2.9) on invariant rings.

(2.4) Definition and Remark. Let $R \subseteq S$ be an extension of commutative rings.
a) An element $s \in S$ is called **integral** over R, if there is $0 \neq f \in R[Y]$ monic, such that $f(s) = 0$. By Exercise (8.5) an element $s \in S$ is integral over R, if and only if there is a finitely generated R-submodule of S containing s. The ring extension $R \subseteq S$ is called **integral**, if each element of S is integral over R.

b) The ring extension $R \subseteq S$ is called **finite**, if S is a finitely generated R-algebra and integral over R. By Exercise (8.5) the ring extension $R \subseteq S$ is finite, if and only if S is a finitely generated R-module.

c) By Exercise (8.5) the subset $\overline{R}^S := \{s \in S; s \text{ integral over } R\} \subseteq S$ is a subring of S, called the **integral closure of** R in S. If $\overline{R}^S = R$ holds, then R is called **integrally closed in** S. If R is an integral domain and R is integrally closed in its field of fractions $\mathrm{Quot}(R)$, then R is called **integrally closed**.

(2.5) Proposition. Let $S(V) := \mathrm{Quot}(S[V])$ and let G be a finite group.
a) For the **invariant field** $S(V)^G \subseteq S(V)$ we have $S(V)^G = \mathrm{Quot}(S[V]^G)$, and the field extension $S(V)^G \subseteq S(V)$ is finite Galois with Galois group $G/\ker(D_V)$.
b) The invariant ring $S[V]^G$ is integrally closed.

Proof. a) We clearly have $\mathrm{Quot}(S[V]^G) \subseteq S(V)^G$. Conversely let $f = \frac{g}{h} \in S(V)^G$, for $g, h \in S[V]$. By extending with $\prod_{1 \neq \pi \in G} h\pi \in S[V]$ we may assume that $h \in S[V]^G$, and hence $g \in S[V]^G$ as well, thus $f \in \mathrm{Quot}(S[V]^G)$. By Artin's Theorem, see [10, Thm.6.1.8], the field extension $S(V)^G \subseteq S(V)$ is Galois.
b) If $f \in S(V)^G \subseteq S(V)$ is integral over $S[V]^G$, it is also integral over $S[V]$. As $S[V]$ is a unique factorization domain, from Exercise (8.5) we find that $S[V]$ is integrally closed in $S(V)$. Hence we have $f \in S[V]$, thus $f \in S[V]^G$. ♯

(2.6) Definition and Remark. Let R be a commutative ring.
a) An R-module M is called **Noetherian** if for each chain $M_0 \leq M_1 \leq \cdots M_i \leq \cdots \leq M$ of R-submodules there is $k \in \mathbb{N}_0$ such that $M_i = M_k$ for all $i \geq k$. The ring R is called **Noetherian**, if the R-module R_R is Noetherian.

b) By Exercise (8.6) we have: If M is Noetherian, then so are the R-submodules and the quotient R-modules of M. If R is Noetherian, then M is Noetherian if and only if M is a finitely generated R-module.

(2.7) Theorem: Hilbert's Basis Theorem, 1890.
Let R be a Noetherian commutative ring. Then the polynomial ring $R[Y]$ is Noetherian as well.

Proof. See [1, Thm.1.2.4] or [10, Thm.4.4.1]. ♯

(2.8) Corollary. A finitely generated commutative F-algebra is Noetherian.

(2.9) Theorem: Hilbert, 1890; Noether, 1916, 1926.
Let G be a finite group.
a) The ring extension $S[V]^G \subseteq S[V]$ is finite.
b) The invariant ring $S[V]^G$ is a finitely generated F-algebra.

Proof. a) Let $S := S[V]$. If $s \in S$, then for $f_s := \prod_{\pi \in G}(Y - s\pi) \in S^G[Y]$ we have $f_s(s) = 0$. As f_s is monic, the ring extension $S^G \subseteq S$ is integral. As S is finitely generated even as an F-algebra, the ring extension $S^G \subseteq S$ is finite.

b) Let $\{s_1, \ldots, s_k\} \subseteq S$ be an F-algebra generating set of S. Let $R \subseteq S^G \subseteq S$ be the F-algebra generated by the coefficients of the polynomials $\{f_{s_1}, \ldots, f_{s_k}\} \subseteq S^G[Y]$. As R is a finitely generated F-algebra, by Corollary (2.8) it is Noetherian. By the choice of R, the R-module S is finitely generated, and hence a Noetherian R-module. Thus by Definition (2.6), the R-submodule $S^G \leq S$ also is Noetherian, hence S^G is a finitely generated R-module. As R is a finitely generated F-algebra, S^G is a finitely generated F-algebra as well. ♯

The above Proof of Theorem (2.9) is purely non-constructive. At Hilbert's times this led to the famous exclamation of Gordan, then the leading expert on invariant theory and a dogmatic defender of the view that mathematics must be constructive: *Das ist Theologie und nicht Mathematik!* (*This is theology and not mathematics!*) Actually, Hilbert's ground breaking work now is recognized as the beginning and the foundation of modern abstract commutative algebra.

(2.10) Remark. The statement on finite generation in Theorem (2.9) does not hold for arbitrary groups. There is a famous counterexample by Nagata (1959), see [4, Ex.2.1.4]. But it holds for so-called **linearly reductive** groups, see the remarks after Definition (3.3). Actually, Hilbert worked on linearly reductive

groups, although this notion has only been coined later, while Noether developed the machinery for finite groups.

Moreover, the statement on finite generation in Theorem (2.9) is related to **Hilbert's 14th problem**, see [4, p.40]. If $K \subseteq S(V)$ is a subfield, is $K \cap S[V]$ a finitely generated algebra? As by definition $S(V)^G \cap S[V] = S[V]^G$ for any group G, Nagata's counterexample gives a negative answer to this problem as well.

3 Noether's degree bound

We turn attention to the question, whether we can possibly bound the degrees of the elements of an algebra generating set of an invariant ring. We collect the necessary tools, again partly general notions from commutative algebra.

(3.1) Definition. a) A commutative F-algebra R is called **graded**, if we have $R = \bigoplus_{d\geq 0} R_d$ as F-vector spaces, such that $R_0 = 1 \cdot F \cong F$ and $\dim_F(R_d) \in \mathbb{N}_0$ as well as $R_d R_{d'} \subseteq R_{d+d'}$, for $d, d' \geq 0$.

Note that R is a direct sum, i. e. for $0 \neq r = [r_d; d \geq 0] \in \bigoplus_{d\geq 0} R_d$ there is $k \in \mathbb{N}_0$ minimal such that $r_d = 0$ for all $d > k$; and the **degree** of r is defined as $\deg(r) = k \in \mathbb{N}_0$. The F-subspace $R_d \leq R$ is called the d-th **homogeneous component** of R. Let $R_+ := \bigoplus_{d>0} R_d \lhd R$ be the **irrelevant ideal**, i. e. the unique maximal ideal of R.

b) Let R be a graded F-algebra. An R-module M is called **graded**, if we have $M = \bigoplus_{d\geq N_M} M_d$ as F-vector spaces, for some $N_M \in \mathbb{Z}$, such that $\dim_F(M_d) \in \mathbb{N}_0$ as well as $M_d R_{d'} \subseteq M_{d+d'}$, for $d \geq N_M$ and $d' \geq 0$. For $0 \neq m \in M$ there is $k \geq N_M$ minimal such that $m_d = 0$ for all $d > k$; and the **degree** of m is defined as $\deg(m) = k \in \mathbb{Z}$. The F-subspace $M_d \leq M$ is called the d-th **homogeneous component** of M.

c) The **Hilbert series** (**Poincaré series**) $H_R \in \mathbb{C}[[T]] \subseteq \mathbb{C}((T))$ of a graded F-algebra R is the formal power series defined by $H_R(T) := \sum_{d\geq 0} \dim_F(R_d) T^d$. The **Hilbert series** (**Poincaré series**) $H_M \in \mathbb{C}((T))$ of a graded R-module M is the formal Laurent series defined by $H_M(T) := \sum_{d\geq N_M} \dim_F(M_d) T^d$.

(3.2) Remark. a) The symmetric algebra $S[V] := \bigoplus_{d\in\mathbb{N}_0} S[V]_d$, see Definition (2.1), is graded. The polynomial ring $F[X]$, see Remark (1.1), is graded as well, where the grading is given by the degree $\deg_X$. As the Proof of Proposition (2.2) shows, the isomorphism $\beta\colon S[V] \to F[X]$ of F-algebras indeed is an isomorphism of graded rings, i. e. for $f \in S[V]$ we have $\deg_X(f\beta) = \deg(f)$.

b) As the homogeneous components $S[V]_d$, for $d \in \mathbb{N}_0$, are FG-submodules of $S[V]$, the invariant ring $S[V]^G$ is graded as well, and we have $S[V]^G = \bigoplus_{d\geq 0} S[V]^G_d$, where indeed $S[V]_0 = 1 \cdot F$.

c) By Exercise (8.7) we have $\dim_F(F[X]_d) = \binom{n+d-1}{d}$, for $d \in \mathbb{N}_0$, hence we have $H_{F[X]} = \frac{1}{(1-T)^n} \in \mathbb{C}((T))$. Moreover, if $X' := \{X'_1, \ldots, X'_m\} \subseteq F[X]$, for $m \in \mathbb{N}_0$, is algebraically independent, where X'_i is homogeneous such that $\deg_X(X'_i) = d_i$, then we similarly obtain $H_{F[X']} = \prod_{i=1}^m \frac{1}{1-T^{d_i}} \in \mathbb{C}((T))$.

(3.3) Definition and Remark. a) Let $H \leq G$ such that $[G\colon H] < \infty$, and let $\mathcal{T} \subseteq G$ be a **right transversal** of H in G, i. e. a set of representatives of the right cosets $H|G$ of H in G. The **relative transfer map** Tr_H^G is defined as as the F-linear map

$$\mathrm{Tr}_H^G\colon S[V]^H \to S[V]^G\colon f \mapsto \sum_{\pi\in\mathcal{T}} f\pi.$$

If $|G| < \infty$, then the F-linear map $\mathrm{Tr}^G := \mathrm{Tr}^G_{\{1\}}\colon S[V] \to S[V]^G$ is called the **transfer map**.

b) It is easy to check that Tr_H^G is well-defined and independent of the choice of the transversal $\mathcal{T}$. Moreover, we have $\mathrm{Tr}_H^G|_{S[V]_d^H}\colon S[V]_d^H \to S[V]_d^G$, for $d \in \mathbb{N}_0$. Finally, for $f \in S[V]^G \subseteq S[V]^H$ and $g \in S[V]^H$ we have $\mathrm{Tr}_H^G(fg) = f \cdot \mathrm{Tr}_H^G(g)$. Hence Tr_H^G is a homomorphism of $S[V]^G$-modules, and as we have $\mathrm{Tr}_H^G(1) = 1 \cdot [G\colon H]$, we conclude $\mathrm{Tr}_H^G|_{S[V]^G}\colon f \mapsto f \cdot [G\colon H]$.

Moreover, we have $\mathrm{im}\,(\mathrm{Tr}_H^G) \trianglelefteq S[V]^G$. For G finite we by Exercise (8.8) have $\mathrm{im}\,(\mathrm{Tr}^G) \neq \{0\}$, but possibly $\mathrm{im}\,(\mathrm{Tr}^G) \neq S[V]^G$. We are better off under an additional assumption, which is quite natural from the viewpoint of group representation theory:

c) If $\mathrm{char}(F) \nmid [G\colon H]$, then the **relative Reynolds operator** $\mathcal{R}_H^G$ is the homomorphism of $S[V]^G$-modules defined by

$$\mathcal{R}_H^G := \frac{1}{[G\colon H]} \cdot \mathrm{Tr}_H^G\colon S[V]^H \to S[V]^G,$$

which by the above is a projection onto $S[V]^G$. If $\mathrm{char}(F) \nmid |G| < \infty$, using the surjective **Reynolds operator** $\mathcal{R}^G := \mathcal{R}^G_{\{1\}}\colon S[V] \to S[V]^G$ we in particular obtain $S[V] = S[V]^G \bigoplus \ker(\mathcal{R}^G)$ as $S[V]^G$-modules.

For G finite, the case $\mathrm{char}(F) \nmid |G|$ is called the **non-modular case**, otherwise it is called the **modular case**. The existence of the Reynolds operator in the non-modular case leads to another proof of the finite generation property of invariant rings, see Theorem (2.9). Note that in the Proof of Theorem (3.5) only the formal property of $\mathcal{R}^G\colon S[V] \to S[V]^G$ being a degree preserving $S[V]^G$-module projection is used.

More generally, the groups which possess a **generalized Reynolds operator** are called **linearly reductive**, see [4, Ch.2.2]. As the generalized Reynolds operator shares the above formal properties with the Reynolds operator, the Proof of Theorem (3.5) remains valid for linearly reductive groups.

(3.4) Definition and Remark. a) The ideal, generated by all homogeneous invariants of positive degree, $\mathcal{I}_G[V] := S[V]^G_+ \cdot S[V] = (S[V]_+ \cap S[V]^G) \cdot S[V] \lhd S[V]$ is called the **Hilbert ideal** of $S[V]$ with respect to G.
b) By Corollary (2.8) the F-algebra $S[V]$ is Noetherian, hence by Definition (2.6) the Hilbert ideal $\mathcal{I}_G[V] \lhd S[V]$ is generated by a finite set of homogeneous invariants. Note that $\mathcal{I}_G[V] \lhd S[V]$ is a **homogeneous ideal**, i. e. for $f \in S[V]$ we have $f \in \mathcal{I}_G[V]$ if and only if $f_d \in \mathcal{I}_G[V]$ for all $d \in \mathbb{N}_0$.

(3.5) Theorem. Let G be a finite group such that $\mathrm{char}(F) \not| \, |G|$. Let $\mathcal{I}_G[V] = \sum_{i=1}^r f_i S[V] \lhd S[V]$, where $f_i \in S[V]$ is homogeneous. Then $\{f_1, \ldots, f_r\}$ is an F-algebra generating set of $S[V]^G$.

Proof. Let $h \in S[V]^G$ homogeneous such that $\deg(h) = d$. We proceed by induction on d, the case $d = 0$ is clear, hence let $d > 0$. Let $h = \sum_{i=1}^r f_i g_i$, for $g_i \in K[V]_{d-\deg(f_i)}$. By Definition (3.3) we have $h = \mathcal{R}^G(h) = \sum_{i=1}^r f_i \cdot \mathcal{R}^G(g_i)$. As $\deg(\mathcal{R}^G(g_i)) = d - \deg(f_i) < d$ we are done by induction. ♯

We are prepared to prove Noether's degree bound, which holds in the non-modular case. Actually, Noether stated the result only for the case $\mathrm{char}(F) = 0$, but her proof is valid for the case $|G|! \neq 0 \in F$. Finally Fleischmann closed the gap to all non-modular cases. We present a proof based on a simplification due to Benson.

(3.6) Proposition: Benson's Lemma, 2000.
Let G be a finite group such that $\mathrm{char}(F) \not| \, |G|$, and let $\mathcal{I} \trianglelefteq S[V]$ be an FG-invariant ideal. Then we have $\mathcal{I}^{|G|} \subseteq (\mathcal{I} \cap S[V]^G) \cdot S[V] \trianglelefteq S[V]$.

Proof. Let $S := S[V]$ and $\{f_\pi; \pi \in G\} \subseteq \mathcal{I}$. Then we have $\prod_{\pi \in G}(f_\pi \pi\sigma - f_\pi) = 0$, for $\sigma \in G$. Expanding the product and summing over $\sigma \in G$ yields

$$\sum_{M \subseteq G} (-1)^{|G \setminus M|} \cdot \left(\sum_{\sigma \in G} \prod_{\pi \in M} f_\pi \pi\sigma \right) \cdot \left(\prod_{\pi \in G \setminus M} f_\pi \right) = 0,$$

where the sum runs over all subsets $M \subseteq G$. If $M \neq \emptyset$, then we have $(\sum_{\sigma \in G} \prod_{\pi \in M} f_\pi \pi\sigma) \in \mathcal{I} \cap S^G$, and thus the corresponding summand of the above sum is an element of $(\mathcal{I} \cap S^G) \cdot S$. Hence for $M = \emptyset$ we from this obtain $\pm|G| \cdot (\prod_{\pi \in G} f_\pi) \in (\mathcal{I} \cap S^G) \cdot S$, hence $(\prod_{\pi \in G} f_\pi) \in (\mathcal{I} \cap S^G) \cdot S$. ♯

(3.7) Theorem: Noether, 1916; Fleischmann, 2000.
Let G be a finite group such that $\mathrm{char}(F) \not| \, |G|$. Then there is an ideal generating set of the Hilbert ideal $\mathcal{I}_G[V] \lhd S[V]$ all of whose elements are homogeneous of degree $\leq |G|$.

Proof. See [4, Ch.3.8] or [12, Thm.2.3.3].
Let $S := S[V]$. Using the identification from Proposition (2.2), let $X^\alpha \in S$ be a monomial of degree $\geq |G|$. By Proposition (3.6), applied to the irrelevant ideal $S_+ \lhd S$, we have $X^\alpha \in (S_+ \cap S^G) \cdot S = \mathcal{I}_G[V] \lhd S$. If $\deg(X^\alpha) > |G|$, let $X^\alpha = X^{\alpha'} \cdot X^{\alpha''}$, such that $\deg(X^{\alpha'}) = |G|$. Hence we already have $X^{\alpha'} \in \mathcal{I}_G[V]$,

Let $\mathcal{I}_G[V] = \sum_{i=1}^r f_i S \lhd S$ be a minimal homogeneous generating set, where $\deg(f_r) > |G|$, say. By the above we conclude that $f_r \in \sum_{j,\deg(f_j)\leq|G|} f_j S \lhd S$, a contradiction. ♯

(3.8) Corollary. There is an F-algebra generating set of $S[V]^G$ all of whose elements are homogeneous of degree $\leq |G|$.

(3.9) Remark. a) By Theorems (3.5) and (3.7), an F-algebra generating set of $S[V]^G$ is found in $\bigoplus_{d=1}^{|G|} S[V]_d^G$. Using the degree-preserving surjective Reynolds operator, see Definition (3.3), we have $\mathcal{R}^G(\bigoplus_{d=1}^{|G|} S[V]_d) = \bigoplus_{d=1}^{|G|} S[V]_d^G$. Hence evaluating the Reynolds operator at monomials X^α, where $\deg(X^\alpha) \leq |G|$, yields a, not necessarily minimal, F-algebra generating set of $S[V]^G$. For an example see Exercise (8.9).

b) Noether's degree bound is best possible in the sense that no improvement is possible in terms of the group order alone: Let $G = \langle \pi \rangle \cong C_n$ be the cyclic group of order n, let F be a field such that $\mathrm{char}(F) \not| \, n$, let $\zeta \in F$ be a primitive n-th root of unity, and let $G \to GL_1(F) \colon \pi \mapsto \zeta$. Hence the invariant ring is $S[V]^G \cong F[X_1^n] \subseteq F[X_1] \cong S[V]$.

For more involved improvements of Noether's degree bound, see [4, Ch.3.8]. Actually, in most practical non-modular cases both Noether's degree bound and its improvements are far from being sharp.

c) In the modular case, Noether's degree bound does not hold, see Exercise (8.10). For some known but unrealistic degree bounds, see [4, Ch.3.9]. Even Benson's Lemma, see Proposition (3.6), does not hold in the modular case, see Exercise (8.11).

4 Molien's Formula

For all of Section 4 let G be a finite group and let $F \subseteq \mathbb{C}$. The aim is to use character theory of finite groups to determine the Hilbert series of invariant rings. As a general reference, see [12, Ch.3.1], [4, Ch.3.2] and [1, Ch.2.5].

(4.1) Proposition. For $\pi \in G$ we have

$$\sum_{d\geq 0} \mathrm{Tr}_{S[V]_d}(\pi) \cdot T^d = \frac{1}{\det_V(1 - T\pi)} \in F((T)),$$

where $\mathrm{Tr}_{S[V]_d}(\pi) \in F$ denotes the usual matrix trace, and where $1 - T \cdot D_V(\pi) \in F[T]^{n \times n}$ and $\det_V(1 - T\pi) := \det_{F[T]^{n\times n}}(1 - T \cdot D_V(\pi)) \in F[T]$.

Proof. We may assume $\mathbb{Q}[\zeta_{|G|}] \subseteq F$, where $\zeta_{|G|} := \exp \frac{2\pi i}{|G|} \in \mathbb{C}^*$ is a primitive $|G|$-th root of unity. Hence $D_{S[V]_d}(\pi) \in F^{n\times n}$ is diagonalizable. In particular, let $\lambda_1, \ldots, \lambda_n \in F$ be the eigenvalues of $D_V(\pi)$. Hence we have $\det_V(1 - T\pi) = \prod_{i=1}^n (1 - \lambda_i T) \in F[T]$.

Moreover, the eigenvalues of $D_{S[V]_d}(\pi)$ are $\prod_{i=1}^n \lambda_i^{\alpha_i} \in F$, where $\alpha \in \mathbb{N}_0^n$ such that $\sum_{i=1}^n \alpha_i = d$. Thus we have $\sum_{d\geq 0} \mathrm{Tr}_{S[V]_d}(\pi) \cdot T^d = \sum_{\alpha \in \mathbb{N}_0^n} \prod_{i=1}^n (\lambda_i T)^{\alpha_i} = \prod_{i=1}^n \sum_{j\geq 0} (\lambda_i T)^j = \prod_{i=1}^n \frac{1}{1-\lambda_i T} \in F((T))$. ♯

(4.2) Theorem: Molien's Formula, 1897.
We have $H_{S[V]^G} = \frac{1}{|G|} \cdot \sum_{\pi \in G} \frac{1}{\det_V(1-T\pi)} \in F((T))$.

Proof. The Reynolds operator $\mathcal{R}^G$, see Definition (3.3), projects $S[V]_d$ onto $S[V]_d^G$, for $d \in \mathbb{N}_0$. Using this we obtain $\dim_F(S[V]_d^G) = \mathrm{Tr}_{S[V]_d}(\mathcal{R}^G) = \frac{1}{|G|} \sum_{\pi \in G} \mathrm{Tr}_{S[V]_d}(\pi) \in F$. Hence the assertion follows from Proposition (4.1). ♯

(4.3) Remark. a) By Molien's Formula, see Theorem (4.2), the Hilbert series $H_{S[V]^G} \in F(T)$ even is a rational function.

b) To evaluate Molien's Formula, note that $\det_V(1 - T\pi) = \prod_{i=1}^n (1 - \lambda_i T) = T^n \cdot \prod_{i=1}^n (T^{-1} - \lambda_i)$ for $\pi \in G$. Thus by Definition (1.3) we get $\det_V(1 - T\pi) = T^n \cdot \big(T^{-n} + \sum_{i=1}^n (-1)^i e_i(\lambda_1, \ldots, \lambda_n) T^{i-n}\big) = 1 + \sum_{i=1}^n (-1)^i e_i(\lambda_1, \ldots, \lambda_n) T^i \in F[T]$. By the Newton identities, see Exercise (8.4), the elementary symmetric polynomials $e_i(\lambda_1, \ldots, \lambda_n) \in F$, for $i \in \{1, \ldots, n\}$, can be determined from the power sums $p_{n,j}(\lambda_1, \ldots, \lambda_n) \in F$, for $j \in \{1, \ldots, n\}$. Finally, we have $p_{n,j}(\lambda_1, \ldots, \lambda_n) = \sum_{i=1}^n \lambda_i^j = \mathrm{Tr}_V(\pi^j) = \chi_V(\pi^j) \in \mathbb{C}$, where $\chi_V \in \mathbb{Z}\mathrm{Irr}_{\mathbb{C}}(G)$ denotes the ordinary character of G afforded by V.

Hence Molien's Formula can be evaluated once χ_V and the so-called **power maps** $p_j \colon \mathcal{C}l(G) \to \mathcal{C}l(G)$, for $j \in \{1, \ldots, n\}$, on the conjugacy classes $\mathcal{C}l(G)$ of G are known. This information is usually contained in the available character table libraries, e. g. the one of the computer algebra system GAP [6], and actually Molien's Formula also is implemented there.

c) There is a straightforward generalization of Molien's Formula to the non-modular case, for $\mathrm{char}(F) = p > 0$ using p-modular Brauer characters of G, see see [12, Ch.3.1] or [4, Ch.3.2].

(4.4) Example. For $k \in \mathbb{N}$ let $G = \langle \delta, \sigma \rangle \cong D_{2k}$ be the dihedral group of order $2k$, let $\zeta_k := \exp \frac{2\pi i}{k} \in \mathbb{C}^*$ be a k-th primitive root of unity, and let

$$D_V \colon G \to GL_2(\mathbb{C}) \colon \delta \mapsto \begin{bmatrix} \zeta_k & \cdot \\ \cdot & \zeta_k^{-1} \end{bmatrix}, \sigma \mapsto \begin{bmatrix} \cdot & 1 \\ 1 & \cdot \end{bmatrix}.$$

We have $G = \{\delta^i, \sigma\delta^i; i \in \{0, \ldots, k-1\}\}$, where $\delta^i \in G$ is a rotation having the eigenvalues $\zeta_k^{\pm i} \in \mathbb{C}$, and where $\sigma\delta^i \in G$ is a reflection, hence having the eigenvalues $\pm 1 \in \mathbb{C}$. Thus by Molien's Formula, see Theorem (4.2), the Hilbert series of $S[V]^G$ is given as

$$H_{S[V]^G} = \frac{1}{2k} \cdot \left(\frac{k}{(1-T)\cdot(1+T)} + \sum_{i=0}^{k=1} \frac{1}{(1-\zeta_k^i T)\cdot(1-\zeta_k^{-i} T)} \right) \in \mathbb{C}((T)).$$

Using Exercise (8.12), where the rightmost summand is evaluated, we straightforwardly obtain $H_{S[V]^G} = \frac{1}{(1-T^2)\cdot(1-T^k)} \in \mathbb{C}((T))$.

Hence by Exercise (8.7) we are tempted to conjecture that $S[V]^G$ is a polynomial ring in two indeterminates of degrees $2, k$. Indeed, using the identification from Proposition (2.2), we have $f_1 := X_1 X_2 \in S[V]^G$ and $f_2 := X_1^k + X_2^k \in S[V]^G$. By the Jacobian Criterion, see Proposition (5.8) below, we easily conclude that $\{f_1, f_2\} \subseteq \mathbb{C}[X_1, X_2]$ is algebraically independent, and hence the Hilbert series of $\mathbb{C}[f_1, f_2] \subseteq S[V]^G$ is given as $H_{\mathbb{C}[f_1,f_2]} = \frac{1}{(1-T^2)\cdot(1-T^k)} \in \mathbb{C}((T))$. Thus we conclude $\mathbb{C}[f_1, f_2] = S[V]^G$, which hence indeed is a polynomial ring. ♯

5 Polynomial invariant rings

We address the question, whether we can characterize the representations whose invariant ring is a polynomial ring, the main result being Theorem (5.9). We begin by considering the Laurent expansion of $H_{S[V]^G}$ at $T = 1$, which straightforwardly leads to a consideration of pseudoreflections. As a general reference see [7, Ch.3], [1, Ch.2.5, Ch.7] or [12, Ch.7.1].

For all of Section 5 let G be a finite group, let $F \subseteq \mathbb{C}$, and let D_V be a **faithful** F-representation, i. e. we have $\ker(D_V) = \{1\} \leq G$.

(5.1) Definition. a) An element $1 \neq \pi \in G$ is called a **pseudoreflection** if for the F-space $\mathrm{Fix}_V(\pi) \leq V$ of fixed points of $\pi \in G$ we have $\dim_F \mathrm{Fix}_V(\pi) = n-1$, and if additionally $\pi^2 = 1$ then π is called a **reflection**. The F-space $\mathrm{Fix}_V(\pi) \leq V$ of fixed points of a pseudoreflection is called its **reflecting hyperplane**.

Let $N_G \in \mathbb{N}_0$ be the **number of pseudoreflections** in G. Note that these notions of course depend on the representation D_V, and make sense for an arbitrary field F.

b) For a rational function $0 \neq H = \frac{H'}{H''} \in \mathbb{C}(T)$, for coprime $H', H'' \in \mathbb{C}[T]$, and $c \in \mathbb{C}$ let $k \in \mathbb{Z}$ such that $\left((T-c)^{-k} \cdot H\right)(c) \neq 0, \infty$. Then $\mathrm{ord}_c(H) := k \in \mathbb{Z}$ is called the **order** of H at $T = c$. If $H = 0$ then let $\mathrm{ord}_c(H) := \infty$.

(5.2) Remark. As in the Proof of Proposition (4.1) let $\lambda_1, \ldots, \lambda_n \in F$ be the eigenvalues of $D_V(\pi)$, for $\pi \in G$. As $\det_V(1 - T\pi) = \prod_{i=1}^n (1 - \lambda_i T) \in F[T]$, we have $\mathrm{ord}_1(\det_V(1-T\pi)) \leq n$, while $\mathrm{ord}_1(\det_V(1-T\pi)) = n$ if and only if $\pi = 1$. Thus we have $\mathrm{ord}_1(H_{S[V]^G}) = -n$. Moreover, $\left((T-1)^n \cdot H_{S[V]^G}\right)(1) = \frac{(-1)^n}{|G|}$.

Let $H_{S[V]^G} = \frac{(-1)^n}{|G|} \cdot (T-1)^{-n} + H'_{S[V]^G} \in F(T)$. Hence we have $\mathrm{ord}_1(H'_{S[V]^G}) \geq -(n-1)$. Again we have $\mathrm{ord}_1(\det_V(1-T\pi)) = n-1$ if and only if $\pi \neq 1$ has the eigenvalue 1 with multiplicity $n-1$, i. e. if and only if π is a pseudoreflection. In this case, let $1 \neq \lambda \in F$ be the non-trivial eigenvalue of π. Hence we have $\left(\frac{(T-1)^{n-1}}{\det_V(1-T\pi)}\right)(1) = \frac{(-1)^{n-1}}{(1-\lambda)}$. As $\frac{1}{1-\lambda} + \frac{1}{1-\lambda^{-1}} = 1$, pairing each pseudoreflection with its inverse, and summing over all the pseudoreflections in G, yields $\left((T-1)^{n-1} \cdot H'_{S[V]^G}\right)(1) = \frac{(-1)^{n-1} \cdot N_G}{2 \cdot |G|}$. Thus we obtain

$$H_{S[V]^G} := \frac{(-1)^n}{|G|} \cdot (T-1)^{-n} + \frac{(-1)^{n-1} \cdot N_G}{2 \cdot |G|} \cdot (T-1)^{-(n-1)} + H''_{S[V]^G} \in F(T),$$

where $\mathrm{ord}_1(H''_{S[V]^G}) \geq -(n-2)$. ♯

We set out to prove one direction of Theorem (5.9), which will turn out to be the harder one. We need the technical Lemma (5.3) first.

(5.3) Lemma. Let G be generated by pseudoreflections, and let $R := S[V]^G \subseteq S[V] =: S$. Moreover, let $h_1, \ldots, h_r \in R$ and $h \in R \setminus (\sum_{i=1}^r h_i R)$, and let $p, p_1, \ldots, p_r \in S$ homogeneous such that $hp = \sum_{i=1}^r h_i p_i$. Then we have $p \in \mathcal{I}_G[V]$, where $\mathcal{I}_G[V] \lhd S$ denotes the Hilbert ideal, see Definition (3.4).

Proof. Induction on $\deg(p)$, let $\deg(p) = 0$ and $p \neq 0$. Hence we have $hp = \mathcal{R}^G(hp) = \sum_{i=1}^r h_i \cdot \mathcal{R}^G(p_i) \in \sum_{i=1}^r h_i R$, where $\mathcal{R}^G$ denotes the Reynolds operator, see Definition (3.3). This contradicts the choice of $h \in R$.

Let $\deg(p) > 0$. Let $\pi \in G$ be a pseudoreflection, and we may assume that its reflecting hyperplane is given as $\mathrm{Fix}_V(\pi) = \langle b_2, \ldots, b_n \rangle_F$, where $\{b_1, \ldots, b_n\} \subseteq V$ is an F-basis of V. Using the identification of Proposition (2.2) we obtain $X_i \pi = X_i$, for $i \geq 2$. Hence we have $X^\alpha(\pi - 1) = 0$ for all monomials $X^\alpha \in F[X]$, where $\alpha \in \mathbb{N}_0^n$ such that $\alpha_1 = 0$. From that we conclude that there are $p', p'_i \in S$ homogeneous such that $p(\pi - 1) = X_1 p' \in S$ and $p_i(\pi - 1) = X_1 p'_i \in S$, for $i \in \{1, \ldots, r\}$. In particular we have $\deg(p') < \deg(p)$. Applying $\pi - 1$ to the equation $hp = \sum_{i=1}^r h_i p_i$ we obtain $X_1 \cdot hp' = X_1 \cdot \sum_{i=1}^r h_i p'_i$. Hence by induction we have $p' \in \mathcal{I} := \mathcal{I}_G[V]$, and thus $p(\pi - 1) = X_1 p' \in \mathcal{I}$ as well.

Let $\overline{\ }: S \to S/\mathcal{I}$ denote the natural epimorphism of F-algebras. As $\mathcal{I} \lhd S$ is an FG-submodule, the group G acts on the quotient F-algebra $S/\mathcal{I}$. By the above we have $\overline{p}\pi = \overline{p}$ for all pseudoreflections $\pi \in G$, and as G is generated by pseudoreflections, we have $\overline{p}\pi = \overline{p}$ for all $\pi \in G$. Since $\mathcal{R}^G(p) \in R_+ \subseteq \mathcal{I}$ we conclude $p + \mathcal{I} = \mathcal{R}^G(p) + \mathcal{I} = 0 + \mathcal{I} \in S/\mathcal{I}$, hence $p \in \mathcal{I}$. ♯

(5.4) Theorem. Let G be generated by pseudoreflections. Then $S[V]^G$ is a polynomial ring.

Proof. We keep the notation of Lemma (5.3), and let $\mathcal{I} := \mathcal{I}_G[V] = \sum_{i=1}^{r} f_i S \lhd S$, where $f_i \in R$ is homogeneous such that $d_i := \deg(f_i)$, and $r \in \mathbb{N}_0$ is minimal. As by Theorem (3.5) the set $\{f_1, \ldots, f_r\} \subseteq R$ is an F-algebra generating set of R, it is sufficient to show that $\{f_1, \ldots, f_r\}$ is algebraically independent. Assume to the contrary that there is $0 \neq h \in F[Y] := F[Y_1, \ldots, Y_r]$ such that $h(f_1, \ldots, f_r) = 0$. We may assume that there is $d \in \mathbb{N}_0$ such that for all monomials $Y^\alpha \in F[Y]$, where $\alpha \in \mathbb{N}_0^r$, occurring in h we have $\sum_{i=1}^{r} \alpha_i d_i = d$.

Let $h_i := \frac{\partial h}{\partial Y_i}(f_1, \ldots, f_r) \in R$, for $i \in \{1, \ldots, r\}$. Hence we have $\deg(h_i) = d - d_i$. We may assume by reordering that $\sum_{i=1}^{r'} h_i R = \sum_{i=1}^{r} h_i R \trianglelefteq R$, where $1 \leq r' \leq r$ is minimal. For $j > r'$ let $g_{ij} \in R$, for $i \in \{1, \ldots, r'\}$, be homogeneous such that $\deg(g_{ij}) = \deg(h_j) - \deg(h_i) = d_i - d_j$, and $h_j = \sum_{i=1}^{r'} h_i g_{ij} \in R$.

Differentiation $\frac{\partial}{\partial X_k}$, for $k \in \{1, \ldots, n\}$, using the chain rule yields

$$0 = \sum_{i=1}^{r} h_i \cdot \frac{\partial f_i}{\partial X_k} = \sum_{i=1}^{r'} h_i \cdot \left(\frac{\partial f_i}{\partial X_k} + \sum_{j=r'+1}^{r} g_{ij} \cdot \frac{\partial f_j}{\partial X_k} \right) \in S.$$

Let $p_i := \frac{\partial f_i}{\partial X_k} + \sum_{j=r'+1}^{r} g_{ij} \cdot \frac{\partial f_j}{\partial X_k} \in S$, for $i \in \{1, \ldots, r'\}$. Hence p_i is homogeneous such that $\deg(p_i) = d_i - 1$ or $p_i = 0$. By Lemma (5.3) we conclude that $p_1 \in \mathcal{I}$, thus $p_1 = \sum_{i=1}^{r} f_i q_i$, for homogeneous $q_i \in S$. Multiplying by X_k and summing over $k \in \{1, \ldots, n\}$, we by the Euler identity $\sum_{k=1}^{n} X_k \cdot \frac{\partial f}{\partial X_k} = \deg_X(f) \cdot f$, for $f \in S$, obtain $d_1 \cdot f_1 + \sum_{j=r'+1}^{r} d_j \cdot g_{1j} f_j = \sum_{i=1}^{r} f_i q_i'$, where $\deg(q_i') > 0$ or $q_i' = 0$. As the left hand side of this equation is homogeneous of degree d_1, the right hand side is as well. If $q_1' \neq 0$, then we have $\deg(f_1 q_1') > d_1$, hence the term $f_1 q_1'$ cancels with other terms of the same degree on the right hand side. From that we conclude that $f_1 \in \sum_{i=2}^{r} f_i S \lhd S$, a contradiction. ♯

(5.5) Proposition. Let $S[V]^G = F[f_1, \ldots, f_r]$ be a polynomial ring, where $f_i \in S[V]$ is homogeneous such that $\deg(f_i) = d_i$, and let $N_G \in \mathbb{N}_0$ be the number of pseudoreflections in G, see Definition (5.1). Then we have $r = n$ as well as $\prod_{i=1}^{n} d_i = |G|$ and $\sum_{i=1}^{n} (d_i - 1) = N_G$.

Proof. As $S[V]^G \cong F[Y] := F[Y_1, \ldots, Y_r]$, for the invariant field we have $S(V)^G \cong F(Y)$, where by Proposition (2.5) we have $r = \mathrm{tr.deg}(S(V)^G) = \mathrm{tr.deg}(S(V)) = n$, see [10, Ch.8.1].

By Remark (3.2) the Hilbert series of $S[V]^G$ is given as $H_{S[V]^G} = \prod_{i=1}^{n} \frac{1}{1 - T^{d_i}} = (-1)^n \cdot (T-1)^{-n} \cdot \prod_{i=1}^{n} \frac{1}{\sum_{j=0}^{d_i - 1} T^j} \in F((T))$. Using Remark (5.2) we by multiplication with $(-1)^n \cdot (T-1)^n$ obtain

$$\frac{1}{|G|} - \frac{N_G}{2 \cdot |G|} \cdot (T-1) + (-1)^n \cdot (T-1)^n \cdot H''_{S[V]^G} = \prod_{i=1}^{n} \frac{1}{\sum_{j=0}^{d_i - 1} T^j} \in F((T)),$$

where $\mathrm{ord}_1((T-1)^n \cdot H''_{S[V]^G}) \geq 2$. Evaluating at $T = 1$ yields $\frac{1}{|G|} = \prod_{i=1}^{n} \frac{1}{d_i}$.

By differentiating $\frac{\partial}{\partial T}$ the right hand side of the above equation we obtain $-\left(\prod_{i=1}^n \frac{1}{\sum_{j=0}^{d_i-1} T^j}\right) \cdot \left(\sum_{i=1}^n \frac{\sum_{j=1}^{d_i-1} jT^{j-1}}{\sum_{j=0}^{d_i-1} T^j}\right)$, and evaluating at $T = 1$ yields $-\left(\prod_{i=1}^n \frac{1}{d_i}\right) \cdot \sum_{i=1}^n \frac{d_i(d_i-1)}{2d_i}$. On the left hand side of the above equation we obtain $-\frac{N_G}{2\cdot|G|}$. Hence using $\prod_{i=1}^n d_i = |G|$ we get $N_G = \sum_{i=1}^n (d_i - 1)$. ♯

(5.6) Definition and Remark. a) Let $S[V]^G = F[f_1, \ldots, f_r]$ be a polynomial ring, where $f_i \in S[V]$ is homogeneous such that $\deg(f_i) = d_i$. The set $\{f_1, \ldots, f_n\} \subseteq S[V]^G$ is called a set of **basic invariants**. By Exercise (8.15) the degrees $d_i = \deg(f_i)$ of a set of basic invariants are uniquely defined up to reordering. They are called the **polynomial degrees** of G, where we may assume $d_1 \leq \cdots \leq d_n$.

b) Basic invariants are in general not uniquely defined, even not up to reordering and multiplication by scalars: Let $G = \mathcal{S}_n = \langle (1,2), \ldots, (n-1,n) \rangle$ be the symmetric group as in Section 1, acting on the polynomial ring $F[X]$ by permuting the indeterminates. Hence G is generated by reflections. By the Newton identities, see Exercise (8.4), Corollary (1.7) and the algebraic independence of $\{p_{n,1}, \ldots, p_{n,n}\}$, see Exercise (8.14), we have $F[X]^{\mathcal{S}_n} = F[e_1, \ldots, e_n] = F[p_{n,1}, \ldots, p_{n,n}]$.

We prove a general criterion, to decide whether an n element subset of a polynomial ring $F[X] = F[X_1, \ldots, X_n]$, where $\mathrm{char}(F) = 0$, is algebraically independent. This has already been used in Example (4.4). Just in Definition (5.7) and Proposition (5.8) we allow for more general fields F.

(5.7) Definition. For $\{f_1, \ldots, f_n\} \subseteq F[X] = F[X_1, \ldots, X_n]$ the **Jacobian matrix** is defined as $J(f_1, \ldots, f_n) := [\frac{\partial f_i}{\partial X_j}]_{i,j=1,\ldots,n} \in F[X]^{n \times n}$, its determinant $\det J(f_1, \ldots, f_n) \in F[X]$ is called the **Jacobian determinant**.

(5.8) Proposition: Jacobian Criterion.
Let $\mathrm{char}(F) = 0$. Then $\{f_1, \ldots, f_n\} \subseteq F[X] = F[X_1, \ldots, X_n]$ is algebraically independent, if and only if we have $\det J(f_1, \ldots, f_n) \neq 0 \in F[X]$.

Proof. Let $0 \neq h \in F[X]$ of minimal degree such that $h(f_1, \ldots, f_n) = 0$. Differentiation $\frac{\partial}{\partial X_j}$ using the chain rule yields the system of linear equations, over $F(X) = \mathrm{Quot}(F[X])$,

$$\left[\frac{\partial h}{\partial X_i}(f_1, \ldots, f_n)\right]_{i=1,\ldots,n} \cdot J(f_1, \ldots, f_n) = 0.$$

As $\deg_X(h) > 0$ and $\mathrm{char}(F) = 0$, there is $i \in \{1, \ldots, n\}$ such that $\frac{\partial h}{\partial X_i} \neq 0 \in F[X]$. As $\deg_X(\frac{\partial h}{\partial X_i}) < \deg_X(h)$, we also have $\frac{\partial h}{\partial X_i}(f_1, \ldots, f_n) \neq 0 \in F[X]$. Hence the above system of linear equations has a non-trivial solution, thus $\det J(f_1, \ldots, f_n) \neq 0 \in F[X]$.

Let conversely $\{f_1, \ldots, f_n\}$ be algebraically independent. As $\mathrm{tr.deg}(F(X)) = n$, see [10, Ch.8.1], for $k \in \{1, \ldots, n\}$ the sets $\{X_k, f_1, \ldots, f_n\}$ are algebraically dependent. Let $0 \neq h_k \in F[X_0, X_1, \ldots, X_n] = F[X^+]$ of minimal degree such that $h_k(X_k, f_1, \ldots, f_n) = 0$. Differentiation $\frac{\partial}{\partial X_j}$ yields

$$\left[\frac{\partial h_k}{\partial X_i}(X_k, f_1, \ldots, f_n)\right]_{k,i=1,\ldots,n} \cdot J(f_1, \ldots, f_n) = \mathrm{diag}\left[-\frac{\partial h_k}{\partial X_0}(X_k, f_1, \ldots, f_n)\right]_{k=1,\ldots,n}.$$

As $\{f_1, \ldots, f_n\}$ is algebraically independent, we have $\deg_{X_0}(h_k) > 0$. As $\mathrm{char}(F) = 0$ we get $\frac{\partial h_k}{\partial X_0} \neq 0 \in F[X^+]$, and as $\deg_{X^+}(\frac{\partial h_k}{\partial X_0}) < \deg_{X^+}(h_k)$ we have $\frac{\partial h_k}{\partial X_0}(X_k, f_1, \ldots, f_n) \neq 0 \in F[X^+]$. Hence $\det \mathrm{diag}[-\frac{\partial h_k}{\partial X_0}(X_k, f_1, \ldots, f_n)] \neq 0 \in F[X^+]$, and thus $\det J(f_1, \ldots, f_n) \neq 0 \in F[X]$. ♯

(5.9) Theorem: Shephard-Todd, 1954; Chevalley, 1955.
The invariant ring $S[V]^G$ is a polynomial ring if and only if G is generated by pseudoreflections.

Proof. By Theorem (5.4) it remains to show that if $S[V]^G$ is a polynomial ring, then G is generated by pseudoreflections. Using Proposition (5.5), let $S[V]^G = F[f_1, \ldots, f_n]$, where $f_i \in S[V]$ is homogeneous such that $d_i := \deg(f_i)$. Let $H \leq G$ be the subgroup generated by the pseudoreflections in G. Hence by Theorem (5.4) we have $S[V]^G \subseteq S[V]^H = F[g_1, \ldots, g_n] \subseteq S[V]$, where $g_i \in S[V]$ is homogeneous such that $e_i := \deg(g_i)$. Hence there are $h_i \in F[X]$ such that $f_i = h_i(g_1, \ldots, g_n)$, for $i \in \{1, \ldots, n\}$. We may assume that for all monomials $X^\alpha \in F[X]$, where $\alpha \in \mathbb{N}_0^n$, occurring in h_i we have $\sum_{i=1}^n \alpha_i e_i = d_i$.

Differentiation $\frac{\partial}{\partial X_k}$, for $k \in \{1, \ldots, n\}$, and the chain rule yield $J(f_1, \ldots, f_n) = \left[\frac{\partial h_i}{\partial X_j}(g_1, \ldots, g_n)\right]_{i,j=1,\ldots,n} \cdot J(g_1, \ldots, g_n) \in F[X]^{n \times n}$. By the Jacobian Criterion, see Proposition (5.8), we have $\det J(f_1, \ldots, f_n) \neq 0 \in F[X]$, thus $\det[\frac{\partial h_i}{\partial X_j}(g_1, \ldots, g_n)] \neq 0 \in F[X]$ as well. Hence by renumbering $\{f_1, \ldots, f_n\}$ we may assume that $\prod_{i=1}^n \frac{\partial h_i}{\partial X_i}(g_1, \ldots, g_n) \neq 0 \in F[X]$. Thus we have $d_i \geq e_i$, for $i \in \{1, \ldots, n\}$. Hence by Proposition (5.5) we have $\sum_{i=1}^n (d_i - 1) = N_G = N_H = \sum_{i=1}^n (e_i - 1)$, thus $e_i = d_i$ for $i \in \{1, \ldots, n\}$. Moreover we have $|G| = \prod_{i=1}^n d_i = \prod_{i=1}^n e_i = |H|$. ♯

(5.10) Remark. a) Shephard-Todd (1954) proved Theorem (5.9) by first classifying the finite groups generated by pseudoreflections, and then by a case-by-case analysis verified Theorem (5.4). Later, Chevalley (1955) gave a conceptual proof. For the Shephard-Todd classification of irreducible finite groups generated by pseudoreflections, to which one immediately reduces, see e. g. [1, Tbl.7.1] or [12, Tbl.7.1.1]. Actually, finite groups generated by pseudoreflections play an important role not only in invariant theory, but also in the representation theory of finite groups of Lie type, and currently are in the focus of intensive research.

b) The permutation action of the symmetric group $\mathcal{S}_n$ considered in Section 1 is a reflection representation, see Definition (5.6), but it is afforded by a reducible $\mathbb{Q}\mathcal{S}_n$-module. It is closely related to an irreducible $\mathbb{Q}\mathcal{S}_n$-reflection module, see Exercise (8.17). Another example of an irreducible reflection representation is the action of the dihedral group D_{2k} given in Example (4.4).

c) Theorem (5.9) remains valid in the non-modular case, as was proved by Serre (1967). Moreover, Serre proved that in the modular case, if an invariant ring is polynomial, then the group under consideration is generated by pseudoreflections. But the converse does not hold, see Exercise (8.18). A classification of polynomial invariant rings in the modular case, together with further aspects of invariant rings of pseudoreflection groups, has been given by Kemper-Malle (1997), see also [4, Ch.3.7].

6 Cohen-Macaulay algebras

As Section 5 shows, most of the invariant rings are not polynomial rings. Hence the question arises, which are their common structural features? It turns out in the non-modular case, that invariant rings are Cohen-Macaulay algebras, see Definition (6.9). We need more commutative algebra first, as general references see e. g. [4, Ch.2.4, Ch.2.5, Ch.3.4], [1, Ch.2, Ch.4.3], [12, Ch.4.5] and [5, Ch.12, Ch.13], [2].

(6.1) Theorem: Hilbert, Serre.
Let R be a finitely generated graded F-algebra, being generated as an F-algebra by $\{f_1, \ldots, f_t\} \subseteq R$, where f_i is homogeneous such that $\deg(f_i) = d_i > 0$. Let M be a finitely generated graded R-module, see Definition (3.1).

Then the Hilbert series $H_M \in \mathbb{C}((T))$ is of the form $H_M(T) = \frac{f(T)}{\prod_{i=1}^{t}(1-T^{d_i})} \in \mathbb{C}(T)$, where $f \in \mathbb{Z}[T^{\pm 1}]$ is a Laurent polynomial with integer coefficients. In particular, H_M converges in the pointed open unit disc $\{z \in \mathbb{C}; 0 < |z| < 1\} \subseteq \mathbb{C}$.

Proof. Induction on t, let $t = 0$. Hence $R = F$, and thus M is a F-vector space such that $\dim_F(M) < \infty$. Hence $H_M(T) = f(T) \in \mathbb{Z}[T^{\pm 1}] \subseteq \mathbb{C}(T)$. Let $t > 0$, and for $d \geq N_M$ consider the exact sequence of F-vector spaces

$$\{0\} \to M'_d := \ker_{M_d}(\cdot f_t) \to M_d \xrightarrow{\cdot f_t} M_{d+d_t} \to \operatorname{cok}_{M_{d+d_t}}(\cdot f_t) =: M''_{d+d_t} \to \{0\},$$

induced by multiplication with $f_t \in R$. As R is Noetherian, see Corollary (2.8), the sums $M' := \bigoplus_{d \geq N_M} M'_d$ and $M'' := \bigoplus_{d \geq N_M} M''_d$ are finitely generated graded R-modules, see Definition (2.6). As $M' \cdot f_t = \{0\} = M'' \cdot f_t$, these are finitely generated modules for the F-algebra generated by $\{f_1, \ldots, f_{t-1}\}$, hence by induction $H_{M'} \in \mathbb{C}(T)$ and $H_{M''} \in \mathbb{C}(T)$ have the asserted form. Moreover, the above exact sequence yields $T^{d_t} H_{M'} - T^{d_t} H_M + H_M - H_{M''} = 0 \in \mathbb{C}(T)$, and thus $H_M = \frac{H_{M''} - T^{d_t} H_{M'}}{1 - T^{d_t}} \in \mathbb{C}(T)$ also has the asserted form. ♯

(6.2) Definition. Let R be a finitely generated graded F-algebra, and let M be a finitely generated graded R-module. Then $\dim(M) := -\mathrm{ord}_1(H_M) \in \mathbb{Z}$, see Definition (5.1), is called the **Krull dimension** of M. Moreover, $\deg(M) := \big((1-T)^{\dim(M)} \cdot H_M(T)\big)(1) = \lim_{z \to 1^-}((1-z)^{\dim(M)} \cdot H_M(z)) \in \mathbb{Q}$ is called the **degree** of M.

(6.3) Example. Let $F[Y] = F[Y_1, \ldots, Y_r] \subseteq F[X] = F[X_1, \ldots, X_n]$, where Y_i are homogeneous such that $\deg_X(Y_i) = d_i$, then by Remark (3.2) the Hilbert series of $F[Y]$ is given as $H_{F[Y]} = \prod_{i=1}^{r} \frac{1}{1-T^{d_i}} \in \mathbb{C}(T)$, hence we have $\dim(F[Y]) = r$ and $\deg(F[Y]) = \prod_{i=1}^{r} \frac{1}{d_i}$.

Note that it is not a priorly clear that $\dim(M) \geq 0$ holds. This follows for the dimension of a graded F-algebra from graded Noether normalization, see Theorem (6.6) and Definition (6.7) below. Actually, using a more general variant of Noether normalization for modules, this also follows for the dimension of modules, see e. g. [1, Thm.2.7.7], but we will not use this fact.

(6.4) Theorem. Let R be a finitely generated graded F-algebra, and let $R \subseteq S$ be a finite extension of graded F-algebras, i. e. we have $S_d \cap R = R_d$ for $d \in \mathbb{N}_0$.
a) Then we have $\dim(R) = \dim(S)$.
b) If S is an integral domain, we have $\deg(S) = [\mathrm{Quot}(S) \colon \mathrm{Quot}(R)] \cdot \deg(R)$.

Proof. a) As S is a finitely generated R-module, it is the epimorphic image of a finitely generated free graded R-module A, i. e. the R-module A is a finite direct sum of degree shifted copies of the R-module R. Hence we have $H_A = f \cdot H_R \in \mathbb{C}(T)$, where $0 \neq f \in \mathbb{Z}^{\geq 0}[T]$. As $f(1) > 0$ we have $\dim(R) = \dim(A) =: r \in \mathbb{Z}$.

Moreover, for $d \geq 0$ we have $\dim_F(R_d) \leq \dim_F(S_d) \leq \dim_F(A_d)$, and thus by Theorem (6.1) for $z \in \mathbb{R}$ such that $0 < z < 1$ we have $H_R(z) \leq H_S(z) \leq H_A(z) \in \mathbb{R}$. Thus we also have $\lim_{z \to 1^-}((1-z)^r \cdot H_R(z)) \leq \lim_{z \to 1^-}((1-z)^r \cdot H_S(z)) \leq \lim_{z \to 1^-}((1-z)^r \cdot H_A(z))$, where the first and third limits exist in $\mathbb{R}$ and are different from 0, and hence the second limit also exists in $\mathbb{R}$ and is different from 0. Thus we have $\dim(S) = -\mathrm{ord}_1(H_S) = r$ as well.

b) As S is integral over R and a finitely generated R-algebra, the field extension $\mathrm{Quot}(R) \subseteq \mathrm{Quot}(S)$ indeed is finite, let $t := [\mathrm{Quot}(S) \colon \mathrm{Quot}(R)]$. Moreover, as S is a finitely generated R-module, there is a $\mathrm{Quot}(R)$-basis $\{f_1, \ldots, f_t\} \subseteq S$ of $\mathrm{Quot}(S)$ consisting of homogeneous elements. Let $A := \bigoplus_{i=1}^{t} f_i R \subseteq S$. Hence we have $H_A = f \cdot H_R \in \mathbb{C}(T)$, where $0 \neq f \in \mathbb{Z}^{\geq 0}[T]$ and $f(1) = t$. Moreover, as S is a finitely generated R-algebra, there is $f \in R$ homogeneous such that $S \subseteq f^{-1}A = \bigoplus_{i=1}^{t} f_i f^{-1} R \subseteq \mathrm{Quot}(S)$. We have $H_{f^{-1}A} = T^{-\deg(f)} \cdot H_A \in \mathbb{C}(T)$. Hence we have $\dim(S) = \dim(R) = \dim(A) = \dim(f^{-1}A)$ and $t \cdot \deg(R) = \deg(A) = \deg(f^{-1}A)$. Moreover, since $\dim_F(A_d) \leq \dim_F(S_d) \leq \dim_F((f^{-1}A)_d)$ for $d \in \mathbb{Z}$, we conclude $\deg(A) \leq \deg(S) \leq \deg(f^{-1}A)$. ♯

(6.5) Corollary. Let G be a finite group acting faithfully on the F-vector space V. Then we have $\dim(S[V]^G) = \dim_F(V)$ and $\deg(S[V]^G) = \frac{1}{|G|}$.

Proof. The extension of graded rings $S[V]^G \subseteq S[V]$ is finite, see Theorem (2.9). By Proposition (2.5) we have $[S(V)\colon S(V)^G] = |G|$. Hence the assertions follow from Theorem (6.4) together with Example (6.3). ♯

Note that for $F \subseteq \mathbb{C}$ the assertions of Corollary (6.5) also follow from Molien's Formula, see Theorem (4.2).

We present the main structure theorem for finitely generated graded commutative algebras, which is the case we are interested in. Actually, Noether normalization exists in various variations for various types of commutative algebras and for modules over them, see e. g. [5, Ch.13].

(6.6) Theorem: Graded Noether Normalization Lemma.
Let R be a finitely generated graded F-algebra. Then there is an algebraically independent set $\{f_1, \ldots, f_r\} \subseteq R$, for some $r \in \mathbb{N}_0$, where f_i is homogeneous such that $\deg(f_i) > 0$, such that R is finite over the polynomial ring $P := F[f_1, \ldots, f_r]$.

Proof. See [5, Thm.13.3] or [1, Thm.2.7.7]. ♯

(6.7) Definition and Remark. Let R be a finitely generated graded F-algebra, and let moreover $\{f_1, \ldots, f_r\} \subseteq R$ and P be as in Theorem (6.6). Note that by Definition (2.4) the finiteness condition is equivalent to R being a finitely generated P-module.
a) As by Remark (3.2) we have $H_P = \prod_{i=1}^{r} \frac{1}{1-T^{\deg(f_i)}} \in \mathbb{C}(T)$, we by Theorem (6.4) conclude that $r = \dim(P) = \dim(R) \in \mathbb{N}_0$ holds. In particular, r is uniquely defined, independent of the particular choice of $\{f_1, \ldots, f_r\}$. Moreover, we have $r = \dim(R) = 0$, if and only if $\dim_F(R) < \infty$.
b) Let R be an integral domain. As R is integral over P and a finitely generated P-algebra, the field extension $\mathrm{Quot}(P) \subseteq \mathrm{Quot}(R)$ is finite. Hence we have $\dim(R) = r = \mathrm{tr.deg}(\mathrm{Quot}(P)) = \mathrm{tr.deg}(\mathrm{Quot}(R))$, see [10, Ch.8.1].
c) The set $\{f_1, \ldots, f_r\} \subseteq R$ is called a **homogeneous system of parameters** (**hsop**) of R. If $R = S[V]^G$ is an invariant ring, then a homogeneous system of parameters is called a set of **primary invariants**. If $S[V]^G = \sum_{i=1}^{s} g_i P$ for some $s \in \mathbb{N}_0$, where g_i is homogeneous, then the set $\{g_1, \ldots, g_s\} \subseteq R$ of P-module generators of $S[V]^G$ is called a set of **secondary invariants**.

(6.8) Example. The set $\{X_1, X_2, \ldots, X_n\} \subseteq F[X]$ is a homogeneous system of parameters, we have $P = F[X]$ and the P-module $F[X]$ is generated by $\{1\} \subseteq F[X]$. In particular, if $S[V]^G$ is a polynomial ring, then a set of basic invariants, see Definition (5.6), is a set of primary invariants, and a set of secondary invariants is given by $\{1\} \subseteq S[V]^G$.

The set $\{X_1^2, X_2, \ldots, X_n\} \subseteq F[X]$ is algebraically independent as well, and we have $F[X] = 1 \cdot P \bigoplus X_1 \cdot P$, where $P = F[X_1^2, X_2, \ldots, X_n]$. Hence the set $\{X_1^2, X_2, \ldots, X_n\} \subseteq F[X]$ also is a homogeneous system of parameters. Hence not even the degrees of the elements of a homogeneous system of parameters are in general uniquely defined.

Having Noether normalization at hand, we are led to ask whether the finitely generated module for the polynomial subring has particular properties, and in particular whether it could be a free module. For invariant rings, in the non-modular case this indeed turns out to be true, see Theorem (6.15). We begin by looking at regular sequences, which if of appropriate length turn out to be particularly nice homogeneous systems of parameters.

(6.9) Definition. Let R be a finitely generated graded F-algebra, and let M be a finitely generated graded R-module.
a) A homogeneous element $0 \neq f \in R$ such that $\deg(f) > 0$ is called **regular** for M, if $\ker_M(\cdot f) = \{0\}$, where $\cdot f \colon M \to M \colon m \mapsto mf$. A sequence $\{f_1, \ldots, f_r\} \subseteq R$ of homogeneous elements such that $\deg(f_i) > 0$ is called **regular**, if f_i is regular for $R/(\sum_{j=1}^{i-1} f_j R)$, for $i \in \{1, \ldots, r\}$.
b) The **depth** $\operatorname{depth}(R) \in \mathbb{N}_0$ of R is the maximal length of a regular sequence in R. The F-algebra R is called **Cohen-Macaulay**, if $\operatorname{depth}(R) = \dim(R)$.

(6.10) Example. Let $F[X] = F[X_1, \ldots, X_r]$. Since $F[X]/(\sum_{j=1}^{i-1} X_j F[X]) \cong F[X_i, \ldots, X_r]$, for $i \in \{1, \ldots, r\}$, is an integral domain, we conclude that the sequence $\{X_1, \ldots, X_r\} \subseteq F[X]$ is regular. As $\dim(F[X]) = r$, see Example (6.3), the polynomial ring $F[X]$ is Cohen-Macaulay.

An example of a finitely generated graded F-algebra not being Cohen-Macaulay is given in Exercise (8.23).

(6.11) Proposition. We keep the notation of Definition (6.9)
a) Let $f \in R$ be regular for M. Then we have $\dim(M/Mf) = \dim(M) - 1$, see Definition (6.2). In particular, we have $\operatorname{depth}(R) \leq \dim(R)$.

b) Each regular sequence $\{f_1, \ldots, f_r\} \subseteq R$, for $r \leq \dim(R)$, can be extended to a homogeneous system of parameters. In particular, if $r = \dim(R)$, then $\{f_1, \ldots, f_r\}$ is a homogeneous system of parameters.

c) (Macaulay Theorem) Let R be Cohen-Macaulay and $r \in \mathbb{N}$. Then a sequence $\{f_1, \ldots, f_r\} \subseteq R$ of homogeneous elements such that $\deg(f_i) > 0$ is regular, if and only if $\dim(R/(\sum_{i=1}^{r} f_i R)) = \dim(R) - r$.

Proof. a) We consider the exact sequence of R-modules $\{0\} \to \ker_M(\cdot f) \to M \xrightarrow{\cdot f} M \to \operatorname{cok}_M(\cdot f) = M/Mf \to \{0\}$, see also the Proof of Theorem (6.1). As we have $\ker_M(\cdot f) = \{0\}$, we from this obtain $-T^{\deg(f)} H_M + H_M - H_{M/Mf} = 0 \in \mathbb{C}(T)$, hence $H_M = \frac{H_{M/Mf}}{1 - T^{\deg(f)}} \in \mathbb{C}(T)$, and thus $\dim(M) = \dim(M/Mf) + 1$.

Let $\{f_1, \ldots, f_r\} \subseteq R$ be a regular sequence. Hence this yields $\dim(R) - r = \dim(R/(\sum_{j=1}^{r} f_j R)) \geq 0$, see Definition (6.7). Thus $\operatorname{depth}(R) \leq \dim(R)$.

b) Let $\overline{R} := R/(\sum_{j=1}^{r} f_j R)$ and let $\overline{\ }: R \to \overline{R}$ denote the natural epimorphism of graded F-algebras. Moreover, by Noether normalization, see Theorem (6.6), let $\{g_1, \ldots, g_s\} \subseteq R$ and $\{h_1, \ldots, h_t\} \subseteq R$ where g_i and h_j are homogeneous such that $\deg(g_i) > 0$, such that $\{\overline{g_1}, \ldots, \overline{g_s}\} \subseteq \overline{R}$ is a homogeneous system of parameters of $\overline{R}$, and $\overline{R}$ is as an $F[\overline{g_1}, \ldots, \overline{g_s}]$-module generated by $\{\overline{h_1}, \ldots, \overline{h_t}\} \subseteq \overline{R}$. Note that we have $s = \dim(Q) = \dim(R) - r$.

Let $P \subseteq R$ be the F-algebra generated by $\{f_1, \ldots, f_r, g_1, \ldots, g_s\} \subseteq R$. Hence we have $\overline{P} = F[\overline{g_1}, \ldots, \overline{g_s}] \subseteq \overline{R}$. As the $\overline{P}$-module $\overline{R}$ is generated by $\{\overline{h_1}, \ldots, \overline{h_t}\}$, by the graded Nakayama Lemma, see Exercise (8.21), we conclude that $\{\overline{h_1}, \ldots, \overline{h_t}\}$ generates the F-vector space $\overline{R}/(\sum_{j=1}^{s} \overline{g_j}\overline{R}) \cong R/(\sum_{i=1}^{r} f_i R + \sum_{j=1}^{s} g_j R)$. By the graded Nakayama Lemma again we conclude that $\{h_1, \ldots, h_t\}$ is a generating set of the P-module R. Hence $P \subseteq R$ is a finite extension of graded F-algebras. Thus by Theorem (6.4) we have $\dim(P) = \dim(R) = r + s$, and since P is as an F-algebra generated by $r + s$ elements, by Exercise (8.20) we conclude that $P = F[f_1, \ldots, f_r, g_1, \ldots, g_s]$ is a polynomial ring. Hence $\{f_1, \ldots, f_r, g_1, \ldots, g_s\} \subseteq R$ is a homogeneous system of parameters.

c) By a) regular sequences fulfill the dimension condition. For the converse, see [1, Prop.4.3.4] and also [5, Cor.18.11]. ♯

(6.12) Theorem. Let R be a finitely generated graded F-algebra such that $r = \dim(R) \in \mathbb{N}_0$. Then the following conditions are equivalent:
i) The F-algebra R is Cohen-Macaulay.
ii) Each homogeneous system of parameters $\{f_1, \ldots, f_r\} \subseteq R$ is regular.
iii) For each homogeneous system of parameters $\{f_1, \ldots, f_r\} \subseteq R$, the F-algebra R is a finitely generated free graded P-module, where $P := F[f_1, \ldots, f_r]$.
iv) There is a homogeneous system of parameters $\{f_1, \ldots, f_r\} \subseteq R$, such that R is a finitely generated free graded P-module, where $P := F[f_1, \ldots, f_r]$.

Proof. ii) $\Longrightarrow$ i): By Definition (6.9) we have $\operatorname{depth}(R) = \dim(R)$.

i) $\Longrightarrow$ iii): By the graded Nakayama Lemma, see Exercise (8.21), we have $\dim_F(R/(\sum_{i=1}^{r} f_i R)) < \infty$, and letting $\{g_1, \ldots, g_s\} \subseteq R$ be homogeneous such that $\{g_1, \ldots, g_s\} \subseteq R/(\sum_{i=1}^{r} f_i R)$ is an F-basis of $R/(\sum_{i=1}^{r} f_i R)$, we have $R = \sum_{j=1}^{s} g_j P$. As $\dim(R/(\sum_{i=1}^{r} f_i R)) = 0$, see Definition (6.7), by the Macaulay Theorem, see Proposition (6.11), the sequence $\{f_1, \ldots, f_r\}$ is regular.

Let $h_j \in F[Y] = F[Y_1, \ldots, Y_r]$ such that $\sum_{j=1}^{s} g_j h_j(f_1, \ldots, f_r) = 0 \in R$, where there is j such that $h_j \neq 0$. Let $Y_1^{\alpha_1}$ be the maximal power of Y_1 dividing all h_j, and let $h_j^{(1)} := \frac{h_j}{Y_1^{\alpha_1}} \in F[Y]$. As $f_1 \in R$ is regular, we have $\sum_{j=1}^{s} g_j h_j^{(1)}(f_1, \ldots, f_r) = 0 \in R$. Hence we have $\sum_{j=1}^{s} g_j h_j^{(1)}(0, f_2, \ldots, f_r) = 0 \in R/f_1 R$ also, where by construction there is j such that $h_j^{(1)}(0, Y_2, \ldots, Y_r) \neq$

0. By iteration this yields $\sum_{j=1}^{s} g_j h_j^{(r)} = 0 \in R/(\sum_{i=1}^{r} f_i R)$, where $h_j^{(r)} \in F$, and there is j such that $h_j^{(r)} \neq 0$, a contradiction.

iii) $\Longrightarrow$ ii) and **iv) $\Longrightarrow$ i)**: Let $\{g_1, \ldots, g_s\} \subseteq R$ homogeneous such that we have $R = \bigoplus_{j=1}^{s} g_j F[f_1, \ldots, f_r]$ as $F[f_1, \ldots, f_r]$-modules. As $F[f_1, \ldots, f_r]$ is an integral domain, the element $f_1 \in R$ is regular, and $R/f_1R = \bigoplus_{j=1}^{s} g_j F[f_2, \ldots, f_r]$. By iteration, $\{f_1, \ldots, f_r\} \subseteq R$ is regular.

iii) $\Longrightarrow$ iv): Trivial. ♯

(6.13) Definition and Remark. Let R be Cohen-Macaulay.
a) Let $\{f_1, \ldots, f_r\} \subseteq R$ be a homogeneous system of parameters, where $r = \dim(R)$, let $P := F[f_1, \ldots, _r]$ and let $\{g_1, \ldots, g_s\} \subseteq R$ homogeneous such that $R = \bigoplus_{j=1}^{s} g_j P$. This decomposition of the P-module R as a direct sum of free P-modules is called the corresponding **Hironaka decomposition** of R.
b) Given a Hironaka decomposition of R, its Hilbert series is given as

$$H_R = \frac{\sum_{j=1}^{s} T^{\deg(g_j)}}{\prod_{i=1}^{r}(1 - T^{\deg(f_i)})} \in \mathbb{C}(T).$$

In particular, as $\dim(R) = r$ we have $\deg(R) = \frac{s}{\prod_{i=1}^{r} \deg(f_i)}$, see Definition (6.2).
c) Hence, if a homogeneous system of parameters $\{f_1, \ldots, f_r\}$ has been found, the Hilbert series can be used to find the degrees of the elements of a minimal homogeneous generating set $\{g_1, \ldots, g_s\} \subseteq R$ of the P-module R.

(6.14) Theorem. Let G be a finite group acting faithfully on the F-vector space V, where $\dim_F(V) = n$, see Corollary (6.5). Let $\{f_1, \ldots, f_n\} \subseteq S[V]^G$ be a set of primary invariants, let $d_i := \deg(f_i)$, let $P := F[f_1, \ldots, f_n]$ and let $\{g_1, \ldots, g_s\} \subseteq S[V]^G$ be a minimal set of secondary invariants of $S[V]^G$.
a) Then $|G| \mid \prod_{i=1}^{n} d_i$, and we have $s \cdot |G| \geq \prod_{i=1}^{n} d_i$.
b) The invariant ring $S[V]^G$ is Cohen-Macaulay, if and only if $s \cdot |G| = \prod_{i=1}^{n} d_i$.

Proof. a) As both the ring extensions $P \subseteq S[V]^G \subseteq S[V]$ are finite, see Theorem (2.9), the set $\{f_1, \ldots, f_n\}$ is a homogeneous system of parameters of $S[V]$. Let $\{h_1, \ldots, h_t\} \subseteq S[V]$ be a minimal homogeneous P-module generating set of $S[V]$. As by Example (6.10) the polynomial ring $S[V]$ is Cohen-Macaulay, Definition (6.13) yields $\deg(S[V]) = \frac{t}{\prod_{i=1}^{n} d_i}$. As by Example (6.3) we have $\deg(S[V]) = 1$, we conclude $t = \prod_{i=1}^{n} d_i$.

Moreover, by Theorem (6.12) the P-module $S[V]$ is free of rank t, thus the set $\{h_1, \ldots, h_t\}$ is a $\mathrm{Quot}(P)$-linearly independent generating set of $S(V)$, hence we have $[S(V)\colon \mathrm{Quot}(P)] = t = \prod_{i=1}^{n} d_i$. As by Proposition (2.5) we have $[S(V)\colon S(V)^G] = |G|$, we conclude $[S(V)^G\colon \mathrm{Quot}(P)] = \frac{\prod_{i=1}^{n} d_i}{|G|}$. As $\{g_1, \ldots, g_s\}$ generates $S(V)^G$ as a $\mathrm{Quot}(P)$-vector space, we have $s \geq \frac{\prod_{i=1}^{n} d_i}{|G|}$.

b) If we have $s = \frac{\prod_{i=1}^{n} d_i}{|G|}$, then $\{g_1, \ldots, g_s\}$ is $\mathrm{Quot}(P)$-linearly independent, hence in particular $S[V]^G$ is a free P-module of rank s, thus by Theorem (6.12) is Cohen-Macaulay. Conversely, if $S[V]^G$ is Cohen-Macaulay, then by Definition (6.13) and Corollary (6.5) we have $\deg(S[V]^G) = \frac{s}{\prod_{i=1}^{n} d_i} = \frac{1}{|G|}$. ♯

We are prepared to prove the main structure theorem for invariant rings in the non-modular case.

(6.15) Theorem: Hochster-Eagon, 1971.
Let F be a field, let G be a finite group and let $H \leq G$ such that $\mathrm{char}(F) \nmid [G\colon H]$. If the invariant ring $S[V]^H$ is Cohen-Macaulay, then the invariant ring $S[V]^G$ is Cohen-Macaulay as well. In particular, if $\mathrm{char}(F) \nmid |G|$, then $S[V]^G$ is Cohen-Macaulay.

Proof. Let $\{f_1, \ldots, f_n\} \subseteq S[V]^G$ be a set of primary invariants, i. e. a homogeneous system of parameters, where $n = \dim_F(V)$, see Corollary (6.5). Let $P := F[f_1, \ldots, f_n] \subseteq S[V]^G \subseteq S[V]^H \subseteq S[V]$, hence $S[V]^G$ is a finitely generated P-module. As by Theorem (2.9) the ring extension $S[V]^G \subseteq S[V]$ is finite, the ring $S[V]$ is a finitely generated P-module as well. As P is Noetherian, the P-submodule $S[V]^H \subseteq S[V]$ also is a finitely generated P-module, hence $\{f_1, \ldots, f_n\}$ is a homogeneous system of parameters of $S[V]^H$, i. e. a set of primary invariants. Thus by Theorem (6.12) the P-module $S[V]^H$ is free.

The relative Reynolds operator $\mathcal{R}_H^G\colon S[V]^H \to S[V]^G$, see Definition (3.3), in particular is a projection of graded P-modules. Hence $S[V]^G$ is a direct summand of the free P-module $S[V]^H$, and thus is a finitely generated projective graded P-module, and hence by Exercise (8.21) is a free P-module. Thus $S[V]^G$ is Cohen-Macaulay.

As by Example (6.10) the polynomial ring $S[V]$ is Cohen-Macaulay, the second statement follows from the first. ♯

(6.16) Example. a) Let F be a field such that $\mathrm{char}(F) \neq 2$, and let $F[X]^{\mathcal{A}_X}$ be the invariant ring of the alternating group $\mathcal{A}_X \leq \mathcal{S}_X$, see Exercise (8.2). Hence we have $F[X]^{\mathcal{A}_X} = 1 \cdot F[X]^{\mathcal{S}_X} \bigoplus \Delta_n \cdot F[X]^{\mathcal{S}_X}$, where $F[X]^{\mathcal{S}_X} \cong F[e_1, \ldots, e_n]$ is a polynomial ring, and $\Delta_n^2 \in F[X]^{\mathcal{S}_X}$, see Exercise (8.1). Hence the set of elementary symmetric polynomials $\{e_1, \ldots, e_n\} \subseteq F[X]^{\mathcal{A}_X}$ is a set of primary invariants, and $\{1, \Delta_n\} \subseteq F[X]^{\mathcal{A}_X}$ is a set of secondary invariants, see Definition (6.7), and the above decomposition of $F[X]^{\mathcal{A}_X}$ is the corresponding Hironaka decomposition, see Definition (6.13).

b) Further examples are given in Exercise (8.24), Exercise (8.25) and Exercise (8.26). Moreover, in Section 7 we present an elaborated classical example, the invariants of the icosahedral group.

(6.17) Remark. In the modular case, invariant rings in general are not Cohen-Macaulay, see Exercise (8.27). Actually, the analysis of the structure of invariant

rings in the modular case currently is in the focus of intensive study, but the general picture seems to be only slowly emerging.

7 Invariant theory live: the icosahedral group

In Section 7 we present an elaborated classical example, the invariants of the icosahedral group, due to Molien (1897). This shows invariant theory at work, and in particular how geometric features are related to invariant theory. As a reference see [12, Ex.3.1.4]. The computations carried out below can easily be reproduced using either of the computer algebra systems GAP [6] or MAGMA [3]. We include some relevant GAP code at the end of Section 7.

Let $\mathcal{I} \subseteq \mathbb{R}^{1\times 3}$ be the regular icosahedron, one of the platonic solids. The faces of $\mathcal{I}$ consist of regular triangles, where at each vertex 5 triangles meet. Let $f, e, v \in \mathbb{N}$ be the number of faces, edges, and vertices of $\mathcal{I}$, respectively. Hence by Euler's Polyhedron Theorem we have $f - e + v = 2$. Since we have $e = \frac{3f}{2}$ and $v = \frac{3f}{5}$, we conclude $f = 20$ and $e = 30$ as well as $v = 12$.

Let $G := \{\pi \in O_3(\mathbb{R}); \mathcal{I}\pi = \mathcal{I}\} \leq O_3(\mathbb{R})$ be the symmetry group of $\mathcal{I}$, where we assume $\mathcal{I} \subseteq \mathbb{R}^{1\times 3}$ to be centered at the origin, and $O_3(\mathbb{R})$ is the isometry group of the Euclidean space $\mathbb{R}^{1\times 3}$. Let $H = G \cap SO_3(\mathbb{R})$ be the group of rotational symmetries of $\mathcal{I}$, where $SO_3(\mathbb{R}) := \{\pi \in O_3(\mathbb{R}); \det(\pi) = 1\} \leq O_3(\mathbb{R})$.

By the regularity of $\mathcal{I}$, the group H acts transitively on the vertices of $\mathcal{I}$, where the corresponding point stabilizers have order 5. Hence we have $|H| = 60$. The rotational axes of the elements of H are given by the lines joining opposite vertices, midpoints of opposite edges, and midpoints of opposite faces $\mathcal{I}$. This yields $6 \cdot 4$ elements of order 5, and 15 elements of order 2, as well as $10 \cdot 2$ elements of order 3, respectively, accounting for all the non-trivial elements of H. Using basic group theory it straightforwardly follows that $H \cong \mathcal{A}_5$

Moreover, as for the inversion σ with respect to the origin we have $\sigma \in G \setminus H$. As $\sigma \in Z(O_3(\mathbb{R}))$, we have $G = H \times \langle\sigma\rangle \cong \mathcal{A}_5 \times C_2$, in particular $|G| = 120$. Note that the eigenvalues of σ are $\{-1, -1, -1\}$, hence σ is not a reflection. The group H is generated by its elements of order 2. These are rotations, thus have eigenvalues $\{1, 1, -1\}$, and hence are not reflections either. From that we conclude that G is generated by the set of reflections $\{\pi\sigma \in G; 1 \neq \pi \in H; \pi^2 = 1\}$. Thus G is a reflection group; actually it is the exceptional irreducible pseudoreflection group G_{23} in the Shephard-Todd classification, see Remark (5.10).

The ordinary character table of $H \cong \mathcal{A}_5$, where $\zeta_5 := \exp\frac{2\pi i}{5} \in \mathbb{C}^*$ is a primitive 5-th root of unity, as well as $\zeta := \zeta_5 + \zeta_5^4 \in \mathbb{R} \subseteq \mathbb{C}$ and $\zeta' := \zeta_5^2 + \zeta_5^3 = -1 - \zeta \in \mathbb{R}$, is given as follows, where the conjugacy classes are denoted by the corresponding element orders, and the second power map, see Remark (4.3), as well as the

cardinality of the conjugacy classes are also given.

order	1	2	3	5	$5'$
power_2	1	2	3	$5'$	5
#	1	15	20	12	12
χ_1	1	1	1	1	1
χ_2	3	-1	.	ζ	ζ'
χ_3	3	-1	.	ζ'	ζ
χ_4	4	.	1	-1	-1
χ_5	5	1	-1	.	.

Hence $\mathbb{R}^{1\times 3}$ is an absolutely irreducible $\mathbb{R}\mathcal{A}_5$-module, affording the character $\chi_2 \in \mathbb{Z}\text{Irr}_{\mathbb{C}}(\mathcal{A}_5)$, say, and by Molien's Formula, see Theorem (4.2) and Remark (4.3), we find $H_{S[\mathbb{R}^3]^H} = \frac{1-T^2-T^3+T^6+T^7-T^9}{(1-T^2)^2\cdot(1-T^3)\cdot(1-T^5)} \in \mathbb{C}(T)$. By the Hochster-Eagon Theorem, see Theorem (6.15), the invariant ring $H_{S[\mathbb{R}^3]^H}$ is Cohen-Macaulay, and by the Shephard-Todd-Chevalley Theorem, see Theorem (5.9), it is not polynomial. Hence taking Definition (6.13) and Theorem (6.14) into account we finally end up with the following form of the Hilbert series

$$H_{S[\mathbb{R}^3]^H} = \frac{1+T^{15}}{(1-T^2)\cdot(1-T^6)\cdot(1-T^{10})} \in \mathbb{C}(T).$$

Hence we conjecture that there are primary invariants $\{f_1,\ldots,f_3\}$ such that $\deg(f_1)=2$, $\deg(f_2)=6$ and $\deg(f_3)=10$, and secondary invariants $\{g_1,g_2\}$ such that $g_1=1$ and $\deg(g_2)=15$, such that the corresponding Hironaka decomposition of the invariant ring is $S[\mathbb{R}^3]^H = \bigoplus_{j=1}^2 g_j\mathbb{R}[f_1,\ldots,f_3]$. For the polynomial invariant ring $S[\mathbb{R}^3]^G$ we obtain $H_{S[\mathbb{R}^3]^G} = \frac{1}{(1-T^2)\cdot(1-T^6)\cdot(1-T^{10})} \in \mathbb{C}(T)$, leading to the conjecture that the polynomial degrees, see Definition (5.6), of the pseudoreflection group G are $\{2,6,10\}$, and that we moreover have $S[\mathbb{R}^3]^G = \mathbb{R}[f_1,\ldots,f_3]$.

Let $H := \langle \alpha,\beta,\gamma\rangle$, where $\alpha^2=1$, $\beta^3=1$, $\gamma^5=1$ and $\alpha\beta=\gamma$. Moreover, let $F := \mathbb{Q}(\zeta) \subseteq \mathbb{R}$ be the real number field generated by $\zeta \in \mathbb{R}$, let $V := F^{1\times 3}$ and let $D_V\colon H \to GL_3(F) \leq GL_3(\mathbb{R})$ be given as

$$D_V\colon \alpha \mapsto \begin{bmatrix} . & 1 & . \\ 1 & . & . \\ . & . & -1 \end{bmatrix}, \beta \mapsto \begin{bmatrix} . & . & 1 \\ \zeta & 1 & -1 \\ -1 & . & -1 \end{bmatrix}, \gamma \mapsto \begin{bmatrix} \zeta & 1 & -1 \\ . & . & 1 \\ 1 & . & 1 \end{bmatrix}.$$

Hence we indeed have $\chi_V = \chi_2 \in \mathbb{Z}\text{Irr}_{\mathbb{C}}(\mathcal{A}_5)$. Moreover, as H acts by isometries of the Euclidean space $\mathbb{R}^{1\times 3}$, there is an H-invariant scalar product on V. As H acts absolutely irreducibly on V, it is uniquely defined up to scalars, and its matrix turns out to be given as

$$\Phi := \begin{bmatrix} 1 & \frac{\zeta'}{2} & -\frac{1}{2} \\ \frac{\zeta'}{2} & 1 & \frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} & 1 \end{bmatrix} \in \mathbb{Q}(\zeta)^{3\times 3}.$$

We use the identification $S[V] \cong F[X_1, \ldots, X_3]$, see Proposition (2.2), and let $\mathcal{X} := [X_1, \ldots, X_3] \in F[X]^{1\times 3}$ and $D := D_V(\pi)$, for $\pi \in H$. Note that for $L \in F^{3\times 1}$ we have $(\mathcal{X} \cdot L)^D = \mathcal{X} \cdot D^{\mathrm{tr}} L$, where by $\cdot^D$ we denote the action of D on $F[X]$. As the bilinear form described by Φ is H-invariant, we have $D\Phi D^{\mathrm{tr}} = \Phi$, hence $D^{-\mathrm{tr}}\Phi^{-1}D^{-1} = \Phi^{-1}$, and thus $D^{\mathrm{tr}}\Phi^{-1}D = \Phi^{-1}$ as well. From this we obtain $(\mathcal{X}\Phi^{-1}\mathcal{X}^{\mathrm{tr}})^D = (\mathcal{X}\Phi^{-1})^D \cdot (\mathcal{X}^D)^{\mathrm{tr}} = (\mathcal{X}D^{\mathrm{tr}}\Phi^{-1}) \cdot (\mathcal{X}D^{\mathrm{tr}})^{\mathrm{tr}} = \mathcal{X}D^{\mathrm{tr}}\Phi^{-1}D\mathcal{X}^{\mathrm{tr}} = \mathcal{X}\Phi^{-1}\mathcal{X}^{\mathrm{tr}}$ Thus $f_1 := \mathcal{X}\Phi^{-1}\mathcal{X}^{\mathrm{tr}} \in S[V]^H$ is homogeneous such that $\deg(f_1) = 2$.

The group H permutes the 6 lines joining opposite vertices of $\mathcal{I}$ transitively. A vector $0 \neq v_1 \in V$ on one of these lines is found as an eigenvector of $\gamma \in H$ with respect to the eigenvalue 1. Note that γ has order 5, and as γ is a rotation the corresponding eigenspace has F-dimension 1. It turns out that the H-orbit $\{\pm v_1, \ldots, \pm v_6\} \subseteq V$ of v_1 has length 12. We choose $\{v_1, \ldots, v_6\} \subseteq V$, one from each of 2-element sets $\{\pm v_i\}$, and let $f_2 := \prod_{k=1}^{6} v_k \in S[V]$ homogeneous such that $\deg(f_2) = 6$. As H permutes $\{\pm v_1, \ldots, \pm v_6\}$, we conclude that $\langle f_2 \rangle_F \in S[V]_6$ is a 1-dimensional FH-submodule. As $H \cong \mathcal{A}_5$ is a perfect group, we conclude that $f_2 \in S[V]^H$.

Analogously, the group H permutes the 10 lines joining the midpoints of opposite faces of $\mathcal{I}$ transitively. We consider the eigenspace of $\beta \in H$ with respect to the eigenvalue 1, which again has F-dimension 1, and where β has order 3. This leads to an H-orbit of length 20, and as above we get $f_3 \in S[V]^H$ homogeneous such that $\deg(f_3) = 10$.

By the Jacobian Criterion, see Proposition (5.8), we find that $\det J(f_1, \ldots, f_3) \neq 0 \in S[V]$, hence $\{f_1, \ldots, f_3\}$ is algebraically independent. Note that this does not a priorly qualify $\{f_1, \ldots, f_3\}$ to be a set of primary invariants of $S[V]^H$. As $\sigma \in G \setminus H$ has eigenvalues $\{-1, -1, -1\}$ and $\deg(f_i)$ is even, we have $\{f_1, \ldots, f_3\} \subseteq S[V]^G$. Since we have $H_{S[V]^G} = \frac{1}{(1-T^2)\cdot(1-T^6)\cdot(1-T^{10})} \in \mathbb{C}(T)$ this shows $S[V]^G = F[f_1, \ldots, f_3]$, and hence $\{f_1, \ldots, f_3\} \subseteq S[V]^G$ is a set of basic invariants of $S[V]^G$. As in the Proof of Theorem (6.15) we conclude that $\{f_1, \ldots, f_3\} \subseteq S[V]^H$ is a set of primary invariants of $S[V]^H$.

As $H_{S[V]^H} = (1 + T^{15}) \cdot H_{S[V]^G}$, we by Definition (6.13) are left to find a secondary invariant of $S[V]^H$ of degree 15. As $H \cong \mathcal{A}_5$ is a perfect group, we conclude that $\det_V$ is the trivial H-representation, hence by Exercise (8.13) we have $0 \neq g_2 := \det J(f_1, \ldots, f_3) \in S[V]^H$ homogeneous such that $\deg(g_2) = 15$. As $\deg(f_i)$ is even and $\deg(g_2)$ is odd, we conclude that $\{g_1, g_2\}$ is $F[f_1, \ldots, f_3]$-linearly independent, and hence we have $S[V]^H = \bigoplus_{j=1}^{2} g_j F[f_1, \ldots, f_3]$.

Note that $\det_V(\sigma) = -1$, hence $\det_V$ is not the trivial G-representation, and thus the assumption of Exercise (8.13) is not fulfilled. Indeed, we have already proved that $\det J(f_1, \ldots, f_3) \in S[V]^H \setminus S[V]^G$. Moreover, note that analogously to $f_2, f_3 \in S[V]^H$ we can find a homogeneous H-invariant of degree 15 by using suitable vectors lying on the lines joining the midpoints of opposite edges of $\mathcal{I}$. As $\dim_F(S[V]^H) = 1$, the latter invariant is a scalar multiple of $g_2 \in S[V]^H$. ♯

The GAP code used is as follows. We also provide slides of a corresponding GAP session at the very end of these lecture notes.

```
########################################################################

tbl:=CharacterTable("A5");
hs:=MolienSeries(tbl,Irr(tbl)[2]);
# ( 1-z^2-z^3+z^6+z^7-z^9 ) / ( (1-z^5)*(1-z^3)*(1-z^2)^2 )
MolienSeriesWithGivenDenominator(hs,[2,6,10]);
# ( 1+z^15 ) / ( (1-z^10)*(1-z^6)*(1-z^2) )

z:=E(5)+E(5)^4;
rep:= # representation of A5 over Z[z], on (2,3,5)-triple
[ [ [ 0, 1, 0 ], [ 1, 0, 0 ], [ 0, 0,-1 ] ],
  [ [ 0, 0, 1 ], [ z, 1,-1 ], [-1, 0,-1 ] ],
  [ [ z, 1,-1 ], [ 0, 0, 1 ], [ 1, 0, 1 ] ] ];
h:=Group(rep);

polring:=PolynomialRing(Cyclotomics,["X_1","X_2","X_3"]);
indets:=IndeterminatesOfPolynomialRing(polring);
x1:=indets[1];
x2:=indets[2];
x3:=indets[3];
x:=[x1,x2,x3];

f:= # the A5-invariant scalar product
[ [ 1,          1/2*(-1-z), -1/2 ],
  [ 1/2*(-1-z),          1,  1/2 ],
  [       -1/2,        1/2,    1 ] ];
f1:=x*f^(-1)*x; # invariant of degree 2

v:=NullspaceMat(rep[3]-rep[3]^0)[1];
vorb:=Orbit(h,v);
PermList(List(vorb,x->Position(vorb,-x)));
# (1,12)(2,11)(3,10)(4,9)(5,6)(7,8)
vvecs:=vorb{[1,2,3,4,5,7]};
# [ [ -E(5)-2*E(5)^2-2*E(5)^3-E(5)^4,
#     -E(5)-2*E(5)^2-2*E(5)^3-E(5)^4, 1 ],
#   [ -E(5)-2*E(5)^2-2*E(5)^3-E(5)^4,
#     -E(5)-2*E(5)^2-2*E(5)^3-E(5)^4, -1 ],
#   [ E(5)+E(5)^4, -E(5)-2*E(5)^2-2*E(5)^3-E(5)^4, -1 ],
#   [ -E(5)-2*E(5)^2-2*E(5)^3-E(5)^4, E(5)+E(5)^4, 1 ],
#   [ -E(5)-E(5)^4, E(5)+E(5)^4, 1 ],
#   [ -E(5)-E(5)^4, E(5)+E(5)^4, -E(5)+E(5)^2+E(5)^3-E(5)^4 ] ]
f2:=Product(List(vvecs,i->x*i)); # invariant of degree 6
```

```
w:=NullspaceMat(rep[2]-rep[2]^0)[1];
worb:=Orbit(h,w);
PermList(List(worb,x->Position(worb,-x)));
# (1,20)(2,19)(3,17)(4,14)(5,18)(6,15)(7,16)(8,11)(9,12)(10,13)
wvecs:=worb{[1,2,3,4,5,6,7,8,9,10]};
f3:=Product(List(wvecs,i->x*i)); # invariant of degree 10

prim:=[f1,f2,f3];
jac:=List(prim,p->List(x,i->Derivative(p,i)));
g2:=DeterminantMat(jac); # invariant of degree 15

#########################################################################
```

8 Exercises

(8.1) Exercise: Elementary symmetric polynomials.
Let F be a field and $F[X] := F[X_1, \ldots, X_n]$. Let $\Delta_n := \prod_{1 \le i < j \le n}(X_i - X_j) \in F[X]$ be the **discriminant** and let $p_{n,k} := \sum_{i=1}^{n} X_i^k \in F[X]$, for $k \in \mathbb{N}$, be the k-th **power sum**.

Show that Δ_n^2 and $p_{n,k}$ are symmetric polynomials, and write Δ_3, as well as $p_{n,2}$, $p_{n,3}$ and $p_{n,4}$ as polynomials in the elementary symmetric polynomials $\{e_1, \ldots, e_n\} \subseteq F[X]$.

(8.2) Exercise: Alternating polynomials.
Let F be a field such that $\mathrm{char}(F) \neq 2$, and let $F[X] := F[X_1, \ldots, X_n]$. A polynomial $f \in S$ is called **alternating**, if $f\pi = \mathrm{sgn}(\pi) \cdot f$ for all $\pi \in \mathcal{S}_X$.
a) Show that $f \in F[X]$ is alternating, if and only if $f = \Delta_n \cdot g$, where $g \in F[X]$ is a symmetric polynomial and $\Delta_n \in F[X]$ is the discriminant as in Exercise (8.1).
b) Let $F[X]^{\mathcal{A}_X} := \{f \in F[X]; f\pi = f \text{ for all } \pi \in \mathcal{A}_X\} \subseteq F[X]$ be the invariant ring of the alternating group $\mathcal{A}_X \le \mathcal{S}_X$. Show that we have $F[X]^{\mathcal{A}_X} = F[X]^{\mathcal{S}_X} \bigoplus \Delta_n \cdot F[X]^{\mathcal{S}_X}$ as F-vector spaces, i. e. each $f \in F[X]^{\mathcal{A}_X}$ can be uniquely written as $f = g + \Delta_n \cdot h$, where $g, h \in F[X]^{\mathcal{S}_X}$.
c) Conclude that $F[X]^{\mathcal{A}_X}$ is not a polynomial ring.

(8.3) Exercise: An algebraic equation system.
Let $n \in \mathbb{N}$ and let F be a field such that $\mathrm{char}(F) > n$. Determine all solutions $[x_1, \ldots, x_n] \in F^{1 \times n}$ of the system of $n-1$ equations

$$\sum_{i=1}^{n} x_i = 0, \quad \sum_{i=1}^{n} x_i^2 = 0, \quad \ldots \quad , \sum_{i=1}^{n} x_i^{n-1} = 0.$$

Proof. Uses the Newton identities, see Exercise (8.4). ♯

(8.4) Exercise: Newton identities.
Let F be a field and $F[X] := F[X_1, \ldots, X_n]$. Moreover, let $p_{n,k} := \sum_{i=1}^{n} X_i^k \in F[X]$, for $k \in \mathbb{N}$, be the power sums as in Exercise (8.1), let $e_1, \ldots, e_n \in F[X]$ be the elementary symmetric polynomials, and let $e_0 := 1 \in F[X]$. For $k \in \{1, \ldots, n\}$ show that

$$k e_k = \sum_{i=1}^{k} (-1)^{i-1} p_{n,i} e_{k-i}.$$

Proof. See [12, p.81]. ♯

(8.5) Exercise: Integral ring extensions.
Let $R \subseteq S$ be an extension of commutative rings.
a) Show that an element $s \in S$ is integral over R, if and only if there is a finitely generated R-submodule of S containing s.
b) Show that the ring extension $R \subseteq S$ is finite, if and only if S is a finitely generated R-module.
c) Show that the subset $\overline{R}^S := \{s \in S; s \text{ integral over } R\} \subseteq S$ is a subring of S.
d) Let R be a unique factorization domain. Show that R is integrally closed.

(8.6) Exercise: Noetherian rings and modules.
Let R be a commutative ring and let M be an R-module.
a) Show that, if M is Noetherian, then so are the R-submodules and the quotient R-modules of M.
b) Show that, if R is Noetherian, then M is Noetherian if and only if M is a finitely generated R-module.

Proof. See [1, Ch.1.2] or [12, Ch.2.1]. ♯

(8.7) Exercise: Hilbert series.
Let $F[X] := F[X_1, \ldots, X_n]$ and $F[X]_d := \{f \in F[X]; \deg_X(f) = d\}$, for $d \in \mathbb{N}_0$.
a) Show that $\dim_F(F[X]_d) = \binom{n+d-1}{d}$ and conclude that the Hilbert series of the polynomial ring $F[X]$ is given as $H_{F[X]} = \frac{1}{(1-T)^n} \in \mathbb{C}((T))$.
b) Let $Y := \{Y_1, \ldots, Y_m\} \subseteq F[X]$, for $m \in \mathbb{N}_0$, be algebraically independent, where Y_i is homogeneous such that $\deg_X(Y_i) = d_i$. Show that the Hilbert series of the polynomial ring $F[Y]$ is given as $H_{F[Y]} = \prod_{i=1}^{m} \frac{1}{1-T^{d_i}} \in \mathbb{C}((T))$.

(8.8) Exercise: Transfer map.
a) Let F be a field, let G be a finite group and let V be a finite-dimensional FG-module. Moreover let $\mathrm{Tr}^G \colon S[V] \to S[V]^G$ be the transfer map. Show that $\mathrm{im}\,(\mathrm{Tr}^G) \neq \{0\}$ holds.
b) Let F be a field of $\mathrm{char}(F) = 2$, let $F[X] = F[X_1, \ldots, X_n]$, for $n \geq 2$, be the polynomial ring acted on by the symmetric group $\mathcal{S}_X$, and let $\Delta_n \in F[X]$ be as in Exercise (8.1). Show that $\mathrm{im}\,(\mathrm{Tr}^G) = \Delta_n \cdot F[X]^{\mathcal{S}_X} \lhd F[X]^{\mathcal{S}_X}$.

Proof. a) See [12, Prop.2.2.4]. **b)** See [12, Ex.2.2.1]. ♯

(8.9) Exercise: Generators of invariant rings.
Let $G = \langle \pi \rangle \cong C_3$ be the cyclic group of order 3, let F be a field such that $\mathrm{char}(F) \neq 3$, and let

$$D_V \colon G \to GL_2(F) \colon \pi \mapsto \begin{bmatrix} \cdot & 1 \\ -1 & -1 \end{bmatrix}.$$

Compute a minimal F-algebra generating set of $S[V]^G$, and show that Noether's degree bound is attained in this case.

Proof. See [12, Ex.2.3.1]. ♯

(8.10) Exercise: Noether's degree bound.
Let $G = \langle \pi \rangle \cong C_2$ be the cyclic group of order 2, let F be a field such that $\mathrm{char}(F) = 2$, let $V = W \oplus W \oplus W$ as FG-modules, where

$$D_W \colon G \to GL_2(F) \colon \pi \mapsto \begin{bmatrix} . & 1 \\ 1 & . \end{bmatrix}.$$

Show that Noether's degree bound does not hold for $S[V]^G$.

Proof. See [4, Ex.3.5.7] or [12, Ex.2.3.2]. ♯

(8.11) Exercise: Noether's degree bound.
Let $G = \langle \pi \rangle \cong C_2$ be the cyclic group of order 2, let F be a field such that $\mathrm{char}(F) = 2$, let $V = W \oplus W$ as FG-modules, where

$$D_W \colon G \to GL_2(F) \colon \pi \mapsto \begin{bmatrix} 1 & 1 \\ . & 1 \end{bmatrix}.$$

Compute a minimal F-algebra generating set of $S[V]^G$, determine the Hilbert ideal $\mathcal{I}_G[V]$, and show that Benson's Lemma does not hold for $S[V]_+ \lhd S[V]$.

Proof. See [4, Rem.3.8.7]. ♯

(8.12) Exercise: Molien's Formula.
For $k \in \mathbb{N}$ let $G = \langle \pi \rangle \cong C_k$ be the cyclic group of order k, let $\zeta_k := \exp \frac{2\pi i}{k} \in \mathbb{C}^*$ be a k-th primitive root of unity, and let

$$D_V \colon G \to GL_2(\mathbb{C}) \colon \pi \mapsto \begin{bmatrix} \zeta_k & . \\ . & \zeta_k^{-1} \end{bmatrix}.$$

a) Show that $S[V]^G \cong \bigoplus_{i=0}^{k-1} (X_1X_2)^i \cdot F[X_1^k, X_2^k]$. Conclude that the Hilbert series of $S[V]^G$ is given as $H_{S[V]^G} = \frac{1-T^{2k}}{(1-T^2)\cdot(1-T^k)^2} \in \mathbb{C}((T))$.
b) Prove the identity

$$\frac{1}{k} \cdot \sum_{i=0}^{k=1} \frac{1}{(1-\zeta_k^i T)\cdot(1-\zeta_k^{-i}T)} = \frac{1}{(1-T^k)^2} \cdot \sum_{i=0}^{k-1} T^{2i} \in \mathbb{C}((T)).$$

c) Evaluate the sum $\sum_{i=0}^{k-1} \frac{1}{|1-\zeta_k^i|^2} \in \mathbb{C}$.

Proof. See [12, Ex.3.1.1, Ex.3.1.2] and [4, Ex.5.6.1]. ♯

(8.13) Exercise: Jacobian and Hessian determinant.
Let G be a group, let V be an FG-module such that $\dim_F(V) = n \in \mathbb{N}$, and let $\det_V \colon G \to F \colon g \mapsto \det_V(g)$ denote the corresponding **determinant representation**. Moreover, let $S[V] \cong F[X] = F[X_1, \ldots, X_n]$ using the identification from Proposition (2.2).
a) For $\{f_1, \ldots, f_n\} \subseteq S[V]^G$ let $J(f_1, \ldots, f_n) := [\frac{\partial f_i}{\partial X_j}]_{i,j=1,\ldots,n} \in F[X]^{n \times n}$ be the corresponding **Jacobian matrix**. Show that if $\det_V$ is the trivial representation, then for the determinant $\det J(f_1, \ldots, f_n) \in F[X]$ we have $\det J(f_1, \ldots, f_n) \in S[V]^G$.
b) For $f \in S[V]^G$ let $H(f) := J([\frac{\partial f}{\partial X_i}]_{i=1,\ldots,n}) \in F[X]^{n \times n}$ denote the corresponding **Hessian matrix**. Show that if $(\det_V)^2$ is the trivial representation, then for the determinant $\det H(f) \in F[X]$ we have $\det H(f) \in S[V]^G$.

(8.14) Exercise: Jacobian Criterion.
Let F be a field such that $\mathrm{char}(F) = 0$, let $F[X] := F[X_1, \ldots, X_n]$ and let $p_{n,k} := \sum_{i=1}^n X_i^k \in F[X]$, for $k \in \mathbb{N}$, be the power sums as in Exercise (8.1). Show that $\{p_{n,1}, \ldots, p_{n,n}\} \subseteq F[X]$ is algebraically independent.

Proof. See [7, Exc.3.10]. ♯

(8.15) Exercise: Polynomial degrees.
Let R be a finitely generated graded F-algebra, and let $\{f_1, \ldots, f_n\} \subseteq R$ and $\{f'_1, \ldots, f'_n\} \subseteq R$ be algebraically independent sets of homogeneous elements such that $R = F[f_1, \ldots, f_n] = F[f'_1, \ldots, f'_n]$. Let moreover $d_i = \deg(f_i)$ and $d'_i = \deg(f'_i)$, where $d_1 \leq \cdots \leq d_n$ and $d'_1 \leq \cdots \leq d'_n$. Show that $d_i = d'_i$ holds, for $i \in \{1, \ldots, n\}$.

Proof. See [7, Prop.3.7]. ♯

(8.16) Exercise: Polynomial invariant rings.
Let F be a field, let G be a finite group, and let V be a faithful FG-module, where $n := \dim_F(V)$.
a) Let $S[V]^G = F[f_1, \ldots, f_r]$, for $r \in \mathbb{N}_0$, be a polynomial ring, where $f_i \in S[V]$ is homogeneous. Show that $r = n$ and $\prod_{i=1}^n \deg(f_i) = |G|$.
b) Let $\{f_1, \ldots, f_r\} \subseteq S[V]^G$ be a homogeneous system of parameters such that $\prod_{i=1}^r \deg(f_i) = |G|$. Show that $r = n$ and $S[V]^G = F[f_1, \ldots, f_n]$.
c) Let $F \subseteq \mathbb{C}$, let G be generated by pseudoreflections, and let $\{f_1, \ldots, f_n\} \subseteq S[V]^G$ be an algebraically independent set of homogeneous invariants, such that $\prod_{i=1}^n \deg(f_i) = |G|$. Show that $S[V]^G = F[f_1, \ldots, f_n]$.

Proof. See [7, Prop.3.12], [1, Ch.2.4], [12, Prop.4.5.5] and [4, Thm.3.7.5]. ♯

(8.17) Exercise: Reflection representations of $\mathcal{S}_n$.
Let $n \in \mathbb{N}$ and let W be the natural permutation $\mathbb{Q}\mathcal{S}_n$-module, having permutation $\mathbb{Q}$-basis $\{b_1, \ldots, b_n\} \subseteq W$.
a) Show that $W' := \langle \sum_{i=1}^n b_i \rangle_{\mathbb{Q}} \leq W$ is a $\mathbb{Q}\mathcal{S}_n$-submodule, and that $V := W/W'$ is an absolutely irreducible faithful reflection representation of $\mathcal{S}_n$.
b) Determine algebraically independent invariants $\{f_1, \ldots, f_{n-1}\} \subseteq S[V]^{\mathcal{S}_n}$ such that $S[V]^{\mathcal{S}_n} = \mathbb{Q}[f_1, \ldots, f_{n-1}]$.

(8.18) Exercise: Modular pseudoreflection groups.
Let p be a prime, let

$$G := \left\{ \begin{bmatrix} 1 & . & a+b & b \\ . & 1 & b & b+c \\ . & . & 1 & . \\ . & . & . & 1 \end{bmatrix} \in GL_4(\mathbb{F}_p); a, b, c \in \mathbb{F}_p \right\} \leq GL_4(\mathbb{F}_p),$$

and let $V := \mathbb{F}_p^{1\times 4}$ be the natural FG-module.
a) Show that G is a pseudoreflection group of order $|G| = p^3$.
b) Show that $S[V]^G$ is not a polynomial ring.

Proof. Needs Exercise (8.16), see [4, Ex.3.7.7]. ♯

(8.19) Exercise: Coefficient growth.
Let $H := \frac{f(T)}{\prod_{i=1}^r (1-T^{d_i})} = \sum_{d\geq 0} h_d T^d \in \mathbb{C}((T))$, where $f \in \mathbb{Z}[T^{\pm 1}]$ as well as $r \geq 1$ and $d_i \in \mathbb{N}$. Let $k \in \mathbb{Z}$ be the smallest integer such that the sequence $\{\frac{h_d}{d^k} \in \mathbb{C}; d \geq 0\} \subseteq \mathbb{C}$ is bounded. If $\mathrm{ord}_1(H) \leq -1$, show that $k = -\mathrm{ord}_1(H) - 1$.

Proof. See [1, Prop.2.1.2]. ♯

(8.20) Exercise: Krull dimension.
Let R be a finitely generated graded F-algebra.
a) Let $P \subseteq R$ be an extension of graded F-algebras, and let $R \to Q$ be an epimorphism of graded F-algebras. Show that $\dim(P) \leq \dim(R)$ as well as $\dim(Q) \leq \dim(R)$.
b) Let R be generated by a set of cardinality $r \in \mathbb{N}_0$. Show that $\dim(R) \leq r$, and that $\dim(R) = r$ if and only if $R \cong F[X_1, \ldots, X_r]$.

Proof. Uses $\lim_{z\to 1^-}(\cdots)$. ♯

(8.21) Exercise: Graded Nakayama Lemma.
Let R be a finitely generated graded F-algebra, an let $M = \bigoplus_{d\geq 0} M_d$ be a finitely generated $\mathbb{N}_0$-graded R-module.

a) Let $\bar{}: M \to M/MR_+$ be the natural epimorphism of graded R-modules. Moreover, let $X \subseteq M$ be a set of homogeneous elements. Show that the following conditions are equivalent:

i) The set X is a generating set of the R-module M.
ii) The set $\overline{X}$ is a generating set of the F-vector space M/MR_+.

b) Show that M is a projective R-module if and only if M is a free R-module.

Proof. a) See [4, La.3.5.1]
b) See [1, La.4.1.1] or [5, Exc.4.6.11] or [11, Thm.2.5]. ♯

(8.22) Exercise: Homogeneous systems of parameters.
Let R be a finitely generated graded F-algebra, and let $\{f_1, \ldots, f_r\} \subseteq R$, where f_i is homogeneous such that $\deg(f_i) > 0$ and $r = \dim(R) \in \mathbb{N}_0$. Show that $\{f_1, \ldots, f_r\}$ is a homogeneous system of parameters, if and only if for $j \in \{1, \ldots, r\}$ we have $\dim(R/(\sum_{i=1}^{j} f_i R)) = r - j$.

Proof. See [4, Prop.3.3.1]. ♯

(8.23) Exercise: Cohen-Macaulay algebras.
Let F be a field, and let $R \subseteq F[X] = F[X_1, X_2]$ be the subalgebra generated by $\{X_1^4, X_1^3X_2, X_1X_2^3, X_2^4\} \subseteq F[X]$.
a) Show that $\{X_1^4, X_2^4\} \subseteq R$ is a homogeneous system of parameters.
b) Show that R is not Cohen-Macaulay.

Proof. See [4, Ex.2.5.4]. ♯

(8.24) Exercise: Hironaka decomposition.
Let $G = \langle (1,2)(3,4), (1,3)(2,4) \rangle \leq \mathcal{S}_4$ be the Klein group of order 4, acting on $\mathbb{Q}[X] = \mathbb{Q}[X_1, \ldots, X_4]$ by permuting the indeterminates.
a) Show that the Hilbert series of $\mathbb{Q}[X]^G$ is given as $H_{\mathbb{Q}[X]^G} = \frac{1+T^3}{(1-T)\cdot(1-T^2)^3}$.
b) Find primary invariants $\{f_1, \ldots, f_4\} \subseteq S[V]^G$ such that $\deg(f_1) = 1$ and $\deg(f_2) = \deg(f_3) = \deg(f_4) = 2$, and secondary invariants $\{g_1, g_2\} \subseteq S[V]^G$ such that $\deg(g_1) = 1$ and $\deg(g_2) = 3$, yielding the Hironaka decomposition $S[V]^G = \bigoplus_{i=1}^{2} g_i \mathbb{C}[f_1, \ldots, f_4]$.

Proof. See [4, Ex.3.3.6(a)]. ♯

(8.25) Exercise: Hironaka decomposition.
Let $G = \langle \alpha, \beta \rangle \cong C_2 \times C_4$ be the abelian group of order 8 defined by

$$D_V : G \to GL_3(\mathbb{C}) : \alpha \mapsto \begin{bmatrix} 1 & . & . \\ . & 1 & . \\ . & . & i \end{bmatrix}, \beta \mapsto \begin{bmatrix} -1 & . & . \\ . & -1 & . \\ . & . & 1 \end{bmatrix}.$$

a) Show that the Hilbert series of $S[V]^G$ is given as $H_{S[V]^G} = \frac{1}{(1-T^2)^3} \in \mathbb{C}(T)$.
b) Show that there is no set of primary invariants $\{f_1, \ldots, f_3\} \subseteq S[V]^G$ such that $\deg(f_1) = \deg(f_2) = \deg(f_2) = 2$.

c) Find primary invariants $\{f_1, \ldots, f_3\} \subseteq S[V]^G$ such that $\deg(f_1) = \deg(f_2) = 2$ and $\deg(f_3) = 4$, and secondary invariants $\{g_1, \ldots, g_s\} \subseteq S[V]^G$ for some $s \in \mathbb{N}$, yielding the Hironaka decomposition $S[V]^G = \bigoplus_{i=1}^{s} g_i \mathbb{C}[f_1, \ldots, f_3]$.

Proof. See [4, Ex.3.3.6(b)]. ♯

(8.26) Exercise: Hironaka decomposition.
Let $G = \langle \sigma, \tau \rangle \cong Q_8$ be the quaternion group of order 8, and let

$$D_V \colon G \to GL_2(\mathbb{C}) \colon \sigma \mapsto \begin{bmatrix} i & . \\ . & -i \end{bmatrix}, \tau \mapsto \begin{bmatrix} . & -1 \\ 1 & . \end{bmatrix}.$$

a) Show that the Hilbert series of $S[V]^G$ is given as $H_{S[V]^G} = \frac{1+T^6}{(1-T^4)^2} \in \mathbb{C}(T)$.
b) Find primary invariants $\{f_1, f_2\} \subseteq S[V]^G$ such that $\deg(f_1) = \deg(f_2) = 4$, and secondary invariants $\{g_1, g_2\} \subseteq S[V]^G$ such that $\deg(g_1) = 1$ and $\deg(g_2) = 6$, yielding the Hironaka decomposition $S[V]^G = \bigoplus_{i=1}^{2} g_i \mathbb{C}[f_1, f_2]$.
c) Show that $S[V]^G \cong \mathbb{C}[X, Y, Z]/(Z^3 - X^2Y + 4Y^3)\mathbb{C}[X, Y, Z]$ as graded $\mathbb{C}$-algebras, where $\deg(X) = \deg(Y) = 4$ and $\deg(Z) = 6$.

Proof. See [1, Exc.2.5] or [12, Ex.5.5.1]. ♯

(8.27) Exercise: Cohen-Macaulay property.
Let p be a prime, let $G := \langle \pi \rangle \cong C_p$ be the cyclic group of order p, let F be a field such that $\mathrm{char}(F) = p$, and let $V = W \oplus W \oplus W$ as FG-modules, where

$$D_W \colon G \to GL_2(F) \colon \pi \mapsto \begin{bmatrix} 1 & 1 \\ . & 1 \end{bmatrix}.$$

Let $S[W] \cong F[X, Y]$ and $S[V] \cong F[X_1, Y_1, X_2, Y_2, X_3, Y_3]$.
a) For $1 \leq i < j \leq 3$ let $h_{ij} := X_iY_j - X_jY_i \in S[V]$. Show that $h_{ij} \in S[V]^G$.
b) Show that $\{Y_1, Y_2, Y_3\} \subseteq S[V]^G$ can be extended to a homogeneous system of parameters of $S[V]^G$, but is not a regular sequence in $S[V]^G$.

Proof. Uses Exercise (8.22), see [4, Ex.3.4.3] and also [12, Ex.5.5.2]. ♯

9 References and further reading

[1] D. Benson: Polynomial invariants of finite groups, London Mathematical Society Lecture Note Series 190, Cambridge University Press, 1993.

[2] W. Bruns, J. Herzog: Cohen-Macaulay rings, Cambridge Studies in Advanced Mathematics 39, Cambridge University Press, 1993.

[3] The Computational Algebra Group: MAGMA-V2.10 — The Magma Computational Algebra System, School of Mathematics and Statistics, University of Sydney, 2003, http://magma.maths.usyd.edu.au/magma/.

[4] H. Derksen, G. Kemper: Computational invariant theory, Invariant Theory and Algebraic Transformation Groups I, Encyclopaedia of Mathematical Sciences 130, Springer, 2002.

[5] D. Eisenbud: Commutative algebra, with a view toward algebraic geometry, Graduate Texts in Mathematics 150, Springer, 1995.

[6] The GAP Group: GAP-4.3 — Groups, Algorithms and Programming, Aachen, St. Andrews, 2003, http://www-gap.dcs.st-and.ac.uk/gap/.

[7] J. Humphreys: Reflection groups and Coxeter groups, Cambridge Studies in Advanced Mathematics 29, Cambridge University Press, 1990.

[8] R. Kane: Reflection groups and invariant theory, CMS Books in Mathematics 5, Springer, 2001.

[9] H. Kraft: Geometrische Methoden in der Invariantentheorie, Aspects of Mathematics D1, Vieweg, 1984.

[10] S. Lang: Algebra, Graduate Texts in Mathematics 211, Springer, 2002.

[11] H. Matsumura: Commutative ring theory, Cambridge Studies in Advanced Mathematics 8, Cambridge University Press, 1989.

[12] M. Neusel, L. Smith: Invariant theory of finite groups, Mathematical Surveys and Monographs 94, American Mathematical Society, 2002.

[13] L. Smith: Polynomial invariants of finite groups, Research Notes in Mathematics 6, Peters, 1995.

[14] H. Weyl: The classical groups, their invariants and representations, Princeton Landmarks in Mathematics, Princeton University Press, 1997.